ISSN 2988-2125

Legal and Technological Aspects of Cybersecurity and Cyber Resilience in Facing Global Cyber Threats

Hassanain Haykal
Maranatha Christian University
E-mail: hassanain.haykal@law.maranatha.edu

The emergence of artificial intelligence has shifted cybercrime patterns in Indonesia from manual to automated and adaptive attacks. Deepfakes, adversarial machine learning, and automated social engineering have become powerful tools that can exploit vulnerabilities in computer systems, algorithms, and data in cyberspace. These threats pose significant dangers to critical sectors, particularly banking and digital public services, due to potential economic losses, data breaches, and violations of public privacy. This paper will focus on issues related to cybersecurity and cyber resilience from a legal and technological perspective in the face of global cyber threats. The methodology applied in this research includes normative juridical research using principles of law, systematic law, synchronous law, and comparative law. The results show that Indonesia has attempted to adapt to the country's legal structure through the enactment of Law No. 1 of 2024 on Information and Communication Technology (ITE), Law No. 27 of 2022 on Personal Data Protection (PDP), and the New Criminal Code No. 20 of 2025, which considers AI as an electronic agent. However, issues remain regarding digital evidence methods and changes in procedural law regarding autonomous AI agents. Traditional cybersecurity measures will not be able to combat AI attacks. Therefore, an integrated cybersecurity approach will be needed to protect against AI threats. This integrated cybersecurity approach will require the ratification of the Cybersecurity and Cyber Resilience Bill as an umbrella law to align PDP and ITE. Furthermore, this cybersecurity approach must include adaptive risk management, mandatory reporting to the BSSN (National Agency for the Protection of Information and Communications), SPBE audits, cybersecurity workforce development, a Pentahelix approach, and national data sovereignty.
Keywords: Artificial Intelligence, Cybercrime, Cyber Resilience, Regulation, Indonesia.

Corresponding Author:
Hassanain Haykal
Maranatha Christian University
hassanain.haykal@law.maranatha.edu

1. Introduction

Indonesia has now entered the era of Society 5.0. The goal of Society 5.0 is to create a human-centered society where economic development and social challenges can be addressed, and people can enjoy a high, active, and comfortable quality of life (Fukuyama, 2018). The key to achieving medium- and long-term growth is realizing Society 5.0, which addresses various social challenges by integrating the rapidly developing innovations of the Fourth Industrial Revolution (eg, IoT, big data, AI, robotics, the sharing economy, and so on) into every industry and social life (Shiroishi et al., 2018).

The era of Society 5.0 is marked by the emergence of advanced technologies such as cloud computing, the Internet of Things (IoT), and Artificial Intelligence. These technologies must be able to collaborate and coexist with humans to help simplify work and increase production efficiency (Roblek et al., 2020). Technology exists to coexist with humans, not replace them. The progress of human civilization in the modern era is also marked by the increasing development of science and technology, which makes human life more practical (Arber, 2009). Daily human activities are becoming more effective with the presence of tools derived from human intelligence. Developing technology is also increasingly diverse and complex (Alemayehu Tegegn, 2024).

One new technology currently widely used and developed is Artificial Intelligence (AI). AI is a term referring to the ability of machines to mimic human intelligence (Jarrahi et al., 2022). Simon defines AI as "artificial intelligence in the fields of research, application, and teaching related to programming computers to perform tasks considered intelligent by humans" (Sari & Harwika, 2022). It encompasses techniques and methods that enable computers to understand, learn, and make decisions based on provided data. For example, AI can understand human language commands, recognize faces, operate production machinery, and even drive vehicles automatically. Currently, AI has many functions and roles in human life, such as in education, services, healthcare, and others (Rangkuti, 2023).

There are two distinct types of AI (Etzioni & Etzioni, 2017; Rivis-Tipei, 2023). The first type of AI involves software that thinks and makes cognitive decisions similar to humans, potentially replacing them. The second type of AI simply provides intelligent assistance to humans. This type of AI requires machines to be better at making decisions than humans in specific areas, and they do so effectively within parameters set by humans or under their close supervision.

One example of an AI product that has gained widespread public acceptance is the GPT chatbot. GPT chatbots offer a variety of conveniences, with their core design including quick access to information, ease of maintenance, quality assurance, and extensibility (Li et al., 2020). According to data from Apptopia, downloads of AI chatbot apps increased by 1.506% in the first quarter of 2023, while revenue from in-app purchases increased by 4.184%, reaching nearly $3 million in March (Putra et al., 2023).

Despite the development and benefits of AI for humanity, its rapid development has raised concerns among AI experts regarding its potential impacts (Sihombing & Syahputra, 2020). In modern human life, AI has become an integral part, even capable of performing functions far superior to other tools. International debates show that AI can be favored to a double-edged sword. On the one hand, AI can be used for various positive purposes, but on the other hand, AI has the potential to threaten civilization if left unchecked (Gema 2022).

There are several impacts of AI use that must be considered. The first concern is the protection of intellectual property content from AI use. AI currently has the ability to automatically generate images or text from input commands or instructions, making it easier for people to create content. This threatens the sustainability of creative workers. The copyright aspect of AI has also been widely questioned (Andanni & Santoso, 2025). The second concern related to issues arising from AI is user privacy. Privacy relates to the use of data used to create AI models. The use of personal data, such as photos or videos, that violates privacy without the owner's consent is particularly concerning. Sensitive personal data can be highly detrimental to society (Yudhad et al., 2025).

