Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime

Muh. Fadli Faisal Rasyid
Faculty of Law, Andi Sapada Institute of Social Sciences and Business, Parepare, Indonesia
fadlifaisal643@gmail.com

Muh. Akhdharisa SJ
Faculty of Law, Muhammadiyah Sorong University, Papua, Indonesia
makhdharisa@gmail.com

Karlin Z. Mamu
Faculty of Law, Gorontalo State University, Gorontalo, Indonesia
karlin@ung.ac.id

Saptaning Ruju Paminto
Faculty of Law, Suryakancana University, Cianjur, Indonesia
saptaning@elemen.ac.id

Wahab Aznul Hidaya
Faculty of Law, Muhammadiyah Sorong University, Papua, Indonesia
wahabaznulhidaya@um-sorong.ac.id

Abdennour Hamadi
Faculty of Law, Sohar university, Sohar, Oman
ahammadi@su.edu.om

Abstract: This study examines the legal implications of artificial intelligence (AI) integration in cybercrime, focusing on the responsibilities of offenders. Through a normative analysis of relevant laws and regulations, the research reveals the challenges AI poses to law enforcement and regulatory frameworks. The findings underscore the urgent need for tailored legislation to address vulnerabilities exploited by AI-driven cybercriminals and enhance international cooperation to combat cross-border cybercrime. In conclusion, understanding and addressing the legal ramifications of AI in cybercrime are crucial. AI equips perpetrators with sophisticated tools, complicating detection and prosecution efforts. Targeted legislation is essential to close loopholes and empower law enforcement. Enhanced international collaboration is also vital to effectively address the transnational nature of cybercrime. By implementing precise legal frameworks and fostering international cooperation, policymakers and law enforcement agencies can strengthen their capacity to prevent, investigate, and prosecute AI-enabled cybercrimes, safeguarding individuals, businesses, and societies from escalating threats

Keywords: Artificial Intelligence, Cybercrime, Legal Implications

Abstrak: Studi ini menguji implikasi hukum dari integrasi kecerdasan buatan (AI) dalam kejahatan dunia maya, dengan fokus pada tanggung jawab para pelaku. Melalui analisis normatif terhadap hukum dan regulasi yang relevan, penelitian ini mengungkap tantangan yang dihadapi oleh penegakan hukum dan kerangka regulasi terkait. Temuan ini menekankan perlunya legislasi yang disesuaikan untuk mengatasi kerentanan yang dieksploitasi oleh para pelaku kejahatan dunia maya yang didukung oleh AI dan meningkatkan kerjasama internasional untuk melawan kejahatan dunia maya lintas batas. Sebagai kesimpulan, memahami dan mengatasi dampak hukum dari penggunaan AI dalam kejahatan dunia maya sangat penting. AI memberikan alat yang canggih kepada pelaku kejahatan, yang mempersulit upaya deteksi dan penuntutan. Legislasi yang ditargetkan penting untuk menutup celah hukum dan memberdayakan penegakan hukum. Kerjasama internasional yang ditingkatkan juga vital untuk mengatasi sifat lintas batas kejahatan dunia maya. Dengan menerapkan kerangka hukum yang tepat dan memperkuat kerjasama internasional, para pembuat kebijakan dan penegak hukum dapat memperkuat kapasitas mereka untuk mencegah, menyelidiki, dan menuntut kejahatan dunia maya yang didukung oleh AI, melindungi individu, bisnis, dan masyarakat dari ancaman yang semakin meningkat.

Keywords: *Kecerdasan Buatan, Kejahatan Cyber, Implikasi Hukum*

Introduction

Artificial intelligence (AI) has ushered in new possibilities across various aspects of life in the increasingly sophisticated digital age. However, it has also facilitated the perpetration of misuse and criminal activities.[1] Cybercrime stands out as one of the sectors significantly affected, with the increasing utilization of Artificial Intelligence as a tool for illicit activities. Investigating the types of cybercrimes employing AI and the associated criminal penalties is crucial in addressing this issue.[2]

Computational Intelligence refers to machines capable of performing tasks traditionally associated with human intelligence when operated by individuals. Advanced artificial intelligence, for instance, can oversee production machinery in industrial settings.[3] Moreover, it demonstrates the ability to recognize faces, comprehend human language commands, and navigate vehicles such as Tesla's self-driving cars, which have become increasingly prevalent. Additionally, AI powers recommendation systems like those found in YouTube, Netflix, and Siri. These systems engage in a spectrum of activities akin to human intelligence, including planning, learning, reasoning, problem-solving, motor control, manipulation, social interaction, and even creativity.[4]

The utilization of computer resources connected to the internet, coupled with the exploitation of other internet-connected computers, constitutes cybercrime. Hackers, crackers, and script kiddies often exploit security vulnerabilities in operating systems to gain unauthorized access to computers.[5] Many applications embedded in electronic devices require user data to deliver various services, particularly during the account registration process, which is essential for utilizing the application. The intended use of this data can vary based on the vendor's policies.[6]

Cybercrime encompasses two distinct meanings. Broadly, it refers to illegal activities involving computer systems and networks, where individuals unlawfully exploit these technologies.[7] Narrowly, it specifically denotes computer crime, where individuals illicitly breach or attack computer security systems and data, often employing separate computer systems for such activities.[8] The contemporary era of technological advancement has brought forth numerous enhancements that streamline human operations. One notable advancement is the integration of Artificial Intelligence (AI), facilitating task automation

[1] J. Rocco Blais and Adam M. Jungdahl, "Artificial Intelligence in a Human Intelligence World," American Intelligence Journal 36, no. 1 (2019): 108–13.

[2] Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, Artificial Intelligence and the Future of Defense: Strategic Implications For Small- and Medium-Sized Force Providers (The Hague Center for Strategic Studies, 2017).

[3] Pandega Abyan Zumarsyah, 'Sejarah Kecerdasan Buatan Atau Artificial Intelligence (AI)', Www.Warstek.Com, 2021.

