JURNAL HUKUM Khaira Ummah

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Master of Law, UNISSULA

Criminal Law Policy in An Efforts to Combat Artifical Intelligance (AI) in Cyber Crime

Yuliana Putri Dharmayanti[1)] & Eko Soponyono[2)]

[1)]Master of Notary Law, Faculty of Law, Sultan Agung Islamic University (UNISSULA) Semarang, Indonesia, E-mail: yulianaputridharmayanti.std@unissula.ac.id

[2)]Master of Notary Law, Faculty of Law, Sultan Agung Islamic University (UNISSULA) Semarang, Indonesia, E-mail: ekosoponyono@unissula.ac.id

Abstract. *The development of Artificial Intelligence (AI) technology has had a major impact on various areas of life, including in the criminal law aspect. AI is not only used for positive purposes, but also opens up opportunities for new cybercrimes such as deepfakes, automated phishing, and digital identity theft. These crimes pose new challenges in law enforcement, especially regarding criminal liability and the lack of legal regulations that specifically regulate AI-based crimes. This study aims to analyze criminal law policies in dealing with AI-based cybercrime, both in the current positive law and the prospects for its regulation in the future. This study uses a normative legal method with a descriptive-analytical approach. Data were collected through a literature study of laws and regulations such as the Criminal Code, the ITE Law, and relevant literature. The results of the study indicate that existing regulations have not explicitly regulated the use and misuse of AI in cybercrime. The applicable legal provisions are still general and have not been able to accommodate the complexity of AI-based crimes. This indicates a legal vacuum that must be filled immediately through the renewal of criminal law policies that are more adaptive and progressive to the development of information technology. Based on the results of the analysis, a reformulation of criminal law policies is needed that can answer the challenges of AI-based cybercrime through the approach of the theory of the rule of law, the theory of criminal responsibility, and the theory of criminal policy. This research provides a theoretical contribution to the development of criminal law in the digital era, as well as being a practical reference for policy makers in formulating relevant and effective regulations. Thus, it is hoped that the Indonesian legal system can respond to technological developments by creating regulations that are fair, clear, and able to protect the public from increasingly complex cybercrimes.*

Keywords: *Artificial Intelligence; Criminal Liability; Criminal Law Policy; Cyber Crime; Legal Vacuum.*

1. Introduction

In the current era of industry 5.0, technological advances are utilized to facilitate the fulfillment of human needs and increase efficiency in daily activities. Innovation in information technology provides significant benefits to society, due to the various positive benefits it offers, such as increased efficiency and productivity, as well as accelerated communication and information dissemination. Information technology can be used to

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

collect, process, and analyze data, resulting in fast and accurate information. The impact of this development is enormous for society, one of which is the increasingly rapid progress of business. Continuous innovation in information technology, such as artificial intelligence (AI), opens up exciting opportunities to create shared value among economic actors in the business world.[1]

Technology plays a very important role in the current era of globalization, where it has become an inseparable element of everyday life. Technological advances have changed the structure of society from being local to more global. This change is triggered by the presence of information technology. The integration of information technology, media, and computers has had a significant impact on the way we interact and communicate. With this progress, access to information has become faster and wider, thus accelerating the process of spreading knowledge and culture. This encourages the formation of wider social networks and enables cross-country collaboration, which in turn strengthens the connectivity between individuals and communities around the world.

Humans and AI can collaborate in decision-making with minimal influence from personal values. In comparing the problem-solving methods between the two, it can be seen that AI is superior in handling problems that have a low level of uncertainty and complexity, and require high analytical skills. In contrast, humans are better able to solve problems that have a higher level of uncertainty and complexity, with relatively lower analytical needs. In addition, AI is expected to be able to handle tasks and problems that involve a greater level of uncertainty through the application of deeper learning processes.[2]

Artificial Intelligence (AI) technology is basically similar to other tools or media, where it has the potential to provide benefits or cause risks. For example,A knife used by a chef can produce delicious food, but if a knife is given to someone who wants to do evil, it will become a dangerous weapon.. Likewise with AI technology, if not applied wisely and proportionally in the context of learning, it can have negative impacts.

Technological advances also have a negative impact on human development and civilization. The increasing use of information and communication technology, especially through social media, has given rise to various types of cybercrime. One example is the cybercrime of manipulation, or what is known as deepfake. This is a new form of crime in the modern era that has emerged thanks to the sophistication of technology that is universal in cyberspace, thus having a negative impact that is not physically visible but is just as detrimental as other crimes. In enforcing the law regarding cybercrime, perpetrators who violate the law must be responsible for the losses incurred, either due to negligence or intent. Therefore, the application of legal rights and obligations needs to emphasize the importance of enforcing legal accountability.

Thus, it is important for the legal system to develop effective mechanisms to deal with cybercrime, including establishing appropriate sanctions and clear law enforcement

[1]Marsella, et al., "Analysis of Artificial Intelligence Implementation for Business: Systematic Literature Review", Journal of Criminal Law. Vol.4, No.2, p.134
[2]Tri Wahyudi, "Case Study of the Development and Use of Artificial Intelligence (AI) as a Support for Indonesian Community Activities", Journal of Criminal Law. Vol.9, No.1, p.29

procedures. Public education and awareness about the risks of cybercrime should also be improved, so that individuals are more careful in using technology. In addition, collaboration between the government, technology service providers, and the community is needed to create a safer digital environment. These efforts will not only protect individuals from cybercrime, but will also support the development of more responsible and ethical technology in society.

In law enforcement against cybercrime, perpetrators who commit unlawful acts must be held accountable for the losses caused, whether due to negligence or intent. The application of legal rights and obligations must emphasize the importance of enforcement through legal accountability mechanisms.[3]

This legal accountability serves to ensure that perpetrators of crimes receive appropriate sanctions, so that they can provide a deterrent effect and prevent similar actions from happening again. In addition, effective law enforcement must also involve cooperation between various parties, including law enforcement agencies, technology service providers, and the general public. This aims to create a safe environment in cyberspace, as well as raise awareness of the risks and consequences of cybercrime. Through this approach, it is hoped that a legal system can be created that is responsive and adaptive to developments in information technology. In addition, it is also important to raise public awareness of the risks of cybercrime and the importance of maintaining the security of personal information. Education and training on cybersecurity must be an integral part of efforts to prevent and combat cybercrime.