The third concern is the potential for criminal cases arising from the use of AI. The misuse of AI has caused significant public unrest. An example is the deepfake phenomenon. The existence of deepfake technology demonstrates that the use of AI must be based on clear regulations. This technology can also cause public confusion and the spread of hoaxes (Kusnadi & Putri, 2025). A fourth concern is the possibility that AI will have the autonomous ability to create or perform actions without human intervention and based on its own will. AI's actions could then be categorized as legal. Because it can perform legal actions, AI's accountability is questionable (Sulistio & Salsabilla, 2023).

Currently, Indonesia has Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE). The ITE Law generally regulates electronic transactions, electronic system management, and the behavior of legal subjects in cyberspace (Sinaga & Lidya, 2024). The government, through the Ministry of Communication and Informatics, also issued Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 (SE Kominfo 9/2023) concerning

Artificial Intelligence Ethics. The purpose of this Circular Letter is to serve as an ethical guideline for (1) creating and formulating internal policies for companies, public sector electronic system operators, and private sector electronic system operators regarding data and internal ethics of artificial intelligence; and (2) implementing artificial intelligence-based consultations, analysis, and programming in accordance with statutory provisions (Simanjuntak et al., 2024).

In addition to AI developments, cybersecurity and cyberresilience are issues within the Cyber Law regime. Cybersecurity refers to protecting cyberspace from various threats and attacks that could damage information, and/or actions that cause damage and/or disruption to information infrastructure in any form. This security includes preventing hacking, data misuse, and other cyberattacks (Maesaroh, 2024). Meanwhile, cyberresilience focuses more on a system's ability to recover and resume normal operations after an incident or after experiencing a disruption and/or cyberattack. This includes appropriate recovery plans and readiness to address evolving threats. This concept differs from general physical security and defense, which relates to the protection of physical assets and infrastructure (Putri, 2021).

As outlined in the background, the research problem in this first year focuses on two main aspects. First, this research will examine how the development of artificial intelligence (AI) technology aligns with the current dynamics of cyber law in Indonesia. Second, this research focuses on formulating the ideal form of regulation to create a robust cybersecurity and resilience system in Indonesia. In line with the aforementioned research problem, this study specifically aims to comprehensively describe the development of AI and the implementation of cyber law in Indonesia. Furthermore, this study aims to conduct an in-depth analysis to identify the ideal regulatory framework to maintain security and enhance national cyber resilience.

2. Method

This research is a legal study using normative jurisprudence methodology and the characteristics of analytical descriptive studies. This study aims to explain and analyze relevant positive laws related to cybersecurity and resilience in Indonesia. The analytical descriptive method is used to systematically describe legal facts by connecting legislative, jurisprudential theory, and practices related to the development of cyber law and international cyber threats (Diantha, 2016). Furthermore, the effectiveness of relevant laws, including the Citizenship Law on Electronic Information and Transactions, the Government Regulation on Electronic Systems and Transactions, and other sectoral laws, will be analyzed in terms of their legal protection for cybersecurity and resilience.

This research is divided into two main parts: a literature review and field research. The literature review was conducted to collect secondary data from three categories of legal sources: primary, secondary, and tertiary legal materials. Primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Law Number 20 of 2025 concerning Criminal Procedure Law, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Secondary legal materials are collected from books, scientific articles, research results, expert opinions, and data from relevant agencies, namely the Ministry of Communication and Digital and the National Cyber and Cryptography Agency. Tertiary legal materials are taken from the internet, mass media, encyclopedias, and other relevant references..

This study not only involved a literature review, but its methodology was also further strengthened by fieldwork involving interviews with knowledgeable individuals in the field of cybersecurity, such as experts,

academics, lawyers, government officials, and relevant authorities, particularly the Ministry of Communication and Digital and the National Cyber and Cryptography Agency. The interviews were conducted in a structured and semi-structured manner, allowing researchers to obtain detailed information regarding the implementation of regulations, cyberspace oversight, and the difficulties in creating regulations for cybersecurity and resilience in Indonesia. The data collected from the interviews were then analyzed using qualitative legal methods, meaning the analysis was conducted based on legal aspects without the aid of statistics, with a focus on legal norms, positive law, and legal theory (Creswell & Poth, 2018) .

3. Results And Discussion

The Development of Artificial Intelligence and the Dynamics of Cyber Law in Indonesia

The last decade has witnessed a dramatic shift in the nature of digital security in Indonesia due to the widespread implementation of AI technology among criminals. The period between 2024 and 2026 witnessed a major shift in cybercrime trends, expanding beyond attacks on technical systems to exploiting human psychological triggers with great precision. One such trend is illustrated by the increasing sophistication and difficulty of identifying various types of cybercrime using traditional methods, as AI technology is used for automated monitoring, malware training, and highly customized phishing attempts (Rustiyana et al., 2025).

Among other major threats to Indonesia's national security, one major concern is digital identity manipulation using deepfake technology, which could potentially be used against celebrities and the general public for fraudulent purposes. Deepfakes allow attackers to fake highly realistic videos or impersonate people close to the victim using their voices (voice cloning), which helps trick victims into sending money or sharing personal information (Kristiyenda et al., 2025). Available data shows that these AI-based attacks are much more successful than phishing, posing a significant risk of financial losses to Indonesia, including losses that could exceed IDR 3.2 billion by 2024 (Tempo.co, 2024). Furthermore, one characteristic of this evolving crime model is the development of AI-based attacks that exhibit autonomous and adaptive behavior, implying that conventional cybersecurity measures are often unable to detect threats directly. Currently, attackers can easily "subscribe" to AI-based cybercrime services such as GPT Fraud or GPT Worm online via the dark web.