[4] Hari Sutra Disemadi, "The Urgency of Special Regulations and the Use of Artificial Intelligence in Realizing Personal Data Protection in Indonesia," Journal of Juridical Insights 5, no. 2 (28 September 2021): 177–99, https://doi.org/10.25072/jwy.v5i2.460.

[5] Dista Amalia Arifah, "Cybercrime cases in Indonesia,"

Journal of Business and Economics 18, no. 2 (2011), https://www.unisbank.ac.id/ojs/index.php/fe3/article/download/2099/767.

[6] Fenty Usmanpuluhulawa, Jufryantopuluhulawa, and Moh Gufran Katili, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era," Jambura Law Review 2, no. 2 (20 June 2020): 182–200, https://doi.org/10.33756/jlr.v2i2.6847.

[7] Miranda Bruce and others, 'Mapping the Global Geography of Cybercrime with the World Cybercrime Index', PLoS ONE, 19.4 April (2024), doi:10.1371/journal.pone.0297312.

[8] Salomon AM Babys, "The Threat of Cyber War in the Digital Era and Indonesian National Security Solutions," Oratio Directa (Communication Science Study Program) 3, no. 1 (2021), http://ejurnal.ubk.ac.id/index.php/oratio/article/view/163.

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

across various computer software. AI possesses the capability to analyze data and make decisions based on the information it processes. [9] In the realm of information processing automation, the characteristics of Artificial Intelligence align with the concept of an Electronic Agent as defined by Indonesian legislation.

Artificial Intelligence presents governments with a plethora of advantageous technologies, encompassing advanced surveillance software, face recognition technology, and speech recognition systems. Regulations are imperative to govern the utilization of AI technologies, particularly those employing Deepfake algorithms, within the realm of personal data protection. [10] Deepfake technology has garnered considerable attention due to its involvement in the creation of explicit videos featuring celebrities, dissemination of fake news, perpetration of hoaxes, and facilitation of financial fraud. Consequently, both businesses and governments are compelled to respond by devising methods to identify and curb its usage. Deepfake technology utilizes facial data, which constitutes personal information, thereby posing risks of abuse, including the propagation of propaganda, creation of illicit content such as pornography, identity theft, and various privacy concerns.[11]

In a study titled 'The Malicious Use of Artificial Intelligence: Predicting, Preventing, and Mitigating,' published in February 2018, a group of 26 researchers from 14 institutions across various sectors identified numerous imminent risks associated with Artificial Intelligence (AI) within a timeframe of less than five years. The paper detailed how AI could jeopardize digital security, especially through the deployment of AI systems trained to carry out criminal activities such as hacking or social engineering against specific targets, thereby compromising privacy.

An example highlighted in the study is the Chinese government's utilization of face recognition technology to surveil its population, monitoring their movements in workplaces, schools, and other public areas. Such extensive surveillance practices raise concerns about potential misuse and the commission of offenses like disseminating propaganda, creating illicit content such as pornography, committing identity theft, or violating individuals' privacy.

Additionally, a chart depicting the distribution of cybercrime data across multiple countries is provided
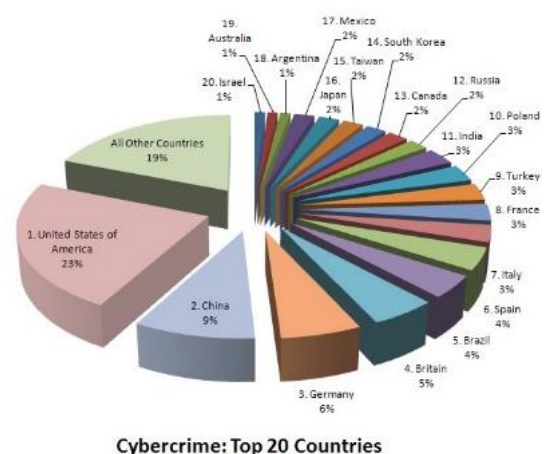
Chart 1. Cybercrime in Top 20 Countries

Figure 1. distribution of cybercrime

---

[9] Nurul Qamar, Human Rights in a Democratic Law State (Human Rights in Democratiche Rechtsstaat) (Makassar: SInar Graphics, 2013).

[10] Ragini Mokkapati and Venkata Lakshmi Dasari, 'An Artificial Intelligence Enabled Self Replication System Against Cyber Attacks', in *Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023*, 2023, pp. 698 – 703,

doi:10.1109/ICSSIT55814.2023.10061089.

[11] Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspects of International Law in the Use of Deepfake Technology for Personal Data Protection," Uti Possidetis: Journal of International Law 2, no. 1 (18 March 2021): 31–57, https://doi.org/10.22437/up.v2i1.11093.

The figure 1 indicates that the largest cybercrime rate is in the United States. Various types of cybercrime that occur in the world are as explained in the following chart:
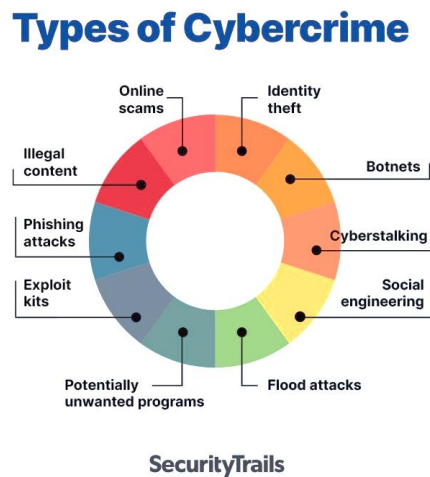
Types of Cybercrime