Due to developments*artificial intelligence,*Nowadays it has spread to various pthe device thatused in almost all sectors of life, from finance and business, engineering, gadgets, aviation, transportation, and so on. Access to artificial intelligence that is increasingly easy and commonly used today is starting to be used for criminal purposes. Some forms of cybercrime based on Artificial*Intelligence*which are currently rampant include things like*Deep FakeFraud*that isthe use of Artificial Intelligence algorithms to create fake videos that resemble someone, Artificial Intelligence - *Generated Phishing Emails*(creating phishing via email withlevelvery high personalization), and Identify Theft (stealing personal data from social media to create fake identities using Artificial Intelligence).[4]

In discussing cyber crime from a criminal law perspective, I will relate it to several crimes regulated in the Criminal Code (KUHP). Some examples of cyber crime that can be related to the provisions of the Criminal Code include: Theft as regulated in Article 362 of the Criminal Code, Fraud as regulated in Article 378 of the Criminal Code, and Extortion and threats as regulated in Article 335 of the Criminal Code.

Based on the author's research, criminal acts related to Malware-AI[5]has not been specifically regulated in Indonesian law. However, there are a number of criminal provisions outside the ITE Law that can be used to ensnare such violations, considering that the ITE

[3]Izil Hidayat Putra, "Legal Protection for Victims of Artificial Intelligence (AI) Abuse in the Form of Pornographic Deepfakes According to Statutory Regulations", vol.1, no.2, p.112

[4]Smith, J. "AI and Fraud: The Rise of Deepfake Scams."*Cybersecurity Review.*Vol. 15, No. 3, pp. 45-50.

[5]Malware-AI is a type of malicious software that uses artificial intelligence to attack computer systems.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Law is the latest and most relevant regulation in dealing with cybercrime. Several articles in the Criminal Code, such as articles 335, 362, 378, and 406, as well as the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, can also be considered in this context.[6]

Artificial Intelligence(AI) is used in public service systems, automated decision-making, and complex digital content creation. However, along with that, new challenges have also emerged in the form of potential violations of the law, unclear criminal liability, and the possibility of misuse by individuals and corporations. In this context, the ITE Law has been amended through Law No. 1 of 2024 on Law No. 11 of 2008, which aims to maintain a clean, healthy, ethical, productive, and just digital space in Indonesia. However, although the ITE Law regulates various aspects of criminal acts in the digital realm, provisions regarding the use of AI-based technology specifically are still very limited. This creates a legal vacuum in directly addressing AI-based crimes.[7]

Thus, a deep theoretical foundation is needed, including:

a. Criminal Policy Theory:

This theory emphasizes the importance of a strategic criminal law approach to prevent and combat criminal acts. In the context of AI, this theory encourages the formulation of criminal law policies that are anticipatory to technological developments.

b. Theory of Criminal Responsibility:

This theory is central to the discussion about who should be held accountable in the context of AI use. In classical criminal law systems, the legal subject is a human or legal entity that has consciousness and will. However, the presence of AI as a semi-autonomous entity challenges this traditional concept.

c. Progressive Legal Approach:

This approach emphasizes that the law must be able to adapt to the development of the times and answer the needs of society that are constantly changing due to technological advances. In this context, criminal law must be able to adapt to technological developments and answer the needs of society that are constantly changing due to technological advances.

In this case, it has also been regulated in the ITE Law No. 1 of 2024 regarding the amendment to the ITE Law No. 11 of 2008 as in Article 13A concerning Digital Identity: This article regulates digital identity used in the implementation of electronic certification. Digital identity is electronic data that can be used to identify a person electronically. The implementation of this article is expected to increase the security and reliability of electronic certification, because digital identity can be used to ensure that the person applying for electronic certification is the real person. This means that digital identity can also be used to prevent fraud and identity misuse. Article 16A, Article 27A, and Article 40A.

---

[6]Supanto, et al. "Deviation RegulationArtificial IntelligenceIn Criminal ActsMalwareBased on the Republic of Indonesia Law Number 19 of 2016", vol.9, no.2, p.132

[7]ITE Law No. 1 of 2024

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Thus, although the ITE Law is the main reference in handling cybercrime, the provisions contained in the Criminal Code and other regulations still have significant relevance. This shows that to address issues that arise due to technological developments, especially in the context of Malware-AI, a comprehensive legal approach is needed.[8]

This study also highlights that the regulations in Law Number 1 of 2024 are designed to deal with the complexity and dynamics of cybercrime that continues to grow. In addition, protection for the financial and banking sectors is also strengthened through significant sanctions. Legal analysis shows that this law provides a clearer legal basis for dealing with cybercrime that is cross-border and rapidly developing. This means that Law Number 1 of 2024, which is planned to come into effect soon, has provided a more comprehensive legal framework in protecting the public from cybercrime. With ongoing legal revisions and reforms, this regulation is expected to be able to keep up with technological developments and modern crime modes, thus creating a safer digital environment in Indonesia.

In addition, the existence of a legal vacuum specifically regarding Malware-AI indicates the need for further efforts in regulatory updates that can accommodate technological developments and the crimes that accompany them. By understanding the existing legal framework, we can formulate more effective steps to protect society from the threats posed by cybercrime. This research is expected to contribute to the discussion regarding the need to revise or add legal provisions that are more in line with current challenges.

2. Research Methods

The approach used by the author in this study is the Normative Juridical approach. The Normative Juridical Approach is a legal research that uses secondary data, and is carried out by emphasizing and adhering to the legal aspect. Normative Juridical Research is a literature, namely secondary data research. The Normative Juridical Approach because what is studied is the legal principle, legal aspects, and legal rules.

3. Results and Discussion

3.1. Criminal Law Policy in Efforts to Tackle AI (Artificial Intelligence) Cyber Crime in Current Positive Law

As the threat of cybercrime increases, such as credit card fraud (carding), ATM/EDC skimming, hacking, system cracking, phishing, malware distribution (such as viruses, worms, trojans, and bots), cybersquatting, pornography, online gambling, and transnational crimes involving drug trafficking, organized crime (mafia), terrorism, money laundering, human trafficking, and the underground economy, it is very important to implement comprehensive data protection. In this case, there is a need for binding and consistently enforced legal rules to protect personal information. These rules also aim to ensure that data subjects remain in full control of their personal information, avoid misuse, and provide security and privacy guarantees in the digital world.[9]

In today's digital era, misuse of technology and social media is increasingly common in society. One case that has recently come under the spotlight is the case of the spread of deviant content through the Facebook platform, carried out by an account named "Fantasi

[8]Supanto, et al., Ibid p. 133
[9]Zainuddin Kasim, "Criminal Law Policy for Combating Cyber Crime in Indonesia, Vol.2, No.1, July 2023, p.20

Sedarah." In the group, various deviant sexual content was spread, especially on the theme of incest (incestuous relationships) and sexual exploitation, which clearly contradicts legal norms, ethics, and public morality.

