Jurnal Idea Hukum

Vol. 11 Issue 2, October 2025
E-ISSN 2442-7454 P-ISSN 2442-7241
DOI: 10.20884/1.jih.2025.11.2.651

Cyber Law Reform in Indonesia: Regulatory Challenges, Technological Dynamics, and Adaptive Policy Directions in Digital Era

Eriene Chindy Octaviandini, Ajeng Aditya Listyani
Universitas Jenderal Soedirman
✉ erienchindy@yahoo.co.id

Submitted : 12/09/2025
Revised : 17/10/2025
Accepted : 03/11/2025

Abstract
The increase in cybercrime in Indonesia, such as data theft, ransomware attacks, and the misuse of artificial intelligence (AI), shows that the national legal framework is not yet fully effective in dealing with the dynamics of the digital era. Although Indonesia has the Electronic Information and Transaction Law (EIT Law) and the Personal Data Protection Law (PDP Law), both still have various weaknesses, including ambiguous norms, weak harmonization between regulations, and limited capacity of law enforcement officials. The purpose of this study is to analyze the effectiveness of the national cyber legal framework in responding to developments in digital technology, identify the main challenges in its enforcement, and formulate the direction of legal reform policies needed to make Indonesia's legal system more adaptive, effective, and responsive to technological developments, particularly in regulations concerning artificial intelligence that guarantee the principles of accountability, transparency, and justice. This study uses a normative juridical method, which is legal research based on literature studies by examining written legal materials. Data was obtained from primary legal materials in the form of laws and regulations related to cyber law, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Law Number 27 of 2022 concerning Personal Data Protection, the Draft Law on Cyber Security and Resilience (RUU KKS), and other related regulations. Secondary legal materials include literature, research results, scientific journal articles, and reports from relevant institutions from a national and international comparative perspective. The analysis was conducted using qualitative normative methods with an emphasis on legal interpretation, consistency of norms, and the relevance of regulations to the needs of cyber law reform in Indonesia. The results of the study indicate that cyber law reform is necessary to establish a legal system that is adaptive and responsive to technological developments. These efforts include accelerating the ratification of the KKS Bill, harmonizing regulations, increasing the capacity of law enforcement officials, and strengthening public digital literacy in order to strengthen national resilience in cyberspace and protect the digital rights of citizens.

Keywords: Accountability; Artificial Intelligence; Cyber Law; Legal Reform; Transparency.

Introduction

The development of information and communication technology has transformed all aspects of human life, including social and economic behavior. Society's dependence on the internet, electronic transactions, and digital data storage has increased rapidly. However, along with this convenience, various cybercrime risks have emerged, becoming increasingly complex and difficult to detect. These crimes include data theft, system hacking, malware distribution, and digital identity theft. This phenomenon demands an updated legal framework that can adapt to rapid

technological change.[1] Cyber law reform is a process of updating the legal system that includes improving regulations, adjusting law enforcement agencies, and harmonizing legal norms with the needs of the digital society.[2] In a legal context, the term reform refers to a comprehensive overhaul of regulations and their implementation to align with social, economic, and technological developments. Cyber law itself is a field of law that regulates human activity in the digital space, including electronic transactions, personal data protection, and network security.[3]

The phrase "urgent cyber law reform" in this title implies that legal reform in the cyber sector has become an urgent need for Indonesia. The development of science and technology produced by human civilization is constantly changing and improving, impacting the behavior of modern society, which relies on technology. This rapid development of science and technology has also been accompanied by several misuses of these developments. As a control tool, the development of science and technology, as an effort to prevent and prosecute crimes, has transformed into a threat that is more difficult to detect.

This intersects with the increasing rate of digital adoption, which also increases the impact of cybercrime. This merits special study because it relates to Indonesian criminal law, which still needs to adapt and develop rapidly to the highly dynamic changes in science and technology. Cyber Law is a legal term related to the use of rapidly developing information technology. Thatcybercrimehas special characteristics compared to other conventional crimes, namely Regarding the scope of the crime, the nature of the crime, the perpetrator, the modus operandi, and the types of losses it causes. Unlimited internet access is no longer uncommon in today's world, as everyone is taking advantage of internet facilities. Using the internet provides us with the convenience of unlimited access to anything. This convenience is the primary factor driving some individuals to commit crimes.Cybercrimeeasily.[4]

In two UN Congress documents regarding The Prevention of Crime and the Treatment of Offenders in Havana, Cuba in 1990 and in Vienna, Austria in 2000, there were two terms known as Cyber Crime the narrow sense it is called computer crime, namely illegal behavior or direct violation attack the security system of a computer or data processed by a computer.Cyber crime in a broad sense it is calledcomputer-related crime, namely illegal or violating behavior relating to computer systems or networks.[5] Cyber crime is defined as a criminal act carried

[1] Maskun, *Kejahatan Siber (Cyber Crime)* (Jakarta: Kencana, 2013), 21.
[2] Muhammad Labib & Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)* (Bandung: PT. Refika Aditama, 2005).
[3] Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: Refika Aditama, 2012), 33.
[4] Sahat Maruli Situmeang, *Cyber Law, International Law, Security, and Military Power* (Bandung: Cakra, 2025).
[5] Eliasta Ketaren, "Cybercrime, Cyber Space, Dan Cyber Law," *Jurnal TIMES* 5, no. 2 (February 2017): 37, https://doi.org/10.51351/jtm.5.2.2016556.

out using technology computers as the main tool of crime. This crime takes advantage of developments computer technology, especially the internet.[6]

Cybercrime refers to criminal activity conducted using computer technology or digital data, particularly in the banking sector, targeting individuals' personal information. The types of crimes referred to include prohibited behavior conducted online, such as unauthorized access to computer systems, stealing sensitive information, distributing malicious software, and so on. According to the Ministry of Communication and Information Technology (Kominfo), Indonesia ranks third in the world for cybercrime cases, after Ukraine. It is important to consistently prioritize awareness of these alarming statistics.[7] As a comparison, research by Judijanto and Nugroho (2025) entitled "Cyber Security Regulation and Law Enforcement against Cybercrime in Indonesia" highlights the weak implementation of the ITE Law and the need for synergy between institution.[8] Aprilianti's research (2025) in the Begawan Abioso Journal emphasizes the ambiguity of norms in the ITE Law which leads to multiple interpretations.[9] Meanwhile Najwa (2024) in the AL-BAHTS Journal highlighted the low effectiveness of law enforcement. cyber at the operational level.[10] In contrast to these studies, this article highlights the urgency of comprehensive cyber law updates that are not only reactive, but also adaptive to new technological developments such as artificial intelligence (artificial intelligence).