Figure 2. Types of Cybercrime

Figure 2 various types of cybercrime that occur in the world. Here's a table outlining specific manifestations of cybercrime involving artificial intelligence, along with the legal consequences:

table 1. cybercrimes involving artificial intelligence

Type of Cybercrime	Description	Legal Consequences
Fraud using AI voice	Criminals utilize artificial intelligence to imitate voices, impersonating individuals	Prosecution for fraud, potential imprisonment
Job application deepfake	Job applicants use manipulated videos, images, or recordings to impersonate others	Identity theft charges, potential legal action by victims
Fake video calls	Perpetrators use deepfake technology to make fake video calls impersonating officials	Fraud charges, potential legal action by authorities
Manipulated media	Individuals manipulate photos and videos to defame or harass others, such as in the cheerleading case	Charges of defamation, potential civil lawsuits

Table 1 highlights various types of cybercrimes involving artificial intelligence (AI) and their legal consequences. This table illustrates the increasing sophistication of cybercrimes through the use of AI, posing

significant challenges for legal systems worldwide in addressing and mitigating these crimes. In Indonesia's context, a noteworthy issue concerning artificial intelligence involves the defacement of the official website of the National Malware Center, specifically the internet address www.pusmanas.bssn.go.id. This incident, reported recently, affected the Twitter handle @son1x777. The website was compromised by the Mxonday hacking group on Wednesday, October 20, 2021. Currently, the BSSN Computer Security Incident Response Team is managing the site, given its inclusion of information related to malware repositories.

The compromised website serves as a repository for managing and researching information regarding malware. Although the hacking incident did not lead to any disruption in public services, effective mitigation efforts by the BSSN ensured the safeguarding of data related to public services on the sub-web pusmanas.bssn.go.id. Investigations indicate that the perpetrator is likely from Brazil. However, further scrutiny is underway as anyone in the digital realm can claim responsibility. According to cybersecurity expert Pratama Persadha, the individual responsible for the defacement conducted this attack as retaliation against a suspected Indonesian hacker who had previously targeted a Brazilian governmental website.

Pratama further explained that website defacement involves unauthorized access to a website and altering its appearance. These alterations can affect specific parts or the entirety of the webpage. For example, hackers can modify the website's style, insert intrusive advertisements, or alter the content. They may also engage in more

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

serious actions, such as stealing data.[12] In terms of application efficiency, Artificial Intelligence (AI) is increasingly prevalent worldwide, with many countries already integrating it into various sectors.[13] In the industrial sector alone, AI adoption has reached up to 56%.[14] To harness the potential of AI in Indonesia, the National Research and Innovation Agency (BRIN) released the National Artificial Intelligence Strategy for Indonesia 2020–2045. This strategy aims to guide the utilization of AI within the country.

The challenges posed by artificial intelligence (AI) today are complex and multifaceted, encompassing cyber security risks as well as ethical and societal implications. The recent defacement incident on the National Malware Centre website underscores the vulnerability of even systems designed to defend against cyber threats. This event highlights the critical importance of cyber security and the necessity for proactive measures to protect digital infrastructure.

The Pusmanas defacement case emphasizes the imperative of global collaboration in combating cybercrime, as perpetrators can operate from any jurisdiction. Strengthening threat detection and response capabilities requires cooperation and information sharing among cybersecurity organizations across different nations.

On the other hand, the widespread application of AI across various industrial sectors holds great promise for enhancing productivity and driving innovation. However, the deployment of AI must be accompanied by careful consideration of ethical concerns such as data privacy, algorithmic bias, and the impact on the workforce. Therefore, the implementation of a national policy, such as the one formulated by the Indonesian National Research and Innovation Agency (BRIN), is essential to ensure the responsible and sustainable use of AI.

The research challenge posed is: "What are the specific forms of cybercrime that leverage artificial intelligence?" Additionally, what are the legal repercussions for engaging in cybercrime involving the use of artificial intelligence?

Literature Review
The Essence of Cybercrime:

The rapid development of information technology, particularly internet services and electronic media, has significantly transformed human civilization. However, alongside these advancements, there have been negative impacts, leading to crimes and violations collectively termed cybercrime—an evolution of traditional computer crime.[15]

In Indonesia's criminal law system, there is no explicit definition of cybercrime outlined in the legislation.[16] Instead, the focus is on criminal acts related to

---

[12] Agus Tri Haryanto, "BSSN Admits Its Official Website Has Been Hacked," detikinet, accessed March 31 2024, https://inet.detik.com/security/d-5782090/bssn-akui- situs-resmi-him-diretas.

[13] Asma Abdulaziz Abdullah Abalkhail and Sumiah Mashraf Abdullah Al Amri, 'Saudi Arabia's Management of the Hajj Season through Artificial Intelligence and Sustainability', *Sustainability (Switzerland)*, 14.21 (2022), doi:10.3390/su142114142.

[14] Kirana Rukmayuninda Ririh et al., "COMPARATION STUDY AND SWOT ANALYSIS ON THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN INDONESIA," J@ti Undip: Journal of Industrial Engineering 15, no. 2 (7 June 2020): 122–33,

https://doi.org/10.14710/jati.15.2.122-133.

[15] Vishalkumar Ravindrakumar Gajjar and Hamed Taherdoost, 'Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies', in *Proceedings - 2024 5th International Conference on Mobile Computing and Sustainable Informatics, ICMCSI 2024*, 2024, pp. 668 – 676, doi:10.1109/ICMCSI61536.2024.00105.

[16] Surya Eko Prasetya, Hasnah Faiza, and Mangatur Sinaga, 'Verbal Violence in Comments of Supporting Candidates Presidential Elections 2019 in Instagram Based on ITE Law', *International Journal of Scientific and Technology Research*, 9.3 (2020).

information technology and electronic transactions as defined in the ITE Law. [17] Cybercrime encompasses various activities, ranging from unauthorized access to computer systems to data theft and malicious vandalism.