Such actions are a form of cybercrime that can be subject to criminal sanctions based on applicable laws and regulations. The perpetrators in this case can be charged with Article 27 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016, which regulates the prohibition of distribution or transmission of content that violates morality. In addition, Article 45 paragraph (1) of the ITE Law can also be imposed, which regulates criminal sanctions for anyone who intentionally and without the right distributes or makes the content accessible.

The increase in cybercrime, which is increasingly diverse and sophisticated, requires systematic efforts in formulating policies that can accommodate the need for personal data protection. Crimes such as credit card fraud (carding), system hacking, and the spread of malware have detrimental impacts on individuals, organizations, and even countries. Therefore, laws governing personal data protection are very relevant and urgent to be implemented in order to mitigate the risks posed.

However, the lack of clear regulations regarding personal data protection has led to increasing cases of misuse of information systems and personal data. Therefore, it is very important to develop a system that can overcome these problems. Currently, Indonesia still does not have a law that specifically regulates personal data protection. The existing regulations are only spread across various different laws, so it is necessary to establish a more comprehensive, detailed, and firm law to regulate the protection of personal property rights.[10]

The importance of personal data protection is increasingly felt along with the increasing use of information technology in everyday life. Without clear and adequate regulations, the potential for misuse of personal data is increasing, both for commercial purposes and cybercrime. This requires the state to immediately take concrete steps in drafting laws that not only regulate individual rights over their personal data, but also provide strict sanctions for perpetrators of misuse. The existence of this comprehensive law is expected to strengthen public trust in the digital system and prevent data exploitation that is detrimental to irresponsible parties..

The Criminal Code (KUHP) is the main foundation for criminal law regulations in Indonesia. Although this Criminal Code originated from the Dutch colonial era, until now, because there has been no change or acceptance of the reforms proposed by Indonesian criminal law experts since 1963, the existing Criminal Code is still used to ensure the existence of criminal law in Indonesian society.[11]

---

[10]Zainuddin Kasim, Ibid, .p.20

[11] Dwila Annisa Rizki Amalia, et.al. “Criminal Law Policy in Efforts to Combat Cyber Terrorism”, Vol.3, No.2, 2021, p.232

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

However, the use of the Criminal Code which is still derived from colonial legal products is not free from criticism, especially regarding its relevance and suitability to the social, political, and cultural conditions of Indonesia which continue to develop. The process of renewing the Criminal Code has been a serious concern for academics and legal practitioners in Indonesia for a long time. Various efforts to renew the Criminal Code have been made, but the expected changes have not been implemented comprehensively to date. Renewing the Criminal Code is considered an important step to align Indonesian criminal law with the values and needs of modern society, including in terms of protecting human rights and social justice..

Cybercrime prevention policies through criminal law are included in the scope of penal policies, which are part of the overall criminal policy. From a criminal policy perspective, efforts to prevent crime, including combating cybercrime, cannot be done by relying solely on criminal law separately. Instead, such prevention needs to be carried out with a more systematic and integrated approach.

Basically, criminal law policy or policy aims to formulate criminal law in an appropriate manner, provide guidelines for lawmakers, and ensure effective implementation of criminal law. Legislative policy plays an important role in determining the direction of criminal legislation, because the objectives to be achieved must be determined from the start. For example, in Article 26 paragraph (2) of the ITE Law, the provision does not provide criminal sanctions for perpetrators, where victims can only file civil lawsuits. In addition, Article 26 of the ITE Law only covers basic protection of personal data. Information technology experts criticize Article 26 because it has shortcomings, namely not providing adequate protection for users of personal data used for certain interests by companies. Data security aims to improve data protection by: 1) Protecting data from being accessed by unauthorized parties; and 2) Preventing unauthorized parties from entering or deleting data.

In this crime, Indonesia needs a more specific legal instrument. Because currently the law in Indonesia, especially in the Criminal Code (KUHP) only regulates the crimes of Theft, Fraud, extortion and robbery. In this case, it has been regulated in Articles 335, 362, 378 of the Criminal Code.

Article 335 of the Criminal Code regulates the crime of unpleasant acts, especially those related to unlawful coercion of will, accompanied by threats or violence. This article is often used in the context of criminal law to prosecute acts such as threats, intimidation, or coercion, which are not explicitly included in other special articles in the Criminal Code. However, the application of this article is often in the spotlight because it is considered to have broad and multi-interpretable elements, so it must be applied carefully so as not to cause excessive criminalization of expression or differences of opinion. Article 335 of the Criminal Code reads:

"Anyone who unlawfully forces another person to do, not do or allow something, by using violence, a threat of violence, or other acts, whether against that person or another person, is punished by imprisonment for a maximum of one year or a fine of up to four thousand five hundred rupiah."

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

In the context of cybercrime using Artificial Intelligence (AI), Article 335 of the Criminal Code can be linked if AI is used to: Send automated threats to someone; Force someone to provide personal data through digital threats.

The criminalization policy itself is a policy that determines an action that was previously not considered a crime, to be a crime. The decision to criminalize or decriminalize must be based on certain policy considerations that take into account various factors, including: 1) Balance between the methods used and the results to be achieved; 2) Analysis of the costs incurred compared to the results obtained in achieving the stated goals; 3) Research or interpretation of the goals to be achieved, taking into account other priorities in the allocation of human resources; 4) The social impact of criminalization and decriminalization, which also considers possible secondary effects.

Criminal law policy in Indonesian positive law is currently still in the early stages of responding to the development of cybercrime based on Artificial Intelligence (AI). The main instruments used in dealing with cybercrime are the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), which was last amended by Law No. 1 of 2024.