In 2000, the government began to initiate initiatives to regulate various activities in cyberspace. Efforts to regulate human activities in cyberspaceincluding the criminal law aspect has been carried out since 2000, namely first with the drafting of the Bill on the Utilization of Information Technology which was initiated by the Directorate General of Post and Telecommunications, Ministry of Transportation.[11] The bill was finally merged into the Information, Communication, and Electronic Transaction Bill (RUU IKTE) initiated by the Directorate General of Post and Telecommunications of the Ministry of Transportation and the Ministry of Industry and Trade. Since March 2003 the formation of the IKTE Bill was then carried out by the Ministry of Communication

---

[6] Lita Sari Marita, "Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia," *Cakrawala:Jurnal Humaniora Unievrsitas Bina Sarana Informatika* 15, no. 2 (2015), https://doi.org/https://doi.org/10.31294/jc.v15i2.4901.

[7] F Muin, "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi," *IDRIS: Indonesian Journal of Islamic Studies* 1, no. 1 (2023): 100.

[8] Loso Judijanto and Budi Nugroho, "Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia," *Sanskara Hukum Dan HAM* 3, no. 03 (April 2025): 120, https://doi.org/10.58812/shh.v3i03.544.

[9] Astri Aprilianti, "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi," *Begawan Abioso* 15, no. 1 (January 2025): 41–50, https://doi.org/10.37893/abioso.v15i1.1002.

[10] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (January 2024): 8–16, https://doi.org/10.32520/albahts.v2i1.3044.

[11] Suseno, *Yurisdiksi Tindak Pidana Siber*.

and Information and became the Electronic Information and Electronic Transaction Bill (RUU IETE). In 2005 the Ministry of Communication and Information based on Government Regulation of the Republic of Indonesia No. 9 of 2005 changed to the Ministry of Communication and Information (DEPKOMINFO) and the preparation of the IETE Bill which later changed to the Information and Electronic Transaction Bill (RUU ITE) was carried out by the Ministry of Communication and Information. Through discussions in the DPR on March 25, 2008, the DPR plenary session approved the ITE Bill to be stipulated as a Law and then on April 21, 2008 by the President of the Republic of Indonesia it was promulgated by Law No. 11 of 2008 concerning Information and Electronic Transactions State Gazette of 2008 No. 58.[12]

From a legal perspective, regulations regarding digital science and technology are generally still in the development stage. According to Barda Nawawi Arief, the national/territorial legal system and jurisdiction do have limitations because it is not easy to reach perpetrators of criminal acts in the virtual world. Artificial intelligence (artificial intelligence/AI) has become a highly influential technology in the digital era. AI, besides assisting and revolutionizing human work, also presents new challenges, including in the field of law enforcement. Conceptually, AI is capable of mimicking human intelligence and even rivaling it. However, in practice, this has backfired on the development of today's digital technology. The speed of digital technology development cannot be controlled at all times, however, law, even though modern, remains inherently rigid, formal, and less flexible, so that it experiences difficulties in accommodating various new phenomena in cybercrime.

The problems faced by society are controlled by the authorities, because the "cyberspace" has become and been used as a "new home." The authorities are already very heavy in dealing with the crimes that occur in society, considering the large number and variety of crimes that occur, which sometimes occur in a society that is not expected at all to be the target of a crime, or suddenly in that society a crime has already occurred, or suddenly in that society a crime has already occurred. [13] The emergence of a crime calledcyberspaceor by another namecybercrimeIt's a justification that this global era is synonymous with the era of vicious minefields. An imaginary, virtual space, an area or zone for everyone to artificially engage in activities that can be carried out in everyday social life. Everyone can communicate with each other, enjoy entertainment, and access anything they find enjoyable or perhaps satisfying. There are various offers in cyberspace in accordance with global information sold by capitalists who are willing to justify any means to gain profit. Ironically, they also intend to undermine

[12] Suseno.
[13] Muhammad Labib & Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)*.

the moral, ideological, and religious resilience of other nations on earth that differ from their own.[14]

The legal rules that are most often used in Indonesia when a crime occurs cyber crimeThese are positive legal regulations, namely the Criminal Code (KUHP) and the Criminal Procedure Code (KUHAP). The Criminal Code, in particular, is still considered a sufficient legal basis, although, frankly, this is not entirely true. However, it remains the only option amidst the legal vacuum in the technology and information sector.[15] As time goes by, Indonesia has legally had several regulations that function as a legal umbrella to addresscyber crime. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was revised by Law Number 19 of 2016 and its amendments, became one of the first legal bases that regulatescyber crime.The classification of prohibited acts in the ITE Law is explained in Articles 27 to 37. The construction of these articles regulates in more detail the development of traditional crime modes as stated in the Criminal Code.

In addition to the ITE Law, the government also passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as a progressive step in provide legal protection for people's personal data.[16] As a legal instrument intended for the public interest, the ITE Law serves as a state control tool for information systems and electronic transactions, which tend to be free. Of course, implementing a legal instrument, including the ITE Law, requires stages tailored to societal needs and actual conditions on the ground. However, issues arise regarding the effectiveness of the ITE Law's implementation in achieving its intended goals and functions.[17] In addition to the ITE Law and the PDP Law, there are other regulations related to cybersecurity in Indonesia, such as the National Cyber and Crypto Agency (BSSN), a government agency tasked with cybersecurity, and the New Regulations for the Financial Sector, developed by the Financial Services Authority (OJK). These regulations cover a wide range of aspects, from personal data protection to cyberattack prevention. However, many of these regulations remain fragmented and do not provide a comprehensive framework.