The evolution of cyber threats in Indonesia reached a critical point in 2024 and 2025, marked by a surge in massive data breaches due to machine learning-based attacks. According to the Awang Long Law Review, more than 30 large-scale data breaches were discovered, indicating a shift in the approach to attacks, shifting from simple phishing attacks to complex AI attacks using malicious machine learning manipulation (Rumbruren & Watofa, 2025). In such situations, perpetrators engage in data poisoning, manipulate datasets used in training, and employ model inversion and membership inference attacks, allowing them to gain access to personal information directly from AI logic. The adoption of agent-based AI that enables autonomous attacks not only poses an increased threat to privacy but also causes significant economic losses at the national level (Dwiandari, 2024).

In addition to cyberattacks on data sets, cybercrime in Indonesia has now expanded to the use of AI-based ransomware targeting financial institutions with alarming precision. Unlike static ransomware, this AI-based malware variant can automatically scan for security flaws, encrypt data on the fly, and modify code during the infection process to evade detection by conventional antivirus programs (Khang, 2025). Because financial institutions handle highly sensitive liquid assets and transaction data, ransomware attacks are typically accompanied by tactics involving double extortion, where the perpetrator not only locks the system

but also threatens to publicly release customer information if the ransom is not paid. This phenomenon is creating unprecedented pressure on the banking industry nationwide, given how quickly AI software can penetrate vital infrastructure in seconds, forcing the industry to adopt zero-trust security systems .

Cyberattacks driven by Artificial Intelligence (AI) are one of the latest developments in which criminals utilize artificial intelligence. The entire attack cycle is automated, from the scanning phase to exploiting vulnerabilities in the system, meaning no human involvement is required at any point in time. Unlike manual attacks, which are limited by human speed, this type of cyberattack can operate non-stop, 24/7, searching for security vulnerabilities among millions of targets simultaneously and responding instantly to defense efforts made by security systems. This advantage is due to its adaptive capabilities, where the attacker's algorithm can "learn" from past failures to modify the attack code to evade detection by traditional security software on the target system (Guembe et al., 2022). In Indonesia, cyberattacks using this technology have posed serious challenges to critical infrastructure and enterprises due to its ability to conduct extremely fast brute-force attacks, more intelligent botnets, and disguise its attack data to make it appear as if it were legitimate user activity. This necessitates the implementation of equally capable AI-based defense systems.

Phishing and social engineering techniques have reached such a high level of sophistication that the use of AI in psychological manipulation can be achieved on a mass scale. However, it still feels highly personalized. With the help of algorithms in Large Language Models (LLMs), cybercriminals behind such crimes can generate thousands of fraudulent email messages without grammatical errors that appear highly convincing and are automatically tailored to the victim's culture, status, or interests. Furthermore, the integration of deepfake technology with voice and video has become possible, enabling the automation of fraudulent phone calls or even video conference calls, making it difficult to distinguish the real from the fake, leading to attacks with robotic, seamless "spear-phishing" schemes (Tiara & Basyarudin, 2026). In Indonesia, such schemes tend to exploit leaks of personal data to quickly build trust and have AI send malicious links or request money transfers at opportune moments, effectively undermining human defenses and triggering systemic security failures long before technical systems can detect the anomaly.

Table 1 Development of AI-Based Cybercrime Modes in Indonesia

Crime Mode	Short Description	Main Techniques	Main Impact
Adversarial Machine Learning	Directly attack the logic and data sets of the target AI system.	Data Poisoning, Model Inversion, Membership Inference.	Leakage of sensitive personal data and damage to the integrity of AI decision-making systems.
AI-Generated Ransomware	Malware capable of locking data has mutated to evade antivirus.	Lightning-fast automatic encryption and adaptive (polymorphic) code.	Paralysis, operational institutions, finance, and blackmail, double blackmail.
AI-Driven Cyber Attacks	24/7 non-stop automated security vulnerability search attacks.	Intelligent botnets, automated vulnerability scanning, and adaptive brute force attacks.	Infiltration infrastructure is critical on a large scale at a speed that exceeds human response capabilities.
Phishing & Social Engineering Automation	Mass personalization psychology fraud.	Deepfake (voice/video) and LLM (Large Language Models) for persuasive messages.	Defenses are collapsing, human firewalls are thriving, and identity fraud is incredibly convincing.

The shift in AI-powered crime modes – a direct link – has shifted cyber law in Indonesia from a reactive to a proactive and multidimensional approach. The emergence of threats such as adversarial machine learning

and agent-based AI presents what can be called a legal "gap" due to the inherent challenges of using conventional law to define criminal liability where attacks are carried out without explicit human command, with only algorithms acting on them. This has created an urgent call for a broader legal interpretation regarding issues such as "malicious intent" (mens rea) and legal entity in autonomous digital environments. The rapid adaptation to the misuse of AI technology is marked by a shift from the lack of a specific normative framework to increased risk-based regulation. Despite lacking an AI law, Indonesia is updating its cyber umbrella law in conjunction with the New Criminal Code.