In general, the regulation has indeed regulated several forms of cybercrime such as illegal access, hacking, dissemination of false information, and violation of personal data. However, in the context of AI-based cybercrime, existing positive law has not explicitly regulated the role, legal responsibility, or limitations of the use of artificial intelligence in cybercrime. For example, crimes using deepfake, automated phishing, or AI-driven malware are still difficult to classify firmly in the category of crimes regulated by the Criminal Code or the ITE Law.

In this case, Indonesia still has a legal vacuum where Artificial Intelligence (AI) is a digital entity that does not have a clear legal status, making it difficult to determine who is criminally responsible for its actions. This creates legal uncertainty and can hamper law enforcement efforts.

From the author's perspective, this shows that the existing criminal law policy is still inadequate in substance and technically in responding to the complexity of AI-based cybercrime. The legal vacuum arises because the Indonesian legal system has not anticipated the very rapid development of digital technology, especially in terms of legal subjects, criminal liability, and digital crime prevention models that use AI as a tool or actor.

Therefore, according to the author, it is necessary to reformulate criminal law policies which include: Preparation of new regulations or revision of the ITE Law which explicitly regulates criminal acts involving AI; Strengthening the capacity of law enforcement officers in understanding AI technology and how it works in cybercrime; Creation of ethical and legal standards for the use of AI, including in the public and corporate sectors; Establishment of special institutions or units that handle high-tech digital crimes. With these steps, criminal law policies are expected to be more adaptive, comprehensive, and effective in dealing with new threats from AI-based cybercrime in the era of digital transformation.

3.2. Criminal Law Policy in Efforts to Tackle Artificial Intelligence Cyber Crime in Future Positive Law

Existing and continuously developing technology is evidence of human civilization advancing very rapidly. The presence of technology has certainly helped humans a lot in carrying out

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

their daily lives. In fact, the presence of technology can gradually replace human tasks, so that tasks can be carried out efficiently using the help of technology. Human ability to develop technology then leads technology companies to continue to innovate to create new devices in the world of technology. Artificial Intelligence or artificial intelligence is one of the most advanced technologies in human civilization today. Artificial intelligence allows people to do work easily, because all work can be done by the system without having to be manually controlled by humans. However, the development of technology including the entry of Artificial Intelligence devices is not without problems. The development of technology also brings new problems in the realm of criminal law. Where the development of existing technology also brings new types and modes of cyber-technology-based crimes, or Cyber Crime.

Despite the purpose of technology in order to improve the efficiency of people's lives, its presence is not without causing new crimes. Currently, technology is not always used for the good of society. Technology that continues to develop coupled with the presence of automation devices such as Artificial Intelligence allows criminals to commit cybercrimes by utilizing the Internet of Things and other technological media.[12]Cybercrime includes various illegal acts carried out using computer networks and the internet, such as hacking, spreading malware, data theft, internet fraud, misuse of Artificial Intelligence, and so on.

The increase in the number of cybercrimes in Indonesia is very high every year. This then encouraged the Government of the Republic of Indonesia to build a stronger and more relevant legal framework in order to reduce the number of cybercrimes in Indonesia. Law Number 11 of 2008 concerning Information and Electronic Transactions became one of the initial legal frameworks in combating cybercrimes. The law was then updated in 2016 because several of its articles were no longer relevant and needed the addition of new articles through Law Number 19 of 2016 concerning Information and Electronic Transactions. Although the legal basis already exists, the implementation of the law faces various challenges.[13]Therefore, there needs to be a reconstruction of existing legal products for combating cybercrime by synchronizing them with existing legal developments and types of cybercrime.

Legal products that regulate artificial intelligence are not yet available. The legal vacuum in the regulation of artificial intelligence and special regulations regarding the handling of crimes based on Artificial Intelligence causes existing crimes to not be accommodated and regulated specifically and in detail according to the portion and type of crime.[14]

The development of artificial intelligence today has penetrated into various devices and is used in almost all sectors of life ranging from finance and business, engineering, gadgets, aviation, transportation, and so on. Access to artificial intelligence that is increasingly easy and commonly used today is starting to be used for criminal purposes. Some forms of

[12]Intan Permata Sari, et.al. "Analysis of Cyber Crime Policy in Positive Law in Indonesia". Journal of Law and Nation (JOLN). Vol. 3, No. 2. May 2024, p. 396.
[13]Mahrina, Joko Sasmito, Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", Pena Justisia Journal: Media *Communication and Legal Studies*, Vol. 21, no. 2, December 2022, p. 345.
[14]Nugroho, HT Wahyuni. "Challenges of Cybercrime Regulation in Indonesia: Perspective of Artificial Intelligence Technology Development". Journal of Law and Technology. Vol. 7, No. 2, p. 129.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

cybercrime based on Artificial Intelligence that are currently rampant include Deepfake Fraud (the use of AI algorithms to create fake videos that resemble someone), AI-Generated Phishing Emails (creating phishing via email with a very high level of personalization), and Identify Theft (theft of personal data from social media to create fake identities using AI).[15]The main challenges in eradicating cybercrime based on artificial intelligence are due to the lack of specific regulations, limited capabilities and knowledge of law enforcement officers, and minimal technological infrastructure in detecting and preventing cyber attacks.

Criminal law regulations regarding the handling of cybercrime based on Artificial Intelligence, especially the Electronic Information and Transactions Law (UU ITE), are a very important main instrument. However, although the law already exists, its implementation has not been able to accommodate the existing problems. Some limitations in positive law in the context of handling AI-based cybercrime include:

1. Lack of regulation especially AI Cyber Crime
2. The definition and scope of cybercrime in the ITE Law tends to be general, so it is not yet able to cover AI-based crimes.
3. Lack of capacity of law enforcement officers, especially in relation to identifying and handling cyber crimes based on artificial intelligence.