The first obstacle is resource constraints, both financial and expert. Furthermore, there is a gap in knowledge and expertise between policymakers and cybersecurity practitioners. This gap makes it difficult to translate policies into effective practice. Therefore, it is crucial to develop law enforcement capacity to address cybercrime. Given the complexity and technical nature of cybercrime, law

[14] Muhammad Labib & Abdul Wahid.
[15] Maskun, *Kejahatan Siber (Cyber Crime)*.
[16] Muhammad Aabid, Tyas Dzaky, and Ibrahim Fikma Edrisy, "Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital," *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 12.
[17] Aprilianti, "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi."

enforcement in Indonesia requires adequate resources and specialized training. This also includes increased inter-agency cooperation, law enforcement capacity building, and the implementation of more adaptive and responsive legal strategies to the dynamics of threats.[18]

Data from the National Cyber and Crypto Agency (BSSN) shows that throughout 2024, there were more than 300 million cyberattacks detected against Indonesia's digital infrastructure, an increase of almost 25% compared to the previous year.[19] This fact illustrates that cyber threats now target not only individuals but also government systems and strategic national sectors. Therefore, cyber law reform is not merely an academic necessity but a strategic aspect in maintaining national resilience in the digital space. Given this situation, Indonesia needs to review the effectiveness of existing regulations such as the ITE Law and the Privacy and Personal Data Law, and expedite deliberations on the Draft Law on Security and Cybersecurity. Cyber Resilience (KKS Bill). Legal reform in this area is expected to create a legal system that is responsive to new threats, strengthen protection of citizens' digital rights, and increase public trust in national cybersecurity.

Research Problems

1. What are the actual conditions and weaknesses of cyber law regulations in Indonesia in responding to the development of digital technology and the increase in cybercrime?
2. What are the main challenges and policy directions needed in cyber law reform to build a legal system that is adaptive, effective, and responsive to the dynamics of the digital era?

Method

This research uses a normative juridical method, namely legal research based on library research by examining written legal materials. Data were obtained from primary legal materials in the form of legislation related to cyber law, as well as secondary legal materials. Primary legal materials include statutory regulations which are directly regulate or are related to cyber law in Indonesia, including:

1. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law);
2. Law Number 19 of 2016 concerning Amendments to the ITE Law;
3. Law Number 27 of 2022 concerning Personal Data Protection (Law PDP);
4. Draft Law on Cyber Security and Resilience (RUU KKS);

[18] Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."
[19] BSSN, "Lanskap Keamanan Siber Indonesia 2024," 2024.

5. Presidential Regulation Number 53 of 2017 concerning the National Cyber and Crypto Agency (BSSN); and
6. Financial Services Authority (OJK) Regulation Number 38/POJK.03/2016 concerning Implementation of Risk Management in the Use of Information Technology by Banks General.

Secondary legal materials consist of literature, research findings, scientific journal articles, and institutional reports relevant to cyber law issues, both from a national legal perspective and from an international comparative perspective. These secondary legal materials are used to strengthen the analysis, compare policies between countries, and clarify the direction of necessary legal reforms. The research analysis is conducted qualitatively and normatively, emphasizing legal interpretation, norm consistency, and their relevance to the need for cyber law reform in Indonesia, in order to examine weaknesses in existing regulations. Secondary legal materials are legal materials that provide explanations of primary legal materials, such as books, previous research results, journal articles, etc.

Discussion

1. Conditions and Weakness of Cyber Law Regulations in Indonesia in Facing the Development of Digital Technology and Increasing Cybercrime

a. The State of Cyber Law Regulation in Indonesia

The Electronic Information and Transactions Law (UU ITE), passed in 2008 and amended in 2016, serves as Indonesia's primary framework for combating cybercrime, addressing offenses such as defamation, hate speech, and electronic fraud.[20] Indonesian cybersecurity regulations, enshrined in the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), provide the legal framework for addressing cybercrime. The ITE Law establishes clear provisions for addressing offenses such as electronic fraud, defamation, and hacking, while the PDP Law enhances data protection by imposing obligations on data handlers and introducing penalties for violations, in line with global privacy regulatory trends. Supporting regulations, such as Presidential Regulation No. 53 of 2017, further strengthen cybersecurity governance by establishing the National Cyber and Crypto Agency (BSSN),[21] As well as regulations related to digital financial transactions developed by the Financial Services Authority (OJK). However, the implementation of cyber law remains reactive, or better known as resolving problems after they occur, rather than preventive, which is the prevention of crime. Cybersecurity has the primary goal of maintaining the

[20] Judijanto and Nugroho, "Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia."
[21] Judijanto and Nugroho.

confidentiality, integrity, and availability of sensitive information, as well as protecting information technology infrastructure from attacks that could damage systems or incur significant losses. Amidst the ever- evolving complexity of threats, collaboration between the government, the private sector, and the public is becoming increasingly important in efforts to maintain national security and sovereignty from potential threats and disruptions.[22]

Cybercrime is indeed a different criminal activity that requires its own set of rules and regulations beyond the scope of The Indonesian Criminal Code (KUHP) requires extraordinary regulation due to the unique characteristics of the rapidly evolving technology that enables it. Conceptually, this ruling requires knowledge of Indonesian (criminal) law. According to Rene David, Indonesia has a "mixed legal system." However, the legacy of continental law appears to be more important in the practice and development of legal science in the field of public law, particularly criminal law. Therefore, an integrated approach to developing regulations regarding cybercrime should be implemented by revising or overhauling the entire Criminal Code.[23]

The ITE Law is the legal framework that underpins the regulation of electronic transactions, personal data protection, electronic transaction security, as well as copyright and intellectual property in the digital world. As written in the book entitled Questions and Answers Regarding Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), it has two main objectives: first, to facilitate the development of the digital economy in Indonesia. Second, to provide a sense of security, justice, and legal certainty for Internet users and operators in Indonesia. In addition, the ITE Law also replaces and expands two previous laws, namely Law No. 7 of 1996 concerning Telecommunications and Law No. 36 of 1999 concerning Telecommunications. As a law regulating the field of information technology, the ITE Law covers a wide range of content, including the rights and obligations of Internet users and electronic system providers. This covers aspects of data security and personal information, protection of intellectual property rights in the digital world, and the responsibilities of anyone using information technology and electronic transactions in Indonesia.