Cybercrime poses a significant threat to the stability of Indonesian society, challenging the government's ability to combat crimes committed through computer technology, especially over the internet and intranet networks. As technology evolves rapidly, so does cybercrime, with perpetrators exploiting cyberspace for illicit activities.[18]

The principle of legality, a fundamental aspect of criminal law, dictates that individuals cannot be punished for actions not expressly prohibited by law. Cybercrimes, particularly those conducted through social media, differ from traditional offenses and can have a profound impact on victims due to their widespread reach and lasting consequences.[19]

Deepfakes in Indonesia and The Regulations Against Them

Deepfake technology, while having constructive applications in fields like filmmaking and virtual reality, also poses significant negative impacts, such as political manipulation, pornography, and social engineering attacks. In Indonesia, instances of deepfake-related incidents include the creation of fake social media accounts supporting controversial causes and the use of deepfakes in sextortion schemes.[20]

The rise of deepfake cases globally and in Indonesia underscores the need for preventive measures and robust law enforcement against such actions. While some states in the US have enacted regulations targeting deepfake-related crimes, Indonesia has yet to specifically regulate offenses involving deepfake technology.[21]

Existing Indonesian laws, particularly the Electronic Information and Transactions Law (UU ITE) and the Pornography Law, can be applied to combat deepfake-related offenses. However, there is a need for more specific legislation to address the unique challenges posed by deepfakes.[22]

Regulations in Indonesia could mirror those enacted in states like Virginia, California, and New York, which criminalize the distribution of pornographic deepfakes and provide legal protections against their dissemination.[23]

Consideration should be given to formulating legislation explicitly targeting deepfakes, similar to the Malicious Deep Fake Prohibition Act proposed in the United States. Such regulations could impose penalties for the creation and dissemination of deepfake content, with provisions for

[17] Nur Qalbi and Putri Ramadhani, 'Urgensi Undang-Undang ITE Di Era Globalisasi', *Jurnal Litigasi Amsir*, 9.2021 (2022).

[18] Rr Dijan Widijowati, 'Analysis of the Development of Cyber Crime in Indonesia', *International Journal Of Artificial Intelegence Research*, 6.1 (2022).

[19] Ach. Tahir, 'Penegakan Hukum Cyber Crime Di Indonesia', *Sasi*, Vol 27.I (2021).

[20] Isnaini Imroatus and others, 'Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia', *International Journal of Multicultural and Multireligious Understanding*, 2023.

[21] Muhammad Ilman Abidin, 'Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography', *MIMBAR : Jurnal Sosial Dan Pembangunan*, 2023, doi:10.29313/mimbar.v39i2.2965.

[22] Muhammad Faqih and Enni Soerjati Priowirjanto, 'Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia', *Jurnal Indonesia Sosial Teknologi*, 3.11 (2022), doi:10.36418/jist.v3i11.528.

[23] Asri Gresmelian Eurike Hailtik and Wiwik Afifah, 'Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia', *Asian Journal of Social and Humanities*, 2.4 (2024), doi:10.59888/ajosh.v2i4.222.

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

content moderation obligations on media companies[24]

Methods

This study employs a normative approach, specifically examining rules and legal documents pertaining to the use of Artificial Intelligence (AI) in the realm of cybercrime. The methodology involves a comprehensive examination of documents, gathering and scrutinizing secondary material obtained from pertinent legal sources. Data sources include the constitution, the Criminal Code, the Criminal Procedure Code, the Electronic Information and Transactions Law (UU ITE) and its subsequent revisions, as well as laws and regulations published by the Ministry of Communication and Information and other government regulations pertaining to electronic systems and transactions.[25]

The study employs a conceptual framework to comprehend and examine the principles included in legal regulations and relevant legal theories, with particular attention to the legal consequences arising from the use of AI in cybercriminal activities. The investigation delineates and contrasts existing legal standards to understand how contemporary legislation addresses and governs the utilization of AI in cybercrime.

This study uses qualitative analytic techniques to interpret data in a narrative format, aiming to construct a cohesive and thorough comprehension of the relevant legal framework and its possible evolution in the future. This research offers valuable insights into the legal ramifications associated with the utilization of AI in cybercrime and presents recommendations

on how legal frameworks can be developed to better regulate and address the emerging challenges posed by AI technology in the realm of cybercrime.

Results and Discussion
Cyber Crime Crimes That Utilize Artificial Intelligence as a Medium for Committing Crimes

There is a distinction between the terminologies and meanings of computer crime and cybercrime. One perspective considers them indistinguishable, while another distinguishes them based on the method and medium used. The US Department of Justice defines computer crime as any unlawful act that necessitates understanding of computer technology for its execution, investigation, or legal proceedings. The Organisation of European Community Development describes data misuse as any unlawful, immoral, or unauthorized action related to the automated processing and/or transfer of data.

According to Andi Hamzah, computer-related crime may be broadly defined as the unlawful use of computers. It involves illegal acts utilizing a computer either as a tool or as the target, with or without the intention of making a profit, while causing harm to individuals or entities. Computer crime generally refers to any illegal activity involving advanced computer systems. In contrast, cybercrime encompasses unethical, illegal, or unauthorized conduct involving the processing or transmission of data, typically performed using computer devices or digital methods in cyberspace.[26]

---

[24] Sayid Muhammad Rifki Noval, 'Indonesia Readiness to Face Social Engineering Attacks with Deepfake Technology', *Journal of Law and Sustainable Development*, 11.12 (2023), doi:10.55908/sdgs.v11i12.727.

[25] Abdurrakhman Alhakim and Sofia Sofia, 'KAJIAN NORMATIF PENANGANAN CYBER CRIME DI SEKTOR PERBANKAN DI INDONESIA', *Jurnal Komunitas Yustisia*, 4.2 (2021), doi:10.23887/jatayu.v4i2.38089.
[26] Andi Hamzah, 'Pidana Dan Pemidanaan Indonesia',

Nazura Abdul Manap differentiates between computer crime and cybercrime based on the mode and media used. Computer crime covers a wide scope of violations where a computer is used as a tool, requiring a direct connection between the criminal and the computer. Examples include bank employees illicitly transferring funds or hackers gaining unauthorized access to download data. Cybercrime, however, refers to criminal activities carried out using the internet or other virtual platforms, often extending beyond national borders.[27]

The integration of computer technology with cyberspace (the internet) has led to passive business expansion and global trade rivalry, optimizing internet media for business transactions and e-commerce. However, this digital expansion also fosters novel forms of economic and business-related criminal activities.