The renewal of legal policies regarding the handling of cybercrime based on artificial intelligence is currently very urgent. This is certainly due to the legal vacuum where there is no regulation that regulates in detail and in detail the problem of cybercrime based on artificial intelligence in Indonesia. The legal vacuum that regulates artificial intelligence in Indonesia is especially related to the position of responsibility of Artificial Intelligence in the legal industry in Indonesia. This legal vacuum in the field of AI is what causes many legal practitioners to still utilize regulations related to technology regulations to respond to problems in the field of artificial intelligence, one of which is through the Electronic Information and Transactions Law or the ITE Law.[16]

Based on the problem of legal vacuum in the field of AI, it is necessary to anticipate all possibilities that could arise due to the lack of regulation in the field of artificial intelligence. In this new regulation, it is hoped that there will be detailed and clear considerations related to the position of Artificial Intelligence in legal accountability. Explicitly, artificial intelligence can indeed carry out legal acts like existing legal subjects. However, in practice, artificial intelligence is a system built by humans and cannot act as a legal subject. Therefore, a detailed interpretation is needed in the new legal regulation that clearly regulates artificial intelligence, especially in the context of overcoming cybercrime based on Artificial Intelligence in Indonesian law.[17]

As is commonly known, Artificial Intelligence's position is still very vague in Indonesia. Only the Electronic Information and Transaction Law and the Government Regulation on the Implementation of Electronic Systems and Transactions regulate the field of artificial

[15]Smith, J. “AI and Fraud: The Rise of Deepfake Scams.” Cybersecurity Review. Vol. 15, no. 3, p. 45-50.
[16]Ni Made Yordha Ayu Astiti. “Strict Liability of Artificial Intelligence: Accountability to AI Regulators or AI Given the Burden of Accountability”. Udayana Master of Law Journal. Vol. 12, No. 4, December 2023, p. 969.
[17]Ni Made Yordha Ayu Astiti. Op.cit, p. 967.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

intelligence. The regulations in these two legal products do not mention artificial intelligence clearly, only the term "Electronic Agent" is explained in the two regulations.

Regulations regarding Artificial Intelligence or artificial intelligence have not been regulated in the latest Criminal Code. In the latest Criminal Code, only cybercrime is regulated. However, the cybercrime instrument in the latest Criminal Code that has been drafted is also very important as one of the legal instruments that regulates crimes using technology and internet media. New regulations in dealing with cybercrime in Law Number 1 of 2023 concerning Criminal Law include hacking, data theft, and the spread of malware. This shows that Law Number 1 of 2024 has a stronger legal basis than previous regulations by explaining the elements of criminal acts in more detail.[18]

The articles in the law cover a variety of cybercrimes, including illegal access in Article 332, attacks on state information systems in Article 333, and violations of the financial and banking system in Article 334. The sanctions imposed are quite severe, ranging from imprisonment to large fines, in order to create a deterrent effect. For example, illegal access involving a security system violation can be punished with up to 8 years in prison, while violations related to confidential government information can reach 12 years in prison.[19]

This study highlights that the regulations in Law Number 1 of 2024 are designed to deal with the complexity and dynamics of cybercrime that continues to grow. In addition, protection for the financial and banking sectors is also strengthened through significant sanctions. Legal analysis shows that this law provides a clearer legal basis for dealing with cybercrime that is cross-border and rapidly developing. This means that Law Number 1 of 2023, which is planned to come into effect soon, has provided a more comprehensive legal framework in protecting the public from cybercrime. With ongoing legal revisions and reforms, this regulation is expected to be able to keep up with technological developments and modern crime modes, thus creating a safer digital environment in Indonesia.

The presence of Law Number 1 of 2024 which comprehensively regulates cybercrime is an important foothold for the development of future regulations, especially in facing new challenges related to crimes involving Artificial Intelligence (AI). With the rapid development of AI technology, the modus operandi of cybercrime is increasingly complex, ranging from automated attacks through bots to data manipulation using intelligent algorithms. In this context, positive legal reform is very urgent so that the legal system can anticipate and overcome emerging threats.

The urgency of updating regulations related to AI in Cyber Crime lies in the ability of this technology to accelerate, expand, and hide traces of crime. AI can be used to create adaptive malware, deepfakes, and data manipulation that is very difficult to detect. In existing positive laws, such as the ITE Law or the new Criminal Code, there are no explicit regulations regarding the use of AI for criminal purposes. This creates a legal vacuum that can be exploited by criminals. Therefore, the revision of existing regulations must include specific elements regarding AI in cybercrime.

---

[18]Yosua Hia. "Legal Analysis of Special Articles Related to Cybercrime in the New Criminal Code (Law Number 1 of 2023)". SELISIK Journal. Vol. 10, No. 1, June 2024, p. 158.
[19]Joshua Hia. Op.cit., pp. 161-163.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

The necessary updates include the addition of provisions on crimes involving the development, use, or distribution of AI technology for illegal purposes. For example, regulations need to specifically regulate the creation of Deepfakes for fraud, the use of AI for attacks on critical infrastructure, and market manipulation through intelligent algorithms. In addition, it is important to define legal responsibilities for irresponsible AI developers and users, including algorithm audit mechanisms and appropriate criminal sanctions.

The legal reform picture should also include international collaboration, given the cross-border nature of AI-based cybercrime. Indonesia can learn from other countries that have begun to regulate this technology, such as the European Union with the Artificial Intelligence Act or the United States' approach through laws governing AI-based data security. Legal reform in Indonesia should emphasize the integration of global standards, monitoring algorithms, and developing the capacity of law enforcement to handle AI Cyber Crime cases. With this reform, the Indonesian legal system will not only be responsive to the challenges of modern technology, but also create a fair and relevant legal framework. This is in line with the objectives of Law Number 1 of 2024, namely to provide stronger legal protection for people in the digital era. This step also reflects a progressive legal vision that not only reacts to threats, but is also proactive in creating a safe and fair digital space.

Although the regulation on cybercrime has existed and is made in more detail in the latest Criminal Code. However, this does not mean that artificial intelligence does not need to be regulated. Legal products of laws and their derivatives are still needed to be present in regulating Artificial Intelligence Cyber Crime or cybercrime based on artificial intelligence. The current legal vacuum has a major impact on law enforcement and preventive efforts that can be carried out by the government, law enforcers, and legal practitioners. The legal vacuum is also feared to cause an increase in the number of abuses of Artificial Intelligence for various types of cybercrime and other crimes in Indonesia. Therefore, a legal reconstruction is needed that aims to present a criminal law update that regulates clearly, in detail, and completely regarding Artificial Intelligence and its law enforcement.