[22] Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2, no. 2 (July 2024): 70, https://doi.org/10.58707/aldalil.v2i2.777.

[23] Martini Idris et al, "Regulation and Enforcement of Cyber Crime Law: Harmonization of the Revision of the ITE Law and the Criminal Code," *Lex Lata: Scientific Journal of Legal Science* 6, no. 3 (2024): 400, https://doi.org/https://doi.org/10.28946/lexl.v6i3.4266.

Before the existence of cyber law specifically regulating the technology and information sector, cybercrime was handled by interpreting the actions taken within existing legislation. Some laws used in this context include:

1) Law Number 14 of 2008 concerning Public Information Disclosure;
2) Law Number 36 of 1999 concerning Telecommunications;
3) Law Number 19 of 2002 as amended by Law Number 28 of 2014 concerning Copyright;
4) Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning the Crime of Money Laundering, as replace by Law Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundring; and
5) Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism.[24]

Existing laws and regulations are still unable to comprehensively address the challenges of cyberspace. Therefore, more adaptive legal adjustments are needed to safeguard national sovereignty and protect the public from various threats emerging in the digital era. As the first cyber law in Indonesia, the ITE Law covers various important aspects of technology and information. It is the first legal product in Indonesia to regulate various aspects related to information technology and cyberspace. The government's efforts to protect the public are realized through various regulations and sanctions outlined in the ITE Law.[25]

Every law must have a specific purpose in its creation. Likewise, the ITE Law explains various objectives related to its purpose. Article 4 of the ITE Law states:

> *The use of Information Technology and Electronic Transactions is carried* out with the aim of:
> a. To enlighten the life of the nation as part of the global information society;
> b. Developing national trade and economy in order to improve the welfare of the community;
> c. Increasing the effectiveness and efficiency of public services;
> d. Opening up the widest possible opportunities to every person to advance their thinking and abilities in the field of using and exploiting Information Technology as optimally as possible and responsibly; and
> e. Provide a sense of security, justice and legal certainty for users and providers of Information Technology.

Article 4 of the ITE Law explains the use of technology. Electronic information and transactions are implemented to improve the life of the nation as part of the global information society; develop national trade and

[24] Aprilianti, "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi."
[25] Aprilianti.

economy in order to improve the welfare of the people; increase the effectiveness and efficiency of public services; open up the widest possible opportunities for everyone to advance their thinking and abilities in the field of optimal and responsible use and utilization of Information Technology, then the general objective of a law is to provide a sense of security, justice and legal certainty in this law, especially for users and providers of Information Technology.[26] Regulatory effectiveness is a discussion of laws based on the positive norms contained therein, while objective effectiveness is a discussion of whether a law can achieve the desired goals of its creation. A distinction between regulatory effectiveness and objective effectiveness is necessary because not every effective regulation can achieve the goals for which it was created.[27]

b. Weaknesses of Cyber Law Regulation

1) Weakness in Coverage

The ITE Law does not fully address all forms of evolving cybercrime. It lacks provisions for regulating complex cybercrimes such as attacks on critical infrastructure and crimes involving new technologies. Digital technology is evolving rapidly, while legal regulation is slow;

2) Weak Implementation

The implementation of the ITE Law is often hampered by a lack of understanding and differing interpretations among law enforcement and the judicial system;

3) Lack of Harmonization

Regional cyber regulations have not been well coordinated with national regulations or international standards, leading to inconsistencies in law enforcement across regions. Regulations are still scattered across various laws and institutions, creating legal uncertainty;[28]

4) Legal Sanctions that are not yet Sufficiently Detterent

Several provisions in the ITE Law are still considered open to interpretation and sometimes disproportionate, and penalties for certain cybercrimes are still considered light compared to the impact of the losses. SAFEnet Executive Director, Damar Juniarto, stated that the ITE Law has not provided a sense of justice and needs to be revised. In

[26] Radita Setiawan and Muhammad Okky Arista, "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana," *Recidive* 2, no. 2 (2018): 139–46.
[27] Setiawan and Arista.
[28] Andri Sahata Sitanggang, Fernanda Darmawan, and Dony Saputra, "Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber," *Jurnal Pendidikan Dan Teknologi Indonesia* 4, no. 3 (September 2024): 82, https://doi.org/10.52436/1.jpti.409.

a webinar held by Amnesty International Indonesia Chapter UNAIR, researcher Adhigama A. Budiman from ICJR stated that the ITE Law limits at least three types of human rights: 1. Freedom of expression and opinion; 2. The right to access information; 3. The right to privacy;[29]

If related to Article 4 of the ITE Law, Indonesia has several inhibiting factors, as follows:

a) From a technological perspective, people still tend to be free in using modern facilities such as technology, meaning they are not yet familiar with the limitations and regulations contained in the ITE Law;
b) In the aim of developing trade and the economy by using technology as a means, Indonesian people in electronic transactions are still often in the public spotlight due to violations that often occur, such as: many parties are harmed by online buying and selling via websites and social media;
c) In Indonesia, the aim of advancing thinking and skills in the field of the use and utilization of Information Technology is declared incompetent, because there are still many users who distribute illegal content via websites and social media, such as: pornography, SARA, threats, and defamation;
d) The ITE Law is said to not provide a sense of security, justice, and legal certainty, especially for users and providers of information technology. This is because law enforcement officials are said to be slow in prosecuting ITE cases and have no deterrent effect, resulting in numerous ITE crimes that continue to disturb the public.[30]

5) Limited Capacity of Law Enforcement Officers

Law enforcement officers still need to improve their competence in the field of digital technology, cases often fail due to weak digital forensic evidence;

6) Victim Protection is Still Weak

The legal focus is more on punishing perpetrators, while mechanisms for compensation or restitution for victims remain minimal. For example, in data breaches, victims lose their right to privacy but struggle to seek adequate compensation;

[29] Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."
[30] Setiawan and Arista, "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana."

