JURISPRUDENSI
Jurnal Ilmu Syari'ah, Perundang-undangan dan Ekonomi Islam
https://doi.org/10.32505/jurisprudensi.v17i1.10612
Vol. 17 No. 1 (Februari-Juni 2025): 206-223

The Existence and Regulation of Cyber Law: The Government's Role in Combating Digital Crime in Indonesia

Auliaurrahman[1]
Universitas Samudera Langsa, Aceh, Indonesia
auliaurrahman@unsam.ac.id

Nur Anshari
IAIN Langsa, Aceh, Indonesia
nuranshari@iainlangsa.ac.id

Sunny Ummul Firdaus
Universitas Sebelas Maret, Surakarta, Indonesia
firdaussunny@yahoo.com

Submission	Accepted	Published
Dec 31, 2024	Mar 7, 2025	Mar 8, 2025

Abstract

Ideally, cyber law regulations in Indonesia should provide comprehensive protection against digital crime in line with the rapid development of information technology. However, in reality, the existing regulations still face various challenges in law enforcement and have not fully succeeded in reducing the increasing rate of digital crime. This study aims to analyze the existence and effectiveness of cyber law regulations in Indonesia and evaluate the role of the government in combating digital crime. This research employs a qualitative approach with a literature review method, involving descriptive analysis and a comparative study between Indonesian cyber regulations and international regulations. The findings indicate that although Indonesia has an adequate legal basis through the Electronic Information and Transactions Law (UU ITE), its implementation remains ineffective due to infrastructure limitations and lack of inter-agency coordination. Furthermore, a comparison with international regulations reveals the need for revision and policy strengthening to enhance national cybersecurity.

Keywords: *Government Regulation, Cyber Law, Digital Crime.*

[1] Corresponding Author

Abstrak

Idealnya, regulasi hukum siber di Indonesia mampu memberikan perlindungan yang komprehensif terhadap kejahatan digital seiring dengan pesatnya perkembangan teknologi informasi. Namun, realitasnya, regulasi yang ada masih menghadapi berbagai tantangan dalam penegakan hukum dan belum sepenuhnya mampu menekan angka kejahatan digital yang terus meningkat. Penelitian ini bertujuan untuk menganalisis eksistensi dan efektivitas regulasi hukum siber di Indonesia serta mengevaluasi peran pemerintah dalam menanggulangi kejahatan digital. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka, melibatkan analisis deskriptif dan komparasi antara regulasi siber Indonesia dengan regulasi internasional. Temuan penelitian menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum yang cukup melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), implementasinya masih kurang efektif akibat keterbatasan infrastruktur dan kurangnya koordinasi antar lembaga. Selain itu, perbandingan dengan regulasi internasional mengungkapkan perlunya revisi dan penguatan kebijakan untuk meningkatkan keamanan siber nasional.

Kata Kunci: *Regulasi Pemerintah, Hukum Siber, Kejahatan Digital.*

Introduction

The rapid development of information and communication technology has brought significant changes to various aspects of human life. The digital era provides easy access to information, enhances communication efficiency, and drives economic transformation through online platforms that are increasingly popular among society. Digitalization has reshaped interactions, work patterns, and global transactions, creating boundless connectivity (Hafizah & Muhaimin, 2023). However, behind these advantages, technological advancements have also introduced new challenges in the form of increasingly complex and diverse digital crimes. Digital crime, or cybercrime, encompasses various illegal activities that exploit information technology, such as hacking, personal data theft, online fraud, and the spread of false information that can incite social conflict (Hendarto & Handayani, 2024). The impact of digital crime is not only financially detrimental to individuals but also affects economic stability and national security. This situation underscores the importance of strong and effective legal regulations to safeguard cybersecurity and user privacy in cyberspace.

In Indonesia, the phenomenon of digital crime has shown an alarming upward trend alongside the widespread use of the internet and digital devices. According to data from the National Cyber and Encryption Agency (BSSN), cybercrime cases continue to rise annually with various modus operandi, ranging from malware attacks and phishing to personal data theft that harms both society and the economic sector. Additionally, cyberattacks have also targeted critical infrastructure such as banking, public services, and government information systems, posing a threat to national security. The Indonesian government has

responded to these threats by implementing various cyber law regulations, including the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law, and other cybersecurity policies (Dinda, 2024). These regulations are expected to provide legal certainty for information technology users and strengthen cybersecurity in Indonesia. However, the effectiveness of these regulations remains questionable, particularly regarding their implementation and enforcement, which are still suboptimal in practice.

Ideally, Indonesia's cyber law regulations should provide comprehensive protection for information technology users and significantly reduce the prevalence of digital crime. Regulations should anticipate the rapid development of technology and impose strict sanctions on cybercriminals. Furthermore, they should foster a secure and conducive digital ecosystem for Indonesia's digital economic growth (Kristianti & Kurniasi, 2024). Beyond criminal law, regulations should also cover personal data protection, intellectual property rights, and electronic transaction security. In this way, cyber law regulations can fully safeguard the rights of technology users. However, in reality, Indonesia's cyber law framework still faces various limitations, including the lack of harmonization between existing regulations, weak supervision, and low public awareness of digital security.