Tubagus Ronny Rahman Nitibaskara argues that applying existing legal provisions to cybercrime cases significantly differs from conventional law enforcement practices, emphasizing the need for technical expertise in information technology. Soerjono Soekanto outlines four factors influencing law enforcement: rules, institutions to enforce the rules, facilities supporting implementation, and legal awareness among affected individuals.

The evolution of computer crime and cybercrime has demonstrated a linear progression with advancements in computer technology. Initially limited to physical world crimes, these activities have extended to virtual realms, including internet-based fraud and threats. Cybercrime utilizes modern information technology, requiring perpetrators to have expertise and stay updated on IT advancements, distinguishing it from traditional crimes.

The rise of e-commerce has expanded the scope of cyber-enabled business crimes. Originally focused on retail, e-commerce now includes financial services and insurance sectors, conducting transactions and inquiries online. Despite the absence of a universally accepted definition, e-commerce has become one of the most rapidly expanding activities in cyberspace.

Artificial Intelligence (AI) systems, increasingly prevalent in the economy and society, lack regulatory oversight, rendering them susceptible to exploitation for criminal activities. The absence of specific regulations pertaining to AI in Indonesia highlights the need for immediate government intervention to impose regulations and oversight.

AI offers numerous benefits, including applications in healthcare, environmental preservation, and resource optimization. However, it also presents threats, such as the potential misuse of autonomous weapons and ethical concerns in various sectors. The European Commission's AI Act and other regulatory measures aim to address these issues, emphasizing the importance of governing the ethical and unethical applications of AI.[28]

AI's profound influence on human existence necessitates comprehensive legal frameworks to address its potential misuse. The current lack of national laws on AI's legal personality, competence, or responsibility places the burden of proof on the AI's owner,

Jakarta: Sinar Grafika, 1993.

[27] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, and Hossein Taji, 'Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime', *Computer Law and Security Review*, 29.3 (2013), doi:10.1016/j.clsr.2013.03.011.

[28] Dipo Dunsin and others, 'A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response', *Forensic Science International: Digital Investigation*, 48 (2024), doi:10.1016/j.fsidi.2023.301675.

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

creator, or operator in unlawful occurrences. This approach limits AI's advancement, restricting its use to human accessory functions. However, AI's potential for malicious use underscores the urgent need for clear regulations to harness its benefits while mitigating risks.

Criminal Accountability for Cyber Crime that Utilizes Artificial Intelligence

Two fundamental aspects common to all legal themes are legal acts and the associated power to act, encompassing rights and duties. Legal acts serve as a foundational element in legal discourse. In the context of Artificial Intelligence (AI), the process involves simulating human intelligence and subsequently embedding it into machines, enabling them to emulate human thought processes and behaviors.[29]

Taking legal entities as artificial legal subjects capable of performing human-like activities, we can categorize simulation and duplication as forms of artificial action. When discussing authority, it's essential to examine it comprehensively, considering its origin as an independent matter.

The process of attaining authoritative status is closely linked to this context. It relies on pertinent rules and regulations as benchmarks for defining the rights and responsibilities of legal entities. [30] In the absence of specific laws addressing the rights and duties of AI, it's feasible to assess AI's rights and responsibilities through a comparable interpretive approach. There's a potential trajectory for AI's future formalization as a distinct legal entity,

considering its classification as a synthetic legal subject.[31]

When discussing the repercussions of AI subjects breaking the law, we must consider the theory of legal actions. According to this theory, the law governs the consequences of lawbreaking, as they reflect the intentions of lawmakers. Statements of will give rise to new legal acts by elevating the actor's will to the core of the act. Legal actions typically fall into two categories: unilateral and two-party. Unilateral actions involve one party engaging in a legally binding activity enforceable only by that individual. Conversely, two-party legal acts entail both parties assuming rights and responsibilities. In essence, AI, as a legal entity, akin to a human, operates under the employment of its owner. Thus, the owner, acting as the employer, may bear responsibility if AI commits a crime.[32]

On the contrary, Indonesia currently lacks specific laws addressing the protection of personal data. As highlighted by a 2016 analysis conducted by the Institute for Community Studies and Advocacy (ELSAM), Indonesia has thirty distinct statutes related to personal safety. These statutes cover various sectors such as health, population administration, banking, and financial services, indicating a comprehensive legal framework governing personal safety across different domains.[33]

Ensuring absolute clarity in the law is crucial for every rule of law system. With the rapid advancements in technology, various forms of technical crime, including cybercrime, have proliferated. Despite this, detailed regulations for safeguarding private

---

[29] Febri Jaya and Wilton Goh, "JURIDICAL ANALYSIS OF THE POSITION OF ARTIFICIAL INTELLIGENCE AS A LEGAL SUBJECT IN INDONESIAN POSITIVE LAW," SUPREMACY OF LAW 17, no. 02 (21 July 2021): 01–11, https://doi.org/10.33592/jsh.v17i2.1287.

[30] Tuti Khairani Harahap et al., "INTRODUCTION TO LEGAL SCIENCE," Tahta Media Publisher, May 30 2023,

https://tahtamedia.co.id/index.php/issj/article/view/255.

[31] Harahap et al.

[32] Embedded, "The Urgency of Special Regulations and the Use of Artificial Intelligence in Realizing Personal Data Protection in Indonesia."

[33] Embedded.

information are notably absent from the Information and Technology Law. However, a new perspective has emerged regarding the protection of electronic data and information, whether public or private.

Government Regulation 82 of 2012 addresses the implementation of electronic systems and transactions, emphasizing the need to describe personal electronic data adequately. Data security within electronic systems is a significant concern under the Information Technology and Telecommunications Law, which mandates measures to prevent unauthorized access, interference, and usage, alongside safeguards provided by system operators. Given the widespread use of personal data across various aspects of life, there is a genuine risk of exploitation, highlighting the necessity for legislation to provide clarity and establish norms for prevention.