7) Lack of Personal Data Protection

Highlighting that the ITE Law does not have sufficiently specific or robust provisions to address large-scale personal data breaches and may lack comprehensive data security requirements, effective data breach reporting mechanisms, and clear provisions on corporate responsibilities in protecting user data. The ITE Law does not have a mandatory provision for reporting data breach incidents to authorities or affected parties within a specified timeframe. This has led to delays in handling cases data leaks and worsen the impact on users whose personal data is leaked.[31]

2. What are the main challenges and policy directions needed in cyber law reform to create a legal system that is adaptive, effective, and responsive to the digital era?

Artificial intelligence is one of the most influential technologies of the modern era. In New Zealand, AI helps judges, court officials, court members, and judicial support staff. The move marks a significant evolution in increased efficiency, accessibility, and technological advances in justice.[32] Some AI systems are more efficient than humans at certain tasks such as mimicking the voices and images of others to influence people and create political change.[33] Besides that, Thailand is also implementing AI in several sectors. In particular, the Thai government views that AI is a tool to enhance the country's competitiveness, especially in the industry, service, and health sectors.[34] Additionally, AI has been widely applied in all sectors of society. AI is thought to make things easier and to improve growth in a system or work process.[35]

The implementation of AI, driven by its autonomous, adaptive, and complex nature, creates unprecedented challenges for the legal system. One fundamental issue is the rapid pace of AI technological development, which far outstrips the ability of the law to adapt. Laws, as products of human legislation, tend to be reactive and require a lengthy process to be enacted. On the other hand, AI technology is evolving rapidly, often creating new, unexpected innovations that

[31] Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."
[32] Nur Putri Hidayah et al., "Artificial Intelligence and Quality of Composition Verdicts in Indonesia: Lessons from New Zealand," *Journal of Human Rights, Culture and Legal System* 4, no. 1 (February 2024): 105, https://doi.org/10.53955/jhcls.v4i1.175.
[33] Naek Siregar et al., "The Use of Artificial Intelligence in Armed Conflict under International Law," *Hasanuddin Law Review* 10, no. 2 (July 2024): 189, https://doi.org/10.20956/halrev.v10i2.5267.
[34] Stanati Netipatalachoochote and Ludovic Pailler, "Developing Artificial Intelligence Legislation in Thailand: Lessons from the European Union," *Journal of Human Rights, Culture and Legal System* 5, no. 1 (March 2025): 10, https://doi.org/10.53955/jhcls.v5i1.424.
[35] Hary Abdul Hakim, Chrisna Bagus Edhita Praja, and Sung Ming-Hsi, "AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia," *Jurnal Hukum Novelty* 14, no. 1 (April 2023): 125, https://doi.org/10.26555/novelty.v14i1.a25943.

fall outside the scope of existing regulations. As a result, the law often lags behind in regulating these developments, creating loopholes that can be exploited by criminals.[36]

In Indonesia, these challenges are further exacerbated by the limitations of the existing legal framework. Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), although amended by Law No. 19 of 2016, still does not fully address the complexities of AI-based crimes. For example, the ITE Law focuses more on traditional cybercrimes such as identity theft and illegal access, while AI-based crimes, such as the misuse of algorithms for data manipulation or the creation of deepfakes, are not explicitly regulated. This creates legal loopholes that criminals can exploit.[37] The absence of specific regulations creates uncertainty in the application of the principle of legality and makes it difficult for law enforcement to prosecute perpetrators with a clear legal basis. Therefore, comprehensive regulatory reforms are needed to accommodate developments in artificial intelligence technology and ensure effective legal protection for the digital community.

The implementation of the ITE Law from 2008 to 2016 was plagued by numerous problems. Provisions prohibiting the dissemination of illegal content often clashed with the protection of the right to freedom of expression, a constitutionally protected right. Legitimate citizen expressions, such as criticism of public policy, complaints about services, reporting on specific cases and public discussion materials, were continually targeted by the ITE Law, both for defamation and slander. Imprisonment for legitimate and protected opinions and expressions has a chilling effect on the public's ability to express opinions and express themselves freely.[38] This condition shows that the implementation of the ITE Law is not fully in line with the principle of proportionality anddue process of lawwhich is the foundation of a state based on the rule of law. Law enforcement against freedom of expression not only violates citizens' constitutional rights but also undermines public trust in the judicial system.

The failure of the House of Representatives (DPR) and the government to implement comprehensive changes and resolve the fundamental issues of the 2008 ITE Law has resulted in an increasing number of expressions being subject to criminal charges. Furthermore, the ITE Law also has the potential to become a tool for criminalizing individuals who should be protected by law. Baiq Nuril, a female teacher who was the victim of sexual harassment by her superior, was instead charged under the ITE Law. Baiq Nuril, who attempted to gather evidence of the

[36] Wahyudi Br, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI" 5 (2025).
[37] Adhansonh Aqilla Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *JURNAL USM LAW REVIEW* 7, no. 3 (2024): 1737–58, https://doi.org/https://doi.org/10.26623/julr.v7i3.10578.
[38] Adhigama A Budiman et al., *Mengatur Ulang Kebijakan Tindak Pidana Di Ruang Siber: Studi Tentang Penerapan UU ITE Di Indonesia*, *Metode Penelitian*, vol. 12, 2021.

harassment by recording her superior's indecent conversation and giving consent for the recording to be used to report her superior to the DPRD, was instead charged with distributing content that violates morality. Baiq Nuril was then charged with violating Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of the ITE Law and sentenced to six months in prison and a fine of 500 million Rupiah, subsidiary to three months in prison in the cassation decision at the Supreme Court, which continued with a rejected PK application. This case ended with the granting of amnesty by the President after widespread public criticism.[39]

The legal vacuum surrounding several regulations covering cybercrimes, including AI, in the ITE Law reflects the challenges Indonesia faces, including a lack of legal infrastructure and human resources with a deep understanding of this technology. While the government aims to provide flexibility for technological development, the lack of regulation actually increases the risk of AI misuse, such as disinformation and privacy violations. Existing ethical guidelines are not yet legally sound, necessitating specific regulations to ensure security, fairness, and transparency in the use of AI. These regulations could also establish AI as a legal entity responsible for its actions.[40] However, implementing the concept of AI as a legal subject certainly requires in-depth legal study, given that the Indonesian legal system still focuses on the accountability of humans and legal entities. Therefore, a normative framework is needed that defines the boundaries of responsibility between developers, users, and the AI system itself, to ensure the principles of legal certainty and justice are maintained in an increasingly autonomous digital era.