Indonesia's dynamic cyber law has evolved beyond mere regulation to become an adaptive law that responds to technological autonomy. From Law No. 11 of 2008, amended by Law No. 19 of 2016, and now highlighted in Law No. 1 of 2024, a paradigm shift in the way the law is viewed is evident. Previously, when the law focused solely on manual human actions, Indonesian law has now evolved to recognize the existence of "Electronic Agents" that can have legal consequences. There has been a transition from a lack of personal accountability to a lack of systematic response, and those who organize or develop algorithmic systems are now held accountable for any anomalies (Jumantoro, 2024).

This dynamic of sharpness is evident in the law's ability to encompass crimes not covered by existing laws. This is a clear human footprint at every stage. Since the introduction of the concept of AI into the category of electronic agents, the gap left by laws used to address human criminals has been filled. The latest ITE law emphasizes transparency and risk mitigation (security by design), which puts pressure on digital industry players to act ethically and with security in mind. This legal dynamic is seen not simply as a barrier to innovation, but as a guardian of digital sovereignty capable of manipulating sophisticated techniques like deepfakes.

Furthermore, the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) marks the beginning of intelligent governance in Indonesia, where data processing for machine learning is now governed by very strict laws that prevent the exploitation of sensitive data. The law requires all AI developers—both individuals and corporations—to have a valid legal basis before they can use personal data as their training datasets, such as an explicit agreement with the data subject or fulfilling contractual obligations. This tightening of regulations is based on the principle of "purpose limitation," where data collected for one purpose cannot be automatically "given" to another AI algorithm without additional permission, thereby closing a gap in preventative practices in automated intelligence that could violate citizens' privacy rights.

In the case of contextual machine learning involving large-scale data, the Personal Data Protection Act (PDPA) requires a shift in focus from simply collecting raw data to proper data management, including conducting an Impact Assessment under the Personal Data Protection Act (DPIA). Data controllers must conduct a risk assessment before implementing new technologies, as there are potential risks involved, especially if they involve automated decision-making that could significantly impact individuals. This is crucial to avoid the misuse of sensitive data such as medical records, biometrics, or even criminal records, which are often targets of adversarial attacks.

From a legal perspective, the power of the Personal Data Protection (PDP) Law is demonstrated by the possibility of imposing severe penalties on perpetrators of data processing violations, including fines of hundreds of billions of rupiah and imprisonment for any individual who intentionally manipulates personal information without their consent. The existence of such a law creates a healthier digital environment for the development of artificial intelligence in Indonesia because it forces companies to implement international security standards such as the GDPR in their technological infrastructure. By creating a supervisory body directly responsible to the President, the PDP Law ensures that national data sovereignty

 ISSN 2988-2125

remains active amidst the storm of automation, providing real legal protection to data subjects amidst the rise of artificial intelligence systems.

The issuance of Law Number 20 of 2025 concerning the new Indonesian Criminal Code (KUHP), recently ratified by President Prabowo Subianto on December 17, 2025, is seen as a drastic response to the stalemate of the old legal procedures used to address current types of crimes. The new law, which will come into effect on January 2, 2026, represents a drastic shift in the justice paradigm in Indonesian criminal law, shifting from a repressive-formalistic law to a more human rights-oriented one through the application of legal principles. In the context of crimes committed using AI-controlled cyberspace, the 2025 KUHP clearly defines the process by which suspect decisions and wiretapping become part of an effort to enforce compliance with strict judicial oversight.

The most important aspect of the new Criminal Code is that it introduces an innovative judicially supervised system of confession and admission of guilt, allowing for expedited trial procedures because the suspect has voluntarily admitted their guilt before the justice system. This innovation is crucial in addressing the growing number of cybercrime cases where the technical aspects of proof are highly complex, without compromising the substance of justice. Furthermore, the 2025 Criminal Code enhances the strength of the pre-trial phase by requiring at least two valid methods of evidence to determine a suspect.

The dynamics of cyber law in the 2025 Criminal Procedure Code are also demonstrated through the statement regarding the Public Prosecutor's role as dominus litis, having full control over matters of merit, thus preventing the possibility of "automatic" prosecutions arising from investigations without strict normative filters. Currently, there are provisions in the law regarding the granting of judicial pardons in certain cases, demonstrating the humanistic approach to justice in this newly formed country. The combination of technology involving digital forensics allows Indonesia to have procedural law that can balance the speed of handling cybercrime cases automatically and guarantee justice for all parties involved.

The implementation of the above law is supported by numerous technical derivative regulations. To ensure the law remains relevant in its application amidst technological advances, the following details the derivative regulations in the dynamics of cyber law in Indonesia: Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PTTP): This regulation is a very important implementing regulation in the context of the Information Technology Law, which regulates the governance of electronic systems, the placement of data centers in Indonesia in the public sector, and the removal of illegal content, including that generated by AI.

Table 2 Cyber Legal Framework in Indonesia

Legal Instruments	Focus & Role	AI Threat Dynamics
ITE Law No. 1 of 2024 (Second Amendment)	Manage agent information, transactions, and electronic devices.	Define AI as an “Electronic Agent”; the owner/PSE is fully responsible for the algorithm’s results (such as deepfakes).
PDP Law Number 27 of 2022	Personal data protection and data processing governance.	Requires a DPIA (Data Protection Impact Assessment) for machine learning to prevent exploitation of sensitive data.
Criminal Procedure Law Number 20 of 2025	Criminal procedural law procedures (effective from January 2026).	Strengthening digital evidence standards and introducing a Judicially Supervised Guilty Plea mechanism for efficiency in cyber cases.
Government Regulation Number 71 of 2019 (PSTE)	Electronic implementation and transaction systems.	Regulates the technical obligations of PSEs in the registration system and content filtering mechanisms (including infringing AI content).