The limitations of Indonesia's cyber law regulations have increased vulnerability to digital crimes, negatively impacting economic stability, social structures, and national security. Cases of personal data theft, information misuse, and online fraud continue to occur without effective countermeasures. Additionally, the government's lack of preparedness in addressing global cyber threats raises concerns about the security of the country's strategic data. Furthermore, the ambiguity in implementing cyber law regulations often leads to legal disputes that disadvantage information technology users (Ghozali et al., 2024). In many cases, digital crime victims struggle to obtain adequate legal protection due to legal gaps or regulatory uncertainties. Therefore, an in-depth study is necessary to examine the existence and effectiveness of cyber law regulations in Indonesia, as well as the government's role in combating digital crime more effectively.

This research aims to analyze the existence and development of cyber law regulations in Indonesia in addressing the increasingly complex landscape of digital crime. Additionally, it seeks to evaluate the government's role in reducing digital crime rates through regulatory and operational approaches. By comparing Indonesia's cyber law framework with international regulations, this study aims to identify adaptive and effective solutions to strengthen the country's cybersecurity legal framework. It also seeks to identify challenges faced by the government in implementing regulations and to provide strategic recommendations for improving digital security in Indonesia.

Academically, this research contributes to the development of cyber law studies and provides valuable insights for legal scholarship in information technology. Practically, the findings are expected to assist the government in formulating more adaptive and effective policies to combat digital crime. Moreover, this study aims to raise public awareness about the importance of digital security and encourage active participation in maintaining cybersecurity in

Indonesia. Thus, this research not only contributes to academic discourse but also has a tangible impact on enhancing digital security and legal protection for information technology users in Indonesia.

Literature Review

Research on cyber law regulations and the role of the government in tackling digital crime in Indonesia is not a new finding. Several researchers have examined this topic from various perspectives, including criminal law policy, law enforcement, and other approaches. Amos Saito, in his work titled; *"Peran Pemerintah Dalam Penanganan Kejahatan Siber Di Era Digital Dalam Konteks Hukum Acara Pidana,"* analyzed the government's role in addressing cybercrime, with a particular focus on the application of criminal procedural law in Indonesia. The strength of this work lies in its in-depth analysis of the mechanisms of criminal procedural law in handling cybercrime, as well as its focus on the preventive and repressive efforts undertaken by the government (Simorangkir, 2024). The similarity between Simorangkir's work and this research is that both discuss the government's role in tackling digital crime. However, the difference lies in the scope of the analysis; Simorangkir's study focuses more on criminal procedural law, whereas this research aims to take a broader look at the existence and regulation of cyber law, both in a national context and in comparison with international regulations.

Zainuddin Kasim, in his article titled; *"Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia,"* has systematically discussed the criminal law policy approach to combating cybercrime, as well as evaluating the effectiveness of the Electronic Information and Transactions Law (UU ITE) in Indonesia (Kasim, 2024). The similarity with this study lies in the focus on efforts to address digital crime in Indonesia. However, the difference is that Kasim's research focuses more specifically on criminal law policy, whereas this study examines cyber law regulations in general, compares them with international regulations, and assesses the effectiveness of the government's role in their implementation.

Fadhila Rahman Najwa, in her article*; "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia,"* has provided a highly constructive analysis, particularly on the challenges of law enforcement in dealing with cybersecurity issues in Indonesia. This work also provides a realistic depiction of the implementation of cyber law in Indonesia (Najwa, 2024). The similarity with this research is that both discuss the enforcement of cyber law in Indonesia. However, the difference is that Najwa's study focuses more on the challenges of law enforcement, while this research not only discusses these challenges but also analyzes the existence of cyber law regulations, compares them with international regulations, and evaluates the government's role in tackling digital crime.

After reviewing the literature, it becomes evident that no previous research has specifically examined the existence and regulation of cyber law in Indonesia in comparison with international frameworks, while also analyzing the effectiveness of the government's role in reducing digital crime. Existing studies tend to focus on

aspects of criminal procedural law, criminal law policy, or the challenges of law enforcement without connecting them to a global context. This research aims to fill that gap by providing a more comprehensive and thorough analysis. It integrates a study on the existence of cyber law, a comparison with international regulations, and an assessment of the government's effectiveness in addressing digital crime in Indonesia. Filling this gap is crucial given the rapid development of information technology and the increasing cross-border threats posed by digital crime.

Research Methodology

This article falls under library research with a qualitative approach, aiming to analyze the existence and regulation of cyber law as well as the role of the government in combating digital crime in Indonesia. The methodology used is a descriptive analytical study to illustrate the existence of cyber law and its implementation in Indonesia, along with a comparative study to examine cyber law regulations in Indonesia in relation to international regulations. This qualitative approach was chosen as it is suitable for exploring the complex and dynamic nature of cyber law and for understanding the government's role in reducing digital crime rates.