In many cases, AI systems act autonomously based on algorithms designed by developers or data provided by users. If AI systems are used to commit crimes, such as market manipulation or political disinformation, it is difficult to determine who should be held legally responsible, whether the developer, the user, or the system itself. This creates legal uncertainty that perpetrators can exploit to avoid criminal liability. Another significant challenge is the mismatch between the development of AI technology and the slow legislative process. The process of formulating laws in Indonesia often takes years, while AI technology is developing very rapidly, producing new innovations in a matter of months. As a result, existing regulations tend to lag far behind the technological realities on the ground, creating a gap. This provides a strategic advantage for criminals who can exploit the lack of relevant regulations.[41]

Indonesia provides ethical guidelines for the use of AI through Circular Letter of the Minister of Communication and Informatics Number 9 of 2023 concerning the Ethics of Artificial Intelligence. However, these ethical guidelines are not yet

[39] Budiman et al.
[40] Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation."
[41] Br, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI."

legally binding, necessitating specific regulations to ensure safety, fairness, and transparency in the use of AI. These regulations could also establish AI as a legal entity responsible for its actions.[42] Indonesia needs to learn from other countries and design appropriate regulations and rules, involving all parties to ensure the responsible use of AI. With the right regulations and rules, AI can be treated as a legal entity, protecting the public and promoting fair and inclusive digital progress. [43] Furthermore, these regulations must be formulated using a multidisciplinary approach involving legal, technological, ethical, and public policy experts to ensure that the resulting norms are not merely reactive but also anticipatory to technological developments. The establishment of an independent oversight body is also necessary to ensure the implementation of the principles of accountability and transparency in the development and use of AI.

Theory Social Engineering Roscoe Pound can be applied to analyze this phenomenon. For Roscoe Pound, laws are enacted with the aim of maximizing the satisfaction of needs and interests. [44] In this context, the theorySocial EngineeringRoscoe Pound emphasized the importance of regulation as a social control to ensure the use of AI is carried out responsibly, protect individual rights, and prevent greater negative impacts on society.[45] This approach positions the law not merely as a repressive instrument, but as a means of social engineering (law as a tool of social engineering) which serves to direct societal behavior toward a more just and orderly order. Therefore, the formation of AI-related regulations must consider the balance between technological innovation and protecting the public interest. Laws need to be able to adapt to social changes brought about by digital developments without losing its primary function as a guardian of justice and public order. Furthermore, coordination between state institutions is needed in formulating cross-sectoral policies to ensure that the application of laws to AI is not partial and overlapping. Comprehensive regulations will ensure that technological developments do not exceed legal capacity but rather proceed in tandem within the framework of human rights protection and legal certainty.

Under Indonesian criminal law, only humans and corporations are considered legal subjects, so it's unclear who is responsible if AI commits a crime. Some experts propose that AI be categorized as a partial legal subject, with limited rights and obligations but no criminal liability. If AI violates the law, responsibility

---

[42] Febri Jaya and Wilton Goh, "Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia," *SUPREMASI HUKUM* 17, no. 02 (July 2021): 01–11, https://doi.org/10.33592/jsh.v17i2.1287.

[43] Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation."

[44] Sofia Mubarokah Sa'bana and Rusdiana Navlia, "Penerapan Teori Fungsi Hukum Roscoe Pound: Soscial Engineering Di Indonesia," *Jurnal Jendela Hukum* 12, no. 1 (April 2025): 47, https://doi.org/10.24929/jjh.v12i1.4217.

[45] Imelda Martinelli et al., "Urgensi Pengaturan Dan Perlindungan Rights of Privacy Terhadap Artificial Intelligence Dalam Pandangan Hukum Sebagai Social Engineering Imelda," *Jurnal Tana Mana* 4, no. 2 (2023): 158–66.

is transferred to the developer or user as a guardian, using the concept of "legal guardianship."in loco parentis" meaning that AI is its child, while the developer or user as the legal subject has power over the partial legal subject. For example, the concept of "in loco parentis"also applied in India as a legal subject for the Ganges River.[46] This approach demonstrates an effort to adapt the principle of criminal liability to the reality of increasingly autonomous technology. However, implementing this concept requires explicit legal recognition through regulatory reforms to avoid uncertainty in determining who should be held responsible for unlawful acts committed by AI systems.

As AI develops, experts believe it will possess increasingly advanced sentient abilities and is predicted to surpass human intelligence. Current technology is also considered capable of creating AI that can understand various aspects of independence and intelligence. Technology can also broaden the philosophical perspective regarding AI independence. Previously, AI was considered independent as long as it could perform its tasks based on previously implemented programs. However, today, AI is much more independent than that. AI can determine its own goals and targets and choose the best way to achieve them.[47]

It's important to understand that AI is a product developed and managed by humans. While AI can operate autonomously, it is still fundamentally dependent on humans. However, with increasingly rapid technological advancements, AI can now make informed decisions. The impact of AI technology is complex and unpredictable, even without direct human intervention. Therefore, appropriate regulations are needed to play a crucial role in ensuring that AI technology is used responsibly without harming public interests. With clear and firm regulations, oversight of AI use can be carried out more effectively, thereby minimizing its negative impacts. Furthermore, these regulations also provide legal certainty for AI developers and users in Indonesia, while ensuring that technological innovation does not neglect security aspects or individual rights. The existence of regulations on the prevention and handling of criminal acts by AI is the first step in the process of enforcing artificial intelligence, namely AI as a subject of criminal offenses.[48]

Regulations related to AI in Indonesia have not been specifically regulated, so an interpretation is needed to determine whether AI is a legal subject or not. Seen from the perspective of Indonesian law, if AI commits an unlawful act, it returns to the concept of criminal liability, namely that the legal subject, in this

[46] FL. Yudhi Priyo Amboro and Khusuf Komarhana, "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia [Prospects of Artificial Intelligence As a Subject of Civil Law in Indonesia]," *Law Review*, no. 2 (November 2021): 145, https://doi.org/10.19166/lr.voi2.3513.