While the law appears to be cognizant of these issues, government systems, the legal profession, and legal professionals have been slow to adopt relevant technologies in recent years. However, interest in and progress toward artificial intelligence surged during the 4.0 industrial revolution, driven by the availability of legal data and the necessity for modernizing legal services.

Furthermore, AI is making significant strides in legal education, where students are encouraged to utilize digital resources more extensively. This trend coincides with the proliferation of legal technology organizations, conferences, and enterprises. Additionally, "artificial intelligence law and technology" training and research centers have been established in several American and European law schools. Moreover, the development of robots capable of practicing law (robolawyers) and making judgments in

courtrooms (robojudges) has begun.

While automation is believed to enhance productivity and efficiency compared to human counterparts, there are concerns regarding the impartiality and ethical considerations of AI-driven legal processes. Nevertheless, the integration of AI into the judicial system holds the potential to positively impact various aspects of the legal process.[34]

To comprehensively assess the impact of AI on the legal system, it's imperative to first establish a foundational understanding of AI itself. In today's digital era, individuals interact with the legal system differently due to technological advancements brought about by the 4.0 industrial revolution. While these advancements offer various methods and variants, they are not without their flaws.

One notable limitation of AI is its susceptibility to analytical mistakes, particularly in scenarios that involve complex legal reasoning or nuanced interpretations. Unlike humans, AI lacks the capacity to incorporate emotions and moral considerations into its decision-making processes. Consequently, the human element remains indispensable in the legal field.

Table 2. Ethical Considerations and Challenges in AI Integration into the Legal System

Considerations/Challenges	Description
Bias and fairness	AI algorithms may exhibit biases, leading to unfair outcomes. Ensuring fairness in decision-making is essential.
Transparency and accountability	The opacity of AI decision-making processes raises concerns about accountability and the ability to understand and challenge decisions.
Privacy and data protection	AI systems may require access to sensitive data, raising questions about privacy and data protection regulations.
Legal liability and responsibility	Determining liability when AI systems make errors or

[34] FL Amboro and Khusuf Komarhana, "Prospects for Artificial Intelligence as a Subject of Civil Law in

Indonesia," Law Review 21, no. 2 (2021): 145–72.

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

Considerations/Challenges	Description
	engage in unlawful activities poses legal challenges.
Ethical decision-making and moral reasoning	AI lacks the capacity for ethical reasoning and moral judgment, raising questions about its role in making ethical decisions.
Access to justice and equality	Ensuring equitable access to AI-driven legal services and preventing the exacerbation of existing inequalities are crucial considerations.

Table 2 outlines several ethical considerations and challenges associated with the integration of AI into the legal system. These points emphasize the importance of addressing ethical and practical challenges to ensure that AI integration into the legal system supports justice, fairness, and accountability.

While AI can streamline certain aspects of the law enforcement process and enhance efficiency when utilized effectively, it cannot replace the nuanced judgment, empathy, and ethical considerations that human legal professionals bring to the table. Thus, while AI can augment and optimize certain functions within the legal system, its integration must be approached with caution and a recognition of its limitations. Ultimately, the successful administration of the legal enforcement process relies on a harmonious collaboration between AI technology and human expertise

Conclusion

In conclusion, this study underscores the critical importance of understanding and addressing the legal implications stemming from the utilization of Artificial Intelligence (AI) in the context of cybercrime. AI presents perpetrators with sophisticated tools to engage in illegal activities, complicating efforts to detect, investigate, and prosecute such crimes. The absence of clear legal frameworks governing AI's role in cybercrime, coupled with the transnational nature of many cybercrimes, exacerbates the challenge.

To confront these challenges effectively, it is imperative to develop targeted legislation specifically addressing the use of AI in cybercrime. This legislation should aim to close existing loopholes and provide law enforcement agencies with the necessary tools and authority to combat AI-enabled criminal activities. Additionally, fostering enhanced international cooperation is essential to effectively address cybercrime, which often transcends national borders.

By implementing more precise legal frameworks and strengthening international collaboration, policymakers and law enforcement agencies can bolster their capacity to prevent, investigate, and prosecute cybercrimes involving AI. This proactive approach is crucial in safeguarding individuals, businesses, and societies from the growing threats posed by AI-enabled cybercriminal activities.

References

Abdussamad, Zamroni, dan Mohamad Hidayat Muhtar. "Etika Penggunaan Media Sosial Dalam Promosi Destinasi Wisata Di Desa Patoameme." *Akuntansi Dan Humaniora: Jurnal Pengabdian Masyarakat* 1, no. 2 (30 Juni 2022): 132–39. https://doi.org/10.38142/ahjpm.v1i2.339.

Amboro, F. L., dan Khusuf Komarhana. "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia." *Law Review* 21, no. 2 (2021): 145–72.

Abalkhail, Asma Abdulaziz Abdullah, and Sumiah Mashraf Abdullah Al Amri, 'Saudi Arabia's Management of the Hajj Season through Artificial Intelligence and Sustainability', *Sustainability (Switzerland)*, 14.21 (2022) <https://doi.org/10.3390/su142114142>

Ach. Tahir, 'Penegakan Hukum Cyber Crime Di Indonesia', *Sasi*, Vol 27.I (2021)

Alhakim, Abdurrakhman, and Sofia Sofia, 'KAJIAN NORMATIF PENANGANAN CYBER CRIME DI SEKTOR PERBANKAN DI INDONESIA', *Jurnal Komunitas Yustisia*, 4.2 (2021), doi:10.23887/jatayu.v4i2.38089

Andi Hamzah, 'Pidana Dan Pemidanaan Indonesia', *Jakarta: Sinar Grafika*, 1993

Anggia Dasa Putri, M. Kom. "SISTEM PAKAR MENDETEKSI TINDAK PIDANA CYBERCRIME MENGGUNAKAN METODE FORWARD CHAINING BERBASIS WEB DI KOTA BATAM." *Jurnal Edik Informatika Penelitian Bidang Komputer Sains Dan Pendidikan Informatika* 3, no. 2 (9 Oktober 2017): 197–210. https://doi.org/10.22202/ei.2017.v3i2.2244.