Based on the explanation above and by looking at the legal facts and facts in society that are currently happening, there are several legal recommendations to carry out legal updates to combat Artificial Intelligence Cyber Crime, especially in the jurisdiction of Indonesia. Legal updates and actions that can be taken immediately include the following:

1. Formation of Artificial Intelligence Law

Until now, Indonesia still does not have a legal product that specifically regulates Artificial Intelligence. Without specific regulations governing artificial intelligence, it is very difficult to distinguish between the legitimate and permitted uses of Artificial Intelligence and those that are prohibited in the context of cybercrime. In the Artificial Intelligence Law, there will be several things that must be regulated. Some of the things that are recommended to be regulated in the law include:

a. Definition and scope of Artificial Intelligence

b. Legal liability if AI is used as a medium and tool to commit crimes

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

c. Technology monitoring and auditing that requires special state institutions or agencies to ensure that the development and use of AI is carried out in accordance with applicable legal norms.

2. Revision of the Electronic Information and Transactions Law

As the main legal umbrella in law enforcement and handling of cybercrime, this law requires revision and legal renewal in it. The ITE Law that currently exists and is in effect does not specifically regulate artificial intelligence. This is what then causes a legal vacuum in enforcing Artificial Intelligence in the context of cybercrime. In the changes made to the ITE Law, there must be clearer regulations regarding the articles that explain the types of AI-based cybercrime as well as the form of law enforcement.

3. Digital Forensic Technology Advances

Cybercrime is very difficult to track, especially cybercrime that uses Artificial Intelligence as a medium for its crimes. That is why digital forensic technology in Indonesia needs to be upgraded. Cybercrime with artificial intelligence is very difficult to detect, this is closely related to the anonymous nature of Artificial Intelligence, making it very difficult to know who is responsible for the crimes that occur. Some things that can be done in order to improve the digital forensic capabilities of law enforcement officers in Indonesia include:

a. Improving digital forensic infrastructure in Indonesia. This can be done by providing software and hardware that can detect, analyze, and track Artificial Intelligence activities in a cybercrime that occurs.[20]

b. Cooperation with international institutions to adopt the digital forensic technology they use so that Indonesia can get technology transfer.

4. International Cooperation

International cooperation with other countries is essential in law enforcement and combating cybercrime based on artificial intelligence. This is because cybercrime is often cross-country and cross-nation. Therefore, handling cybercrime based on artificial intelligence requires collaboration between countries. Making extradition agreements for cybercriminals and actively participating in international forums, for example through the Global Forum on Cyber Expertise, is a cooperation strategy that can be carried out by Indonesia in the future.

5. Strengthening Digital Education and Literacy

Strengthening digital literacy and education for the community is a very important step to take. This is because people who do not understand technology, especially Artificial Intelligence, often become victims of cybercrime. So the strategy of strengthening digital literacy for the community is very important to do by conducting a national campaign on digital literacy and Artificial Intelligence and by creating Artificial Intelligence modules in schools to educate the community from an early age.[21]

---

[20]Casey, E. 2011. "Digital Evidence and Computer Crime: Forensic Science, Computers, and The Internet (3rd edition)". Academic Press.

[21]Livingstone, S., Helsper, E. J. “Gradations in Digital Inclusion: Children, Young People, and the Digital Divide”. New Media & Society. Vol. 9, no. 4, p. 671-696.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

The above recommendations can be stated in government policies either through legal and regulatory reforms or through government programs. The purpose of taking action and legal reforms to combat and enforce the Artificial Intelligence Cyber Crime law above is basically to create regulations that are adaptive to the increasingly advanced technological developments in today's society. With the steps above, it is hoped that Indonesia will be more aware of the technological developments that are occurring and will be able to overcome and combat increasingly frequent artificial intelligence-based cybercrimes.

Regulation of the misuse of artificial intelligence (AI) in cybercrime has become a concern in several developed countries. In the European Union, the Artificial Intelligence Act is designed to regulate the use of AI based on its level of risk, with a special category for high-risk technologies that could harm public security or human rights.[22]This regulation requires a thorough audit of algorithms, transparency of operations, and the imposition of severe sanctions for violations that occur. Meanwhile, the United States through the Algorithmic Accountability Act emphasizes the responsibility of AI developers to ensure that their technology is not misused, including protection against data discrimination or digital security exploitation.[23]In China, the government has strict regulations regarding data security and the use of AI technology, such as requiring companies to include risk prevention mechanisms in every AI-based product.

Indonesia can adapt several key elements of the regulations in these countries. First, implementing a thorough audit for AI technology before it is launched, as the European Union does, can help ensure that the technology in circulation is safe from potential misuse. Second, developing a policy of AI developer liability, as in the United States, allows legal sanctions to be applied to technology manufacturers who fail to anticipate security gaps or misuse of their products. Finally, China's approach to data protection and digital security can be an inspiration in forming comprehensive regulations to prevent data exploitation by AI technology.

In addition, Indonesia needs to encourage international cooperation in designing this regulation, such as the Global Partnership on Artificial Intelligence (GPAI) initiative which aims to strengthen global collaboration for the regulation and development of AI technology ethically and safely. With the right adaptation of international practices, Indonesia can form a legal framework that is more responsive to the risks of AI-based cybercrime.

The Government of the Republic of Indonesia has actually issued Circular Letter Number 9 of 2023 concerning the Ethics of Artificial Intelligence which contains regulations regarding the use of artificial intelligence specifically as well as guidelines for the use of AI in Indonesia.[24]In addition, several things about artificial intelligence have also been regulated

[22]European Commission. Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act).https://eur-lex.europa.eu. Cited on December 7, 2024.
[23]US Congress. Algorithmic Accountability Act of 2019.https://www.congress.gov. Cited on December 7, 2024.
[24]Online Law, Measuring the Prospects of Artificial Intelligence Regulation in Indonesia https://www.hukumonline.com/berita/a/menakar-prospek-pengaturan-artificial-intelligence-diindonesia/Accessed December 7, 2024.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

in the Personal Data Protection Act which can affect the use of artificial intelligence. Then there is also the National Strategy for Artificial Intelligence (SNKI).[25]

In order to handle and enforce the law on Artificial Intelligence Cyber Crime in Indonesia, the government is expected to immediately form regulations that specifically regulate this matter. Based on existing problems, a Law on the Use and Supervision of Artificial Intelligence is needed in the Indonesian national legal system. The creation of this legislation aims to be a legal basis and an important foundation in handling and enforcing the law on Artificial Intelligence Cyber Crime in Indonesia which is currently not regulated. With the formation of the Law on the Use and Supervision of Artificial Intelligence, it is hoped that there will be a strong legal basis in regulating the development, use, and supervision of AI technology as well as overcoming the potential for misuse of artificial intelligence to help humans commit crimes.