[47] Eka Nanda Ravizki and Lintang Yudhantaka, "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia," *Notaire* 5, no. 3 (October 2022): 351–76, https://doi.org/10.20473/ntr.v5i3.39063.

[48] M Wildan Mufti et al., "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence," *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (2024), https://doi.org/https://doi.org/10.5281/zenodo.11422903.

case, is the human as the legal subject, because AI is ordered to do something according to the will of its creator. AI cannot do anything independently and requires human assistance to operate it in doing something. To be held criminally responsible, the legal subject must fulfill two elements: actus reus or the material element of a crime and mens rea or the subjective element of a crime. The subjective element of a crime requires the presence of error, either intentional or negligent.[49]

Based on Van Hamel's opinion, as quoted by Muhammad Tan Abdul Rahman Haris and Tantimin, the limitations in legal responsibility when associated with AI indicate that AI does not have an understanding of the consequences of its actions, cannot determine the will to carry out an act, and does not have awareness in acting legally. In the context of awareness, humans as legal subjects in criminal law can still commit negligence, but AI is only a tool created by humans, so it does not have the necessary awareness. Therefore, based on these limitations, AI does not meet the requirements to be considered a legal subject who can be held criminally responsible.[50]

In dealing with cyber crime, positive law in Indonesia is still arbitrary. Lex locus delicti. However, the situation and conditions of legal violations that occur due to cybercrime are different, where the perpetrator and victim are located in different locations. The vast yet easily accessible nature of cybercrime has led to a surge in crime. [51] In such conditions, the principlelex locus delicti becomes inadequate because it is unable to cover crimes that cross jurisdictional boundaries. Therefore, a more adaptive legal approach is needed through the principleextraterritorial jurisdictionto ensure that cybercriminals can still be held legally accountable even if they are outside of Indonesia.

Conclusion

Cyber law reform in Indonesia is an urgent need amid the increasing complexity of digital crime and the rapid development of information technology. Although Indonesia already has the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law as the basis for regulating cyberspace, both still exhibit fundamental weaknesses, such as norms subject to multiple

[49] S. Hardiyanti QAyunil, S Urrahman, and T Aurelia Rahim, "Kedudukan Dan Konsep Pertanggungjawaban Artificial Intelegence Dalam Hukum Positif Indonesia," *UNES Law Review* 6, no. 4 (2024): 12687–93.
[50] Muhammad Tan Abdul Rahman Haris and Tantimin Tantimin, "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 2022): 307–16, https://doi.org/10.23887/jkh.v8i1.44408.
[51] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Cakrawala Ilmiah* 2, no. 10 (June 2023): 3799–3806, https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

interpretations, reactive law enforcement, and a lack of harmonization between regulations and international standards. Institutional fragmentation and limited capacity of law enforcement officers also hamper effective law enforcement, resulting in suboptimal protection of citizens' digital rights and national security.

In addition, the emergence of artificial intelligence (Artificial Intelligence/AI) raises new legal challenges that have not yet been accommodated in national legal frameworks. The autonomous and adaptive nature of AI creates uncertainty regarding legal liability, while existing ethical guidelines lack normative force.lex locus delictiPositive law is also no longer sufficient to cover cross-border cyber crimes, so it is necessary to apply principles extraterritorial jurisdictionand stronger international cooperation to ensure perpetrator accountability. Therefore, cyber law reform must be directed at establishing a legal system that is adaptive, effective, and responsive to technological developments. Strategic steps needed include accelerating the ratification of the Cyber Security and Resilience Bill, harmonizing the ITE Law and the PDP Law, increasing digital law enforcement capacity, and drafting regulations. Specifically, AI should ensure accountability, transparency, and fairness. Comprehensive reforms will strengthen national resilience in the digital space while establishing a legal framework capable of protecting citizens' digital rights and encouraging responsible technological innovation.

In conclusion, cyber law reform in Indonesia requires not only regulatory updates but also a paradigm shift in understanding the relationship between law and technology. Law must act as a means of social engineering (law as a tool of social engineering) capable of directing digital development towards a just, safe, and equitable order. Integration of legal substance reform, institutional strengthening, increased digital literacy, and cross-sector collaboration is key to creating a resilient legal system in the cyber era. Therefore, cyber law reform is not merely a response to the threat of digital crime, but also a strategic step to ensure that technological progress in Indonesia goes hand in hand with human rights protection, legal certainty, and national resilience in the digital space.

Suggestion

The government needs to expedite the development and ratification of the Cyber Security and Resilience Bill (RUU KKS) as a comprehensive national legal basis for safeguarding digital sovereignty and national data security. Harmonization of the ITE Law, the PDP Law, and other sectoral regulations is essential to prevent overlapping norms and strengthen legal certainty. Furthermore, increasing the capacity of law enforcement officers through digital forensics training, strengthening inter-agency coordination institutions such as the National Cyber and Cyber Security Agency (BSSN), the Indonesian National Police (Polri), and the

Financial Services Authority (OJK), and establishing a recovery and compensation mechanism for victims of cybercrime must be national policy priorities. The government also needs to formulate specific regulations regarding artificial intelligence (AI) that address legal responsibility, accountability, transparency, and ethical use of technology. These regulations must be developed using a multidisciplinary approach involving academics, technology practitioners, and civil society to ensure a balance between innovation and human rights protection. Furthermore, increasing digital literacy and public legal awareness needs to be strengthened through ongoing educational programs, so that public participation in maintaining security and ethics in cyberspace can be effective. Targeted and inclusive cyber law reform is expected to create a national legal system that is adaptive, just, and responsive to the dynamics of the digital era.

References

Aabid, Muhammad, Tyas Dzaky, and Ibrahim Fikma Edrisy. "Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital." *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 12.

Amboro, FL. Yudhi Priyo, and Khusuf Komarhana. "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia [Prospects of Artificial Intelligence As a Subject of Civil Law in Indonesia]." *Law Review*, no. 2 (November 2021): 145. https://doi.org/10.19166/lr.voi2.3513.