Arief, Supriyadi, Mohamad Hidayat Muhtar, dan Geofani Milthree Saragih. "UPAYA PEMBELAAN DIRI DALAM PERSPEKTIF PERSAMAAN DI HADAPAN HUKUM." *Jurnal Yudisial* 16, no. 1 (24 Desember 2023): 25–47. https://doi.org/10.29123/jy.v16i1.475.

Arifah, Dista Amalia. "Kasus cybercrime di indonesia." *Jurnal Bisnis dan Ekonomi* 18, no. 2 (2011). https://www.unisbank.ac.id/ojs/index.php/fe3/article/download/2099/767.

Babys, Salomon AM. "Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia." *Oratio Directa (Prodi Ilmu Komunikasi)* 3, no. 1 (2021). http://ejurnal.ubk.ac.id/index.php/oratio/article/view/163.

Blais, J. Rocco, dan Adam M. Jungdahl. "Artificial Intelligence in a Human Intelligence World." *American Intelligence Journal* 36, no. 1 (2019): 108–13.

Boddy, Matt. "Phishing 2.0: the new evolution in cybercrime." *Computer Fraud & Security* 2018, no. 11 (Januari 2018): 8–10. https://doi.org/10.1016/S1361-3723(18)30108-8.

Bruce, Miranda, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, and Federico Varese, 'Mapping the Global Geography of Cybercrime with the World Cybercrime Index', *PLoS ONE*, 19.4 April (2024) <https://doi.org/10.1371/journal.pone.0297312>

Budhijanto, Danrivanto. *Hukum telekomunikasi, penyiaran dan teknologi informasi: Regulasi dan konvergensi.* -, 1919. http://digilib.fisipol.ugm.ac.id/handle/15717717/16253.

Delamaire, L., H. a. H. Abdou, dan J. Pointon. "Credit Card Fraud and Detection Techniques : A Review." *Banks and Bank Systems* 4, no. 2 (1 Juli 2009). https://salford-repository.worktribe.com/output/1465545.

Dijan Widijowati, Rr, 'Analysis of the Development of Cyber Crime in Indonesia', *International Journal Of Artificial Intelegence Research*, 6.1 (2022)

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (28 September 2021): 177–99. https://doi.org/10.25072/jwy.v5i2.460.

Dunsin, Dipo, Mohamed C Ghanem, Karim Ouazzane, and Vassil Vassilev, 'A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response', *Forensic Science International: Digital Investigation*, 48 (2024), doi:10.1016/j.fsidi.2023.301675

Edmon, Makarim. *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Jakarta: Raja Grafindo Persada, 2005.

Eurike Hailtik, Asri Gresmelian, and Wiwik Afifah, 'Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia', *Asian Journal of Social and Humanities*, 2.4 (2024), doi:10.59888/ajosh.v2i4.222

Faqih, Muhammad, and Enni Soerjati Priowirjanto, 'Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia', *Jurnal Indonesia*

Sosial Teknologi, 3.11 (2022), doi:10.36418/jist.v3i11.528

Gajjar, Vishalkumar Ravindrakumar, and Hamed Taherdoost, 'Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies', in *Proceedings - 2024 5th International Conference on Mobile Computing and Sustainable Informatics, ICMCSI 2024*, 2024, pp. 668 – 676, doi:10.1109/ICMCSI61536.2024.00105

Harahap, Tuti Khairani, Yuyut Prayuti, Nining Latianingsih, Amsari Damanik, Tiyas Maheni, Ida Farida, Mohamad Hidayat Muhtar, dan Mustaqim. "PENGANTAR ILMU HUKUM." *Penerbit Tahta Media*, 30 Mei 2023. https://tahtamedia.co.id/index.php/issj/article/view/255.

Haryanto, Agus Tri. "BSSN Akui Situs Resmi Miliknya Diretas." detikinet. Diakses 31 Maret 2024. https://inet.detik.com/security/d-5782090/bssn-akui-situs-resmi-miliknya-diretas.

Imroatus, Isnaini, Solichah ; Faizin, ; Sulistio, and Milda Istiqomah, 'Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia', *International Journal of Multicultural and Multireligious Understanding*, 2023

Jaya, Febri, dan Wilton Goh. "ANALISIS YURIDIS TERHADAP KEDUDUKAN KECERDASAN BUATAN ATAU ARTIFICIAL INTELLIGENCE SEBAGAI SUBJEK HUKUM PADA HUKUM POSITIF INDONESIA." *SUPREMASI HUKUM* 17, no. 02 (21 Juli 2021): 01–11. https://doi.org/10.33592/jsh.v17i2.1287.

Jufri, Muhammad Ariq Abir, dan Akbar Kurnia Putra. "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi." *Uti Possidetis: Journal of*

International Law 2, no. 1 (18 Maret 2021): 31–57. https://doi.org/10.22437/up.v2i1.11093.

Kurniawijaya, Aditya, Alya Yudityastri, dan Ayuta Puspa Citra Zuama. "PENDAYAGUNAAN ARTIFICIAL INTELLIGENCE DALAM PERANCANGAN KONTRAK SERTA DAMPAKNYA BAGI SEKTOR HUKUM DI INDONESIA." *Khatulistiwa Law Review* 2, no. 1 (2 Juni 2021): 260–79. https://doi.org/10.24260/klr.v2i1.108.

LL.M, Maskun, S. H. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media, 2022.

Manheim, Karl, dan Lyric Kaplan. "Artificial Intelligence: Risks to Privacy and Democracy." *Yale Journal of Law and Technology* 21 (2019): 106.

Mansur, Dikdik M. Arief. *Cyber law: aspek hukum teknologi informasi*. Tiga Serangkai, 2005.