Strong Cybersecurity and Cyber Resilience Regulatory Model in Indonesia

An ideal legal system is not a rigid system and does not only involve formalistic law enforcement, but must have the ability to adapt to changes in society and technological advances without losing its substantive justice characteristics (Nonet et al., 2017). In facing the ever-present threat from cyberspace in the form of artificial intelligence-based technology, the need for responsive law demands that authorities in Indonesia view the regulatory framework not as a set of unchanging texts, but as a dynamic instrument capable of meeting the needs of society to feel safe in cyberspace.

The application of law, which is flexible within the context of a regulatory approach, requires openness to feedback from all parties to bridge the gap between the speed of technological innovation and the force of law. Nonet and Selznick point out that law must function as a tool to achieve social goals; in this case, the social goal is to achieve digital sovereignty and national resilience in cyberspace. Therefore, laws such as the Information Technology Law and the Personal Data Protection Law cannot be considered final products, but require further review and amendment as technology evolves.

Optimal cybersecurity and resilience in Indonesia must evolve from mere administrative compliance to resilience through an adaptive operational perspective. This paradigm shift requires organizations to not only build robust defenses but also have the capacity to detect, respond to, and restore service delivery during intelligent attacks by artificial intelligence. Implementing a Zero Trust framework and real-time threat detection using AI-based regulations will ensure the country's digital infrastructure has sufficient agility to mitigate the impact of disruptions on service delivery and the country's economic stability.

Furthermore, optimal cyber resilience relies heavily on cross-sector collaboration, encompassing contributions from government, industry, and academia to create a cyber defense community. Mandatory regulations require standardization of dynamic risk management processes, requiring every agency to conduct attack simulations (red teaming) and technology audits. To address the evolving machine learning capabilities of adversaries, through policy harmonization that encourages transparency in reporting incidents without fear of repercussions, Indonesia will be able to build a threat intelligence database based on strong national synergy. The following are the main components in building a robust cybersecurity ecosystem in Indonesia:

1. Comprehensive Regulatory Framework
   The ideal model requires harmonious laws that cover all aspects to eliminate overlapping regulations.
   a. Cyber Security and Resilience Bill
      The Cyber Security and Resilience (KKS) Bill was created as a general umbrella regulation to unify various existing regulations that were scattered across various ministries and agencies. The bill largely focuses on enhancing the capacity of regulatory agencies, such as granting the National Cyber and Information Agency (BSSN) the authority to respond to threats at the national level. Under this law, Indonesia will have its own legal framework to protect Vital Information Infrastructure (VIT) in sectors such as energy, transportation, finance, and others from potential digital attacks. However, there may be some challenges in drafting this regulation, as it could lead to overlapping authorities among various agencies. According to LAB 45, the bill has sparked discussions about the division of roles between the BSSN, the Ministry of Communication and Information, and law enforcement agencies such as the police. Furthermore, as critics at Kompas.id have suggested, the regulation should not conflate civil security and military defense. Therefore, it should focus more on proportional individual protection.
   b. Optimization of the PDP Law & ITE Law
      The importance of optimizing the Personal Data Protection (PDP) Constitution is significant because Indonesia needs this law to align with the European Union's General Data Protection

Regulation (GDPR). The continued implementation of the GDPR Law ensures that all parties, both public and private, cannot provide full accountability for the data they manage. This law creates a sense of security for foreign investors and digital service users, as there will always be administrative and legal sanctions for negligent parties in the event of a data breach. At the same time, the synergy between the PDP and the Information Technology Law is crucial in providing a strong legal basis for criminalizing cybercrime. While the PDP focuses on governance and privacy protection, the PDP acts as a law enforcement tool against illegal activities, such as hacking, the spread of fake news, and online fraud. By optimizing both constitutions, Indonesia can create a digital space that not only fulfills human rights but also prevents the state from exploiting economic crimes.

c. Technical Standardization

The implementation of international standards such as ISO 27001 is a concrete step to ensure that organizations in Indonesia have a measurable Information Security Management System (SISM). Compliance with this standard requires organizations to conduct regular risk assessments and implement stringent security measures in their digital infrastructure. This is crucial to ensure uniform information security quality across industry sectors, thereby ensuring the national digital supply chain is relatively resilient to cyberattacks. In addition to ISO, the implementation of the NIST Cybersecurity Framework is highly recommended to help organizations develop the ability to detect and recover from any attack. This framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover. By adopting this framework, an organization not only emphasizes attack prevention but also has specific protocols for handling any incidents, enabling rapid recovery from operational disruptions.