Aprilianti, Astri. "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi." *Begawan Abioso* 15, no. 1 (January 2025): 41–50. https://doi.org/10.37893/abioso.v15i1.1002.

Br, Wahyudi. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI" 5 (2025).

BSSN. "Lanskap Keamanan Siber Indonesia 2024," 2024.

Budiman, Adhigama A, Genoveva Alicia K.S. Maya, Maidina Rahmawati, and Zainal Abidin. *Mengatur Ulang Kebijakan Tindak Pidana Di Ruang Siber: Studi Tentang Penerapan UU ITE Di Indonesia*. *Metode Penelitian*. Vol. 12, 2021.

Dinda, Adinda Lola Sariani. "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2, no. 2 (July 2024): 69–77. https://doi.org/10.58707/aldalil.v2i2.777.

Hakim, Hary Abdul, Chrisna Bagus Edhita Praja, and Sung Ming-Hsi. "AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia." *Jurnal Hukum Novelty* 14, no. 1 (April 2023): 122. https://doi.org/10.26555/novelty.v14i1.a25943.

Hardiyanti QAyunil, S., S Urrahman, and T Aurelia Rahim. "Kedudukan Dan Konsep Pertanggungjawaban Artificial Intelegence Dalam Hukum Positif Indonesia." *UNES Law Review* 6, no. 4 (2024): 12687–93.

Haris, Muhammad Tan Abdul Rahman, and Tantimin Tantimin. "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 2022): 307–16. https://doi.org/10.23887/jkh.v8i1.44408.

Hidayah, Nur Putri, Galih Wasis Wicaksono, Christian Sri Kusuma Aditya, and Yuda Munarko. "Artificial Intelligence and Quality of Composition Verdicts in Indonesia: Lessons from New Zealand." *Journal of Human Rights, Culture and Legal System* 4, no. 1 (February 2024): 101–20. https://doi.org/10.53955/jhcls.v4i1.175.

Jaya, Febri, and Wilton Goh. "Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia." *SUPREMASI HUKUM* 17, no. 02 (July 2021): 01–11. https://doi.org/10.33592/jsh.v17i2.1287.

Judijanto, Loso, and Budi Nugroho. "Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia." *Sanskara Hukum Dan HAM* 3, no. 03 (April 2025): 118–24. https://doi.org/10.58812/shh.v3i03.544.

Ketaren, Eliasta. "Cybercrime, Cyber Space, Dan Cyber Law." *Jurnal TIMES* 5, no. 2 (February 2017): 35–42. https://doi.org/10.51351/jtm.5.2.2016556.

Marita, Lita Sari. "Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia." *Cakrawala:Jurnal Humaniora Unievrsitas Bina Sarana Informatika* 15, no. 2 (2015). https://doi.org/https://doi.org/10.31294/jc.v15i2.4901.

Markus Djarawula, Novita Alfiani, and Hanita Mayasari. "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Cakrawala Ilmiah* 2, no. 10 (June 2023): 3799–3806. https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

Martinelli, Imelda, Yohana, Cora Venessa, and Eudora Joyce Hiumawan. "Urgensi Pengaturan Dan Perlindungan Rights of Privacy Terhadap Artificial Intelligence Dalam Pandangan Hukum Sebagai Social Engineering Imelda." *Jurnal Tana Mana* 4, no. 2 (2023): 158–66.

Martini Idris et al. "Regulation and Enforcement of Cyber Crime Law: Harmonization of the Revision of the ITE Law and the Criminal Code." *Lex Lata: Scientific Journal of Legal Science* 6, no. 3 (2024): 396–411. https://doi.org/https://doi.org/10.28946/lexl.v6i3.4266.

Maskun. *Kejahatan Siber (Cyber Crime)*. Jakarta: Kencana, 2013.

Mufti, M Wildan, M Hiroshi Ikhsan, Rafif Sani, and M Fauzan. "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence." *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (2024). https://doi.org/https://doi.org/10.5281/zenodo.11422903.

Muhammad Labib & Abdul Wahid. *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT. Refika Aditama, 2005.

Muin, F. "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi." *IDRIS: Indonesian Journal of Islamic Studies* 1, no. 1 (2023): 97–113.

Netipatalachoochote, Stanati, and Ludovic Pailler. "Developing Artificial Intelligence Legislation in Thailand: Lessons from the European Union." *Journal of Human Rights, Culture and Legal System* 5, no. 1 (March 2025): 1–32. https://doi.org/10.53955/jhcls.v5i1.424.

Rahman Najwa, Fadhila. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia." *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (January 2024): 8–16. https://doi.org/10.32520/albahts.v2i1.3044.

Ravizki, Eka Nanda, and Lintang Yudhantaka. "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia." *Notaire* 5, no. 3 (October 2022): 351–76. https://doi.org/10.20473/ntr.v5i3.39063.

Respati, Adhansonh Aqilla. "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *JURNAL USM LAW REVIEW* 7, no. 3 (2024): 1737–58. https://doi.org/https://doi.org/10.26623/julr.v7i3.10578.

Sa'bana, Sofia Mubarokah, and Rusdiana Navlia. "Penerapan Teori Fungsi Hukum Roscoe Pound: Soscial Engineering Di Indonesia." *Jurnal Jendela Hukum* 12, no. 1 (April 2025): 45–54. https://doi.org/10.24929/jjh.v12i1.4217.

Setiawan, Radita, and Muhammad Okky Arista. "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana." *Recidive* 2, no. 2 (2018): 139–46.

Siregar, Naek, Desy Churul Aini, Rehulina Rehulina, Agit Yogi Subandi, and Isroni Muhammad Miraj Mirza. "The Use of Artificial Intelligence in Armed Conflict under International Law." *Hasanuddin Law Review* 10, no. 2 (July 2024): 189. https://doi.org/10.20956/halrev.v10i2.5267.

Sitanggang, Andri Sahata, Fernanda Darmawan, and Dony Saputra. "Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan Dan Teknologi Indonesia* 4, no. 3 (September 2024): 79–83. https://doi.org/10.52436/1.jpti.409.

Situmeang, Sahat Maruli. *Cyber Law, International Law, Security, and Military Power*. Bandung: Cakra, 2025.

Suseno. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2012.