The Law on the Use and Supervision of Artificial Intelligence is also expected to cover various important aspects. Some important aspects that are expected to be regulated in this law include:

1. General requirements

The general provisions serve to define the main concepts of cybercrime based on artificial intelligence, the scope of AI-based cybercrime, and other matters in the field of artificial intelligence that still require clearer definition to avoid contradictions in understanding artificial intelligence and this law.

2. Principles of AI Usage

The regulation on the principle of using artificial intelligence here also includes the regulation on certification of AI technology for developers or system developers. In addition, the regulation on legal responsibility for misuse and crimes with artificial intelligence must also be made. The goal is to ensure that the artificial intelligence system created by the developer can run well, is safe to use, and can minimize the possibility of being used to commit crimes.

3. Supervision of Artificial Intelligence Technology

Supervision of the development and use of artificial intelligence must be carried out by forming a special institution tasked with conducting periodic audits in order to ensure that the artificial intelligence created can be run properly and in accordance with legal ethics and legal norms created. The existence of a supervisory institution is also important to provide protection for the personal data of users of systems, applications, or devices that use artificial intelligence, as well as evaluation of the security risks of artificial intelligence.

4. Details of Types of AI-Based Cybercrime

The Law on the Use and Supervision of Artificial Intelligence needs to clearly detail the types of cybercrimes based on artificial intelligence, such as the creation of deepfakes in the form of fraudulent crimes or the creation of malware by utilizing AI, and so on.

[25]Nur Aliya. R, Muhammad Aksay, Muhammad Firdaus. A. "The Urgency of Making Regulations on the Use of AI (Artificial Intelligence) in Indonesia". Indonesian Law Enforcement Journal (JPHI). Vol. 5, No. 1, p. 48.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

5. Sanctions or Punishments for Parties Who Abuse AI

As an instrument of criminal law, of course the Law on the Use and Supervision of Artificial Intelligence must also regulate the types of punishments and sanctions given to parties who misuse artificial intelligence to commit cybercrimes and other crimes.

6. Prevention and Handling of Cyber Crime

In the field of prevention and handling of cybercrime based on artificial intelligence, clear regulations are needed regarding the responsibilities of companies providing artificial intelligence services in the event of misuse or failure to secure the products they make.

7. Digital Literacy and Education

It is necessary to conduct education, training, or campaigns on the use of artificial intelligence in everyday life. Not only that, education also needs to be conveyed about the misuse of artificial intelligence and its handling so that the public does not become perpetrators or victims of increasingly rampant artificial intelligence-based cybercrime.

The Indonesian government must act proactively and strategically in facing this threat. The first step is to increase the digital literacy capacity of the community. Educational campaigns about the risks of AI technology and how to recognize cyber threats must be carried out widely to strengthen the community's resilience to attacks. Furthermore, the government needs to strengthen the national cybersecurity infrastructure. The establishment of a special command center that utilizes AI technology to detect and respond to threats in real time is an urgent need. Collaboration with the private sector and technology experts is also needed to ensure comprehensive cyber defense.

A good legal framework to combat AI-based cybercrime should cover three main aspects: preventive regulation, effective law enforcement, and protection of people’s rights. First, preventive regulation should include obligations for AI developers to ensure their technology is not misused. For example, governments could adopt the European Union’s approach of requiring risk audits before AI is launched on the market. These rules could include provisions on algorithm transparency, security testing, and incident reporting obligations.

Second, the legal framework must provide clear authority to law enforcement agencies to deal with AI-based cybercrime. This includes specific training for law enforcement officers to understand AI technology, as well as providing adequate tools and technology to investigate cybercrime cases. Finally, the legal framework must ensure the protection of human rights, including privacy and freedom of information. Regulation must be balanced, so as not to create excessive surveillance that could violate people's rights.

Reconstruction and renewal of criminal law governing cybercrime using artificial intelligence systems as a tool of crime is important. The government must immediately take action to fill the legal vacuum on artificial intelligence that is currently occurring. If the legal vacuum on combating cybercrime using Artificial Intelligence is allowed to continue, what is feared is that law enforcement against similar cases cannot be carried out properly.

The legal update governing artificial intelligence in Indonesia is carried out so that the national legal system is more responsive in facing the development of technology, society, and crime modes that are always evolving at all times. In addition, the presence of laws and

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

regulations governing the use and supervision of artificial intelligence in Indonesia will create a legal framework that is fairer, more beneficial, and more relevant to the needs of society today and in the future.

The risk of increasing and developing AI-based cybercrime in the future must be balanced with active government efforts in forming policies that regulate these issues. Not only the government, law enforcement officers are also required to continue to upgrade the development of existing types of crimes so that crime handling can be carried out properly and fairly. In addition, the community as a legal subject who is vulnerable to becoming a perpetrator or victim must also understand how to utilize artificial intelligence properly and understand how legal norms in the utilization of artificial intelligence are in order to avoid the risk of misuse of artificial intelligence either as a victim or as a perpetrator of the crime.

4. Conclusion

Based on the research results, the following conclusions can be drawn: 1. The criminal law policy in Indonesia's positive law is currently not fully able to accommodate the complexity and development of cybercrime involving Artificial Intelligence (AI) technology. Although several provisions in the Criminal Code and the ITE Law have regulated the types of cybercrime in general, there are no regulations that specifically and comprehensively regulate the role and impact of the use of AI in digital crime. The absence of explicit regulations regarding AI as a tool or subject that contributes to cybercrime creates a legal vacuum that can weaken law enforcement efforts and protection of the community. 2. In future positive law, a criminal law policy is needed that explicitly regulates the form, accountability, and criminal sanctions for crimes involving AI technology, both as a tool and as a perpetrator through an automation system. In addition, it is also important to strengthen the capacity of law enforcement officers, clarify ethical standards for the use of AI, and build a legal framework that is able to anticipate the risks and social impacts of irresponsible use of AI.

5. References

Journals:

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber crime dalam sudut pandang hukum pidana. Jurnal Kewarganegaraan, 6(1), hlm.2173.

Amalia, D. A. R., et al. (2021). Kebijakan hukum pidana dalam upaya penanggulangan cyber terorism. Jurnal Nama, 3(2), 232.