2. Cyber Resilience Strategy

Cyber resilience is not just about prevention, but also the ability to “learn” from failure.

a. Adaptive Risk Management

Adaptive Risk Management is a dynamic approach that recognizes that cyber threats are constantly evolving, so defense mechanisms are not static. Its primary focus is 24/7 centralized monitoring through a Security Operations Center (SOC) to detect anomalous behavior in the network as early as possible before it escalates into a large-scale attack. With regular evaluations, organizations can update their security measures according to the latest threats, ensuring they are not only able to withstand attacks from legacy methods but also ready to defend against new hacking techniques. Furthermore, another important aspect of risk management here is its simultaneous predictive and preventative nature. Continuous security audits are conducted to enable organizations to identify any vulnerabilities in their infrastructure before external parties exploit them as opportunities. By integrating threat intelligence into its monitoring system, Indonesia can create a digital environment that can react and adapt to any cyber conflict that occurs globally.

b. Mandated Incident Reporting

The Incident Reporting Mandate to the National Cyber and Cryptography Agency (BSSN) serves as an early warning system for the country. When an organization is required to report an attack, the agency can understand attack patterns and notify other parties who may be affected by the same threat. In this regard, this procedure helps avoid sectoral egoism and creates a "digital community" of "immunity," where the failure of one system serves as a valuable lesson for everyone across the national infrastructure. In addition to coordination between technical systems, the mandatory reporting procedure is also intended to ensure transparency in the

process and accountability to the public. Without a clear reporting mandate, most organizations end up hiding information about data breaches to protect their reputations.

c. Periodic Audit

Conducting regular audits on the Government Electronic System (SPBE) is a crucial step to ensure that system services remain safe and secure for the public. Security due diligence includes comprehensive audits to check the integrity, encryption, and resilience of government servers to handle heavy workloads. Through continuous audits, every government agency will be forced to maintain its service quality standards, as potential system failures could halt bureaucratic processes. Reliability testing is another way the government can ensure its technology investments are not wasted and are fully secure. Given the large amount of sensitive information citizens store on SPBE, regular audits serve as a mechanism to ensure compliance with state security protocols.

3. Supporting Pillar Ecosystem

Implementing regulations will not be effective without support from non-technical aspects in accordance with applicable guidelines.

a. Pentahelix Collaboration

Human resource development requires time and effort to bridge the gap between industry needs and available expertise in cybersecurity. This program considers not only the number of graduates in this technology field but also the expertise gained in specific skills through certifications such as the CISSP or CEH. By having its own certified experts, organizations ensure that security systems are operated by individuals who understand ethical security measures and engineering mitigation techniques. Beyond formal methods, another important goal is to empower human resources to increase cybersecurity literacy among the general public, which will help minimize the risk of social engineering attacks. Cybersecurity education from an early age will produce a future generation that is aware of potential dangers such as phishing or identity theft. Furthermore, human resources are needed to successfully implement any type of regulation, as the human error factor will remain the biggest security gap.

b. Human Resource Development

Investing in human resource development requires a long-term approach to bridge the gap between industry demand and the supply of cyber experts. Training programs should focus not only on increasing the number of IT graduates but also on enhancing their skills through international certifications such as the CISSP and CEH. Organizations can ensure that their systems are managed by trained professionals knowledgeable in cybersecurity ethics and countermeasure engineering. Beyond formal channels, organizations should also invest in human resources to increase public cybersecurity literacy to mitigate social engineering-based attacks. Cybersecurity education in schools from an early age will produce a generation aware of cybersecurity threats such as phishing and identity theft. Human resource development plays a crucial role in the implementation of any regulation, regardless of its sophistication, as human error remains the weakest link in cybersecurity.

c. Data Sovereignty

Data sovereignty centers on a country's ability to control and protect its citizens' data within its territory, given the vast volume of information that crosses borders during regulatory processes. This will ensure that sensitive data created in Indonesia is regulated according to standard protocols within the national domain, even if stored in international cloud storage systems. This is crucial to prevent data exploitation by foreign parties that could pose a threat to Indonesia's economic and national security, while also providing legal certainty for electronic system

 ISSN 2988-2125

administrators regarding data boundaries. Furthermore, data management must be balanced with the principle of openness in the digital economy to avoid stifling innovation. Ideally, data sovereignty in Indonesia should emphasize data localization for critical information infrastructure while still allowing international data movement under strict agreements.