The primary data sources in this research include regulations related to cyber and digital crime in Indonesia, such as the *Electronic Information and Transactions Law (UU ITE)*, as well as relevant government policies. Additionally, international regulations on cybersecurity are used for comparative analysis. Secondary data sources consist of scientific journals relevant to this topic, published within the last 10 years to ensure the relevance and currency of the data. The data analysis system involves systematic data collection, classification, and interpretation. Data verification and validation are conducted using source triangulation to ensure accuracy and consistency of information. The drafting of the article follows a deductive narrative method, beginning with a general discussion of cyber law and progressing into a specific analysis of the government's role in addressing digital crime in Indonesia.

Digital Crime: The Existence of Cyberspace and Its History

Digital crime is a phenomenon that continues to evolve alongside the rapid advancement of information and communication technology. In the modern era, human activities rely heavily on the digital world, from financial transactions and communication to personal data storage. This progress not only brings convenience and efficiency but also creates opportunities for new forms of crime known as digital crime. Such crimes encompass various illegal activities carried out in cyberspace, including hacking, identity theft, online fraud, malware distribution, and information manipulation (Hibar et al., 2025). Digital crime does not only target individuals but also poses threats to businesses, government institutions, and even the economic stability of a nation. This phenomenon highlights that cyberspace is not entirely secure and requires special attention in terms of cybersecurity and legal regulations.

Cyberspace is a key domain within the digital world that is frequently targeted by digital crimes. The term 'cyberspace' refers to anything related to the internet, information technology, and computer networks. In the context of digital crime, cyberspace serves as the primary medium used by perpetrators to carry out illegal activities. This is due to its borderless and anonymous nature, allowing criminals to operate from remote locations without being physically detected. For example, a hacker in one country can access and steal data from a company on the other side of the world simply by using an internet connection. Furthermore, cyberspace enables the rapid and widespread dissemination of information, which is often exploited in digital crimes such as the spread of fake news (hoaxes) and the manipulation of public opinion via social media. Therefore, cyberspace plays a crucial role in digital crime and is a major focus in efforts to maintain digital security.

One of the main reasons cyberspace is frequently used as a medium for digital crime is its anonymity and difficulty in being traced. Unlike conventional crimes that usually leave physical evidence, digital crimes often leave only complex electronic traces that require specialized skills to track. Moreover, the cost of committing digital crimes is relatively lower compared to physical crimes, yet the impact can be widespread and highly detrimental. For instance, a cyberattack on a banking system can result in massive financial losses in a short period (Balkin et al., 2007). The anonymity offered by cyberspace also makes perpetrators feel safer and more free to commit digital crimes without fear of being caught. These factors make cyberspace a fertile ground for the growth of various forms of digital crime.

The influence of cyberspace in digital crime is highly significant, especially in terms of data security threats. In today's world, data is one of the most valuable assets, both for individuals and organizations. Data security involves protecting personal information, corporate secrets, and even government strategic data. However, the borderless nature of cyberspace makes data highly vulnerable to theft, manipulation, and misuse. Digital crimes that focus on data theft often lead to financial losses and privacy violations. For example, stolen credit card data can be used for fraudulent transactions, while leaked personal data can be exploited for identity fraud. These threats highlight the critical importance of data security in an increasingly interconnected digital era.

The history of digital crime can be traced back to the early widespread use of computer technology and the internet. Initially, digital crimes were more experimental in nature, carried out by hackers who sought to demonstrate their technical abilities in breaching computer systems. One of the earliest recorded cases was the hacking of telephone systems by a group known as 'phreakers' in the 1970s. They used simple technology to illegally access telephone networks and make long-distance calls without charges (Setiyawan et al., 2024). At that time, digital crimes were primarily motivated by entertainment and technical challenges rather than financial gain. However, as technology and the internet advanced, digital crime evolved into a more serious threat.

In the 1980s, the rise of personal computers (PCs) had a significant impact on the evolution of digital crime. During this period, computer viruses began to emerge and spread through floppy disks used for data exchange between computers. One of the most well-known viruses of that era was “Brain,” discovered

in 1986, which was created by two brothers from Pakistan to protect their software from piracy. However, the virus eventually spread uncontrollably, becoming one of the first major threats in cybersecurity history (Fritama & Wibawa, 2022). This development demonstrated that as technology usage increased, digital crimes also evolved into more complex and far-reaching forms.

Entering the 1990s, the global adoption of the internet opened new opportunities for digital criminals. During this time, hacking incidents against computer systems and internet networks significantly increased. One of the most famous cases involved Kevin Mitnick, a legendary hacker who successfully breached the systems of major telecommunications companies in the United States. Mitnick stole confidential corporate data and caused substantial financial losses. His case garnered public attention and prompted the U.S. government to strengthen digital crime regulations through the Computer Fraud and Abuse Act. This event marked a crucial turning point in cyber law history, aiming to protect the digital world from illegal activities.

In the early 2000s, digital crime continued to develop with the rise of internet-based crimes such as online fraud (phishing) and identity theft. Digital crime methods became more sophisticated, leveraging emails and fake websites to trick victims into providing personal information, such as passwords and credit card numbers. One major case from this period was the "ILOVEYOU" virus attack, which spread via email and caused billions of