Bibit Santoso, “Menata Kebijakan Publik Yang Tepat Agar Tidak Terjadi Gejolak Di Masyarakat Bila Diundangkan” vol.13, no.1, hlm.39.

Budianto, Rafi Septia, dan Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." Binamulia Hukum, vol. 12, no. 2, 2023, hlm.292

Febri Jaya dan Wilton Goh, “Analisis Yuridis Terdahap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia”, Jurnal Supremasi Hukum, Edisi Vol. 17 No.02, Juli 2021, hlm. 2

Intan Permata Sari, et.al. “Analisis Kebijakan Cyber Crime dalam Hukum Positif di Indonesia”. Journal of Law and Nation (JOLN). Vol. 3, No. 2. Mei 2024, hlm. 396.

Izil Hidayat Putra, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan", vol.1, no.2, hlm.112

Livingstone, S., Helsper, E.J. "Gradations in Digital Inclusion: Children, Young People, and the Digital Devide". New Media & Society. Vol. 9, No. 4, hlm. 671-696.

Mahrina, Joko Sasmito, Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", Jurnal Pena Justisia: Media Komunikasi dan Kajian Hukum, Vol. 21, No. 2, December 2022, hlm. 345.

Marsella, dkk, "Analisis Implementasi Artificial Intelligence Untuk Bisnis: Supanto, dkk "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016", vol.9, no.2, hlm.132

Miftakhur Rokhman Habibi, Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangan dalam Sistem Hukum Indonesia". Jurnal Al-Qanun: Pemikiran dan Pembaharuan Hukum Islam. Vol. 23, No.2. Desember 2020. Hlm. 407.

Ni Made Yordha Ayu Astiti. "Strict Llliability of Artificial Intelegence: Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban". Jurnal Magister Hukum Udayana. Vol. 12, No. 4, Desember 2023, hlm. 969.

Nugroho, H.T. Wahyuni. "Tantangan Regulasi Kejahatan Siber di Indonesia: Perspektif Perkembangan Teknologi Kecerdasan Buatan". Jurnal Hukum dan Teknologi. Vol. 7, No. 2, hlm. 129.

Nur Aliya. R, Muhammad Aksay, Muhammad Firdaus. A. "Urgensi Pembuatan Regulasi Penggunaan AI (Artificial Intelegence) di Indonesia". Jurnal Penegakan Hukum Indonesia (JPHI). Vol. 5, No. 1, hlm. 48.

Yosua Hia. "Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)". Jurnal SELISIK. Vol. 10, No. 1, Juni 2024, hlm. 158.

Smith, J. "AI and Fraud: The Rise of Deepfake Scams". Cybersecurity Review. Vol. 15, No. 3, hlm. 45-50.

Supanto, dkk "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016", Vol.9, No.2, Hlm.132

Systematic Literature Review", vol.4, no.2, hlm.134

Tri Wahyudi, "Studi Kasus Pengembangan dan Penggunaan Artificial Intelligence (AI) Sebagai Penunjang Kegiatan Masyarakat Indonesia", vol.9, no.1, hlm.29

Kasim, Z. (2023). Kebijakan hukum pidana untuk penanggulangan cyber crime di Indonesia. Jurnal Nama, 2(1), 20.

Books:

Brenner, S. W. 2010. Cybercrime: Criminal threats from cyberspace. Praeger.

A. S.T. Kansil, 1989, Pengantar Ilmu Hukum dan Tata Hukum Indonesia, Jakarta: Balai Pustaka.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Casey, E. 2011. "Digital Evidence and Computer Crime: Forensic Science, Computers, and The Internet (3rd edision)". Academic Press.

Kaharuddin, & Haq, Z. A. (2024). Kecerdasan buatan dan aspek perlindungan hukum di era digitalisasi. Prenada Media.

Moeljatno. 2002. Asas-asas Hukum Pidana. Jakarta: PT Rineka Cipta.

Philipus M. Hadjon. 2007. Perlindungan Hukum bagi Rakyat Indonesia: Sebuah Studi tentan Prinsip-Prinsipnya, Penanganannya oleh Peradilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara. Surabaya: Peradaban.

Satjipto Rahardjo. 2000. Hukum dan Perubahan Sosial: Suatu Tinjauan Teoritis serta Pengalaman-Pengalaman di Indonesia. Jakarta: Genta Publishing.

Sutan Remy Sjahdeini. Kejahatan Siber: Cybercrime. Jakarta: Pustaka Utama Grafiti, 2003, hlm. 12-15.

Wall, D. S. 2007. Cybercrime: The transformation of crime in the information age. Polity Press.

Regulation:

ITE Law Number 1 of 2024, an amendment to ITE Law No. 11 of 2008

Article 1 paragraph (3) of the 1945 Constitution

Law Number 6 of 2023 amending Law Number 36 of 1999 concerning Telecommunications

Law Number 28 of 2014 amending Law Number 19 of 2002 concerning Copyright

Law Number 5 of 2018 amending Law Number 15 of 2003 concerning the Eradication of Terrorism

Criminal Code (KUHP)

Article 335 paragraph (1) of the Criminal Code concerning Unpleasant Acts

Article 362 of the Criminal Code concerning Theft

Article 378 of the Criminal Code concerning Fraud

Internet:

Ahmad Sudi Pratikno, "Implementation of Artificial Intelligence in Mapping Characteristics, Competencies, and Psychological Development of Elementary School Students Through Offline Platforms", available inhttps://scholar.google.co.id/citations?view_op=view_citation&hl=id&user=-FbwaL4AAAAJ&citation_for_view=-FbwaL4AAAAJ:d1gkVwhDpl0C

European Commission. Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu.

Giovani Dio Prasasti, "Deputy Minister of Communication and Information: 22.1 Percent of Workers in Indonesia Have Started Using AI",https://www.liputan6.com/tekno/read/5467690/wamenkominfo-221-persen-pekerja-diindonesia-sudah-mulai-pakai-ai?page=2.

Online Law, Measuring the Prospects of Artificial Intelligence Regulation in Indonesia

https://www.hukumonline.com/berita/a/menakar-prospek-pengaturan-artificial-intelligence-diindonesia/.

Kaplan, A. M., & Haenlein, M. (2019). Siri, Siri in my hand, who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15-

US Congress. Algorithmic Accountability Act of 2019.https://www.congress.gov.