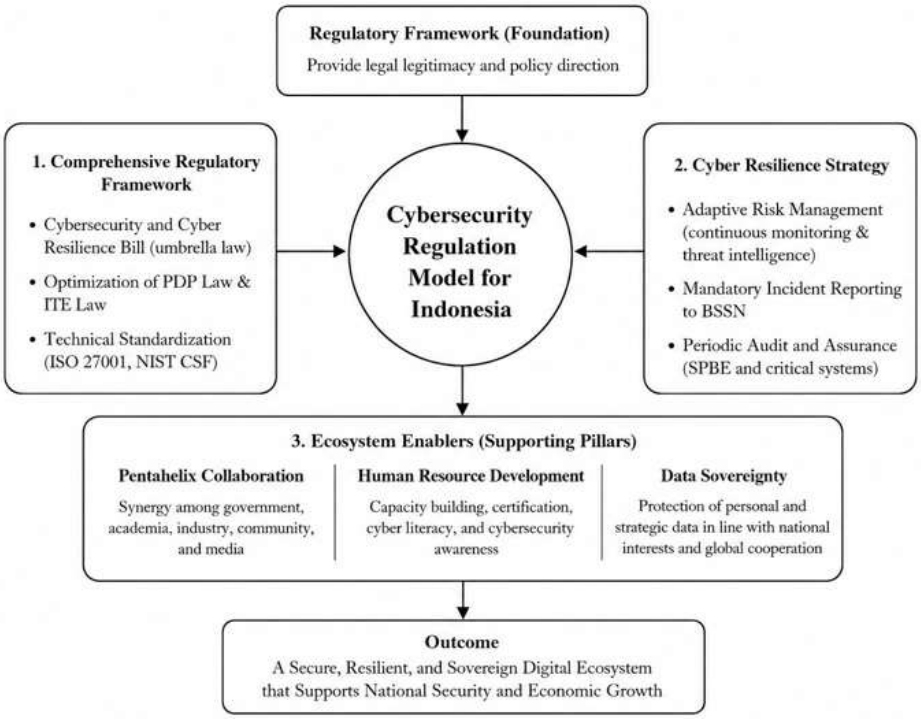

Figure 1 Cybersecurity Regulatory Model for Indonesia

4. Conclusion

The findings of this study indicate that the use of AI has brought about a paradigm shift in the digital crime environment in Indonesia, from unsystematic manual attacks to highly systematic, automated attacks based on AI technology. With the rise of adversarial machine learning, deepfake manipulation, and automated social engineering techniques, it can be said that digital threats have become adept at identifying weaknesses in logical systems and data sets, rather than simply targeting network infrastructure. There is a significant systemic risk associated with this phenomenon, especially for critical industries such as financial companies and public data controllers. From a legal perspective, the development of cyber laws in Indonesia, including Law No. 1 of 2024 on Information Technology, Law No. 27 of 2022 on Personal Data Protection, and Law No. 20 of 2025 (the New Criminal Code), shows a positive trend through the definition of AI as an "Electronic Agent." However, the effectiveness of these laws still faces obstacles due to issues with digital evidence and the speed of adaptation of procedural law to autonomous algorithms. From the perspective of Routine Activity Theory and Technological Criminology, it is clear that defense against new threats cannot be achieved solely through traditional methods (guards), but must also include technology, acting as a "digital guard" (capable guard). The ideal framework for regulation and resilience against cyber threats in Indonesia is a holistic ecosystem involving legal, technical, and social factors through the enactment of the Cyber Security and Resilience Bill as a comprehensive law. This is primarily achieved through the harmonization of the Personal Data Protection (PDP) Law and the Information and Communication Technology (ITE) Law. Essentially , this model will emphasize proactivity and adaptability in terms of risk management, with requirements for incident reporting through centralization at the BSSN (National Agency for the Protection of National Data) and regular audits by the SPBE (National Agency for

the Protection of National Data). Achieving this goal relies heavily on the synergy between Pentahelix collaboration, expert human resource development, and data sovereignty. In this way, the country will not only be able to fend off cyberattacks but also ensure resilience, thereby guaranteeing national security.

5. References

Alemayehu Tegegn, D. (2024). Peran ilmu pengetahuan dan teknologi dalam merekonstruksi sejarah sosial manusia: pengaruh perubahan teknologi terhadap masyarakat. *Ilmu Sosial Cogent* , *10* (1), 2356916.

Andanni , AP, & Santoso, B. (2025). Perlindungan Hukum Terhadap Pelanggaran Karya Cipta yang Dihasilkan Melalui AI dan dikomersilkan Berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* , *5* (3).

Arber, W. (2009). Dampak ilmu pengetahuan dan teknologi terhadap peradaban. *Kemajuan Bioteknologi* , *27* (6), 940-944.

Creswell, JW, & Poth, CN (2018). *Penyelidikan Kualitatif dan Desain Penelitian: Memilih di Antara Lima Pendekatan (edisi ke-4).* Thousand Oaks, CA: SAGE Publications.

Diantha, IMP (2016). *Metodologi penelitian hukum normatif dalam pembenaran teori hukum* . Prenada Media.

Dwiandari , AS (2024). Tantangan hukum kejahatan siber berbasis AI di Indonesia. *Jurnal Studi Hukum Indonesia, 9* (2), 145–162.

Etzioni, A., & Etzioni, O. (2017). Mengintegrasikan etika ke dalam kecerdasan buatan. *Jurnal Etika* , *21* (4), 403-418.

Fukuyama, M. (2018). Masyarakat 5.0: Menuju masyarakat baru yang berpusat pada manusia. *Sorotan Jepang* , *27* (5), 47-50.

Gema, AJ (2022). Masalah Penggunaan ciptaan sebagai data masukan dalam pengembangan kecerdasan buatan di Indonesia. *Jurnal Hukum Teknologi dan Ekonomi* , *1* (1), 1.

Guembe , B., Azeta , A., Misra, S., Osamor , VC, Fernandez-Sanz, L., & Pospelova , V. (2022). Ancaman yang muncul dari serangan siber berbasis AI : Sebuah tinjauan. *Kecerdasan Buatan Terapan* , *36* (1), 2037254.

Jarrahi , MH, Lutz, C., & Newlands, G. (2022). Kecerdasan buatan, kecerdasan manusia dan kecerdasan hibrida berdasarkan peningkatan timbal balik. *Big Data & Society* , *9* (2), 20539517221142824.

Jumantoro , TRP (2024). Menilik Pro dan Kontra Pemanfaatan dan Penetapan Status Hukum Artificial Intelligence (AI) dalam Hukum Positif Indonesia. *Jurnal Penelitian Analitik, Statistika dan Komputasi* , *3* (1).