Mokkapati, Ragini, and Venkata Lakshmi Dasari, 'An Artificial Intelligence Enabled Self Replication System Against Cyber Attacks', in *Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023*, 2023, pp. 698 – 703 <https://doi.org/10.1109/ICSSIT55814.2023.10061089>

Muhammad Ilman Abidin, 'Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography', *MIMBAR : Jurnal Sosial Dan Pembangunan*, 2023, doi:10.29313/mimbar.v39i2.2965

Muhtar, Mohamad Hidayat, Zainal Abdul Aziz Hadju, Zamroni Abdussamad, dan Rahmat Teguh Santoso Gobel. "Perluasan Kewenangan Komisi Penyiaran Indonesia Terhadap Pengawasan Media Digital." *Jurnal Konstitusi* 19, no. 1 (28 Maret 2022):

126–48. https://doi.org/10.31078/jk1916.

Muhtar, Mohamad Hidayat, Ichlas Tribakti, Agus Salim, Harry A. Tuhumury, M. Hasan Ubaidillah, Suwitno Y. Imran, Iskandar Laka, dkk. *Konsep Hukum Indonesia*. Global Eksekutif Teknologi, 2023.

Noval, Sayid Muhammad Rifki, 'Indonesia Readiness to Face Social Engineering Attacks with Deepfake Technology', *Journal of Law and Sustainable Development*, 11.12 (2023), doi:10.55908/sdgs.v11i12.727

Prasetya, Surya Eko, Hasnah Faiza, and Mangatur Sinaga, 'Verbal Violence in Comments of Supporting Candidates Presidential Elections 2019 in Instagram Based on ITE Law', *International Journal of Scientific and Technology Research*, 9.3 (2020)

Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, dan Moh Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (20 Juni 2020): 182–200. https://doi.org/10.33756/jlr.v2i2.6847.

Puluhulawa, Jufryanto, Mohamad Hidayat Muhtar, Mellisa Towadi, Vifi Swarianata, dan Apripari. "The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia." *Law, State and Telecommunications Review* 15, no. 2 (12 September 2023): 132–45. https://doi.org/10.26512/lstr.v15i2.44206.

Qalbi, Nur, and Putri Ramadhani, 'Urgensi Undang-Undang ITE Di Era Globalisasi', *Jurnal Litigasi Amsir*, 9.2021 (2022)

Qamar, Nurul. *Hak Asasi Manusia Dalam Negara Hukum Demokrasi (Human*

Vol. 11, Issue 01, April, 2024
P-ISSN: 2355-5173 E-ISSN: 2656-9477

Cybercrime Threats and Responsibilities from an Islamic Legal Perspective:
The Utilization of Artificial Intelligence in Online Crime

Rights in Democratiche Rechtsstaat). Makassar: SInar Grafika, 2013.

Rich, Elaine. "Artificial Intelligence and the Humanities." *Computers and the Humanities* 19, no. 2 (1985): 117–22.

Ririh, Kirana Rukmayuninda, Nur Laili, Adityo Wicaksono, dan Silmi Tsurayya. "STUDI KOMPARASI DAN ANALISIS SWOT PADA IMPLEMENTASI KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE) DI INDONESIA." *J@ti Undip: Jurnal Teknik Industri* 15, no. 2 (7 Juni 2020): 122–33. https://doi.org/10.14710/jati.15.2.122-133.

RS, Iza Rumesten, Mohammad Hidayat Muhtar, Amanda Adelina Harun, Dolot Alhasni Bakung, dan Nirwan Junus. "Protection of Human Rights Against the Environment in the Indonesian Legal System." *Journal of Law and Sustainable Development* 11, no. 10 (2023): e570–e570.

Sihombing, Eka NAM, dan Muhammad Yusrizal Adi Syaputra. "Implementasi Penggunaan Kecerdasan Buatan dalam Pembentukan Peraturan Daerah." *Jurnal Ilmiah Kebijakan Hukum* 14, no. 3 (2 November 2020): 419–34. https://doi.org/10.30641/kebijakan.2020.V14.419-434.

Spiegeleire, Stephan De, Matthijs Maas, dan Tim Sweijs. *Artificial Intelligence and the Future of Defense: Strategic Implications For Small- and Medium-Sized Force Providers*. The Hague Centre for Strategic Studies, 2017.

Stupp, Catherine. "Fraudsters used AI to mimic CEO's voice in unusual cybercrime case." *The Wall Street Journal* 30, no. 08 (2019). https://fully-human.org/wp-content/uploads/2019/10/Stupp_Fraud

sters-Used-AI-to-Mimic-CEOs-Voice-in-Unusual-Cybercrime-Case.pdf.

Tehrani, Pardis Moslemzadeh, Nazura Abdul Manap, and Hossein Taji, 'Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime', *Computer Law and Security Review*, 29.3 (2013), doi:10.1016/j.clsr.2013.03.011

Williams, Matthew L., Pete Burnap, dan Luke Sloan. "Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns." *The British Journal of Criminology* 57, no. 2 (1 Maret 2017): 320–40. https://doi.org/10.1093/bjc/azw031.

Yudoprakoso, Paulus Wisnu. "KECERDASAN BUATAN (Artificial Intelligence) SEBAGAI ALAT BANTU PROSES PENYUSUNAN UNDANG-UNDANG DALAM UPAYA MENGHADAPI REVOLUSI INDUSTRI 4.0 DI INDONESIA." *Simposium Hukum Indonesia* 1, no. 1 (12 Juni 2019): 450–61.

Zheng, Muwei, Hannah Robbins, Zimo Chai, Prakash Thapa, dan Tyler Moore. "Cybersecurity Research Datasets: Taxonomy and Empirical Analysis," 2018. https://www.usenix.org/conference/cset18/presentation/zheng..

Zumarsyah, Pandega Abyan, 'Sejarah Kecerdasan Buatan Atau Artificial Intelligence (AI)', *Www.Warstek.Com*, 2021

.