Khang, A. (Ed.). (2025). *Keamanan Siber Berbasis AI untuk Perbankan dan Keuangan: Cara Meningkatkan Keamanan, Melindungi Data, dan Mencegah Serangan* . CRC Press.

Kristiyenda , YS, Faradila , J., & Basanova , C. (2025). Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang. *ALADALAH: Jurnal Politik, Sosial , Hukum Dan Humaniora* , *3* (2), 149-164.

Kusnadi , SA, & Putri, DWS (2025). Perlindungan hak privasi dalam a teknologi deepfake di indonesia. *Jurnal Rechtsvinding : Media Pembinaan Hukum Nasional* , *14* (2).

Li, Y., Grandison, T., Silveyra, P., Douraghy , A., Guan, X., Kieselbach, T., ... & Zhang, H. (2020, Juli). Jennifer untuk COVID-19: Chatbot bertenaga NLP yang dibangun untuk masyarakat dan oleh masyarakat untuk memerangi misinformasi. Dalam *Lokakarya ACL 2020 tentang Pemrosesan Bahasa Alami untuk COVID-19 (NLP-COVID)* .

Maesaroh , RS (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan : Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht : Jurnal Hukum Kenegaraan Dan Politik Islam* , *4* (2), 255-274.

Putra, GA, Taniady , V., & Halmadiningrat , IM (2023). Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Perlindungan Hukum Terhadap Penggunanya . *Jurnal Rechtsvinding : Media Pembinaan Hukum Nasional* , *12* (2).

Putri, KVK (2021). Kerja Sama Indonesia dengan ASEAN Mengenai keamanan siber dan ketahanan siber dalam Mengatasi kejahatan dunia maya . *Jurnal Hukum Lex Generalis* , *2* (7), 542-554.

Rangkuti , M. (2023). Mengenal kecerdasan buatan (AI): Pengertian , sejarah , kegunaan , dan contoh penerapannya . *Artikel Dan Berita Opini, Teknologi* .

Riviș-Tipei , I. (2023). Pertimbangan etis dalam pengembangan dan penerapan kecerdasan buatan. *SCIENTIA MORALITAS-International Journal of Multidisciplinary Research* , *8* (2), 13-26.

Roblek, V., Meško, M., Bach, MP, Thorpe, O., & Šprajc , P. (2020). Interaksi antara internet, pembangunan berkelanjutan, dan munculnya masyarakat 5.0. *Data* , *5* (3), 80.

Rumbruren , A., & Watofa , Y. (2025). Analisis Tanggung Jawab Penyelenggara Sistem Elektronik dalam Kasus Pelanggaran Data. *Jurnal Hukum Awang Long* , *7* (2), 481-491.

Rustiyana , R., Judijanto , L., Supartha, IKDG, & Gunawan, PW (2025). *Pemanfaataan AI dalam Keamanan Siber* . PT. Sonpedia Penerbitan Indonesia.

Sari, AP, & Harwika , DM (2022). Tanggung jawab hukum kecerdasan buatan dalam perspektif hukum perdata di Indonesia. *Jurnal Internasional Penelitian dan Tinjauan Ilmu Sosial* , *5* (2), 57-60.

Shiroishi, Y., Uchiyama, K., & Suzuki, N. (2018). Masyarakat 5.0: Untuk keamanan dan kesejahteraan manusia. *Komputer* , *51* (7), 91-95.

Sihombing , EN, & Syaputra , MYA (2020). Implementasi Penggunaan Ini buatan dalam pembentukan peraturan daerah . *Jurnal Ilmiah Kebijakan Hukum* , *14* (3), 419-434.

Simanjuntak, W., Subagyo , A., & Sufianto , D. (2024). Peran pemerintah dalam implementasi kecerdasan buatan (ai) di kementerian komunikasi dan informatika republik Indonesia (kemenkominfo) ri). *Jurnal Penelitian Sosial dan Ekonomi* , *6* (1), 1-15.

Sinaga, D., & Lidya, I. (2024). Perlindungan Hukum Dan Pertanggungjawaban Tindak Pidana Revenge Porn Berdasarkan UU No. 11 Tahun 2008 Tentang Informasi Transaksi Elektronik (ITE) Dan UU No. 12 Tahun 2022 Tentang Tindak Pidana kekerasan Seksual (TPKS). *Tinjauan Hukum Padjadjaran* , *12* (1), 32-45.

Sulistio, F., & Salsabilla , AD (2023). Pertanggungjawaban pada Tindak Pidana yang Dilakukan Agen Otonom Artificial Intelegence . *Tinjauan Hukum Unes* , *6* (2), 5479-5490.

Tempo.co (2024). Deepfake Politik dan Penipuan Digital Meningkat Jelang Pemilu.

Tiara, A., & Basyarudin, B. (2026). Penyalahgunaan Teknologi Artificial Intelligence (Ai) Sebagai Modus Baru Kejahatan Penipuan Digital Dalam Perspektif Hukum Pidana Di Indonesia. *Legis Nexus: Jurnal Ilmu Hukum* , *1* (1), 17-22.

Yudha , MW, Ramli, AM, & Ramli, TS (2025). Penggunaan Data Pribadi Sebagai Sarana Pelatihan Kecerdasan Buatan: Studi Komparatif Perlindungan Hak Privasi Di Indonesia Dengan Uni Eropa. *Penyebab: Jurnal Hukum dan Kewarganegaraan* , *12* (7), 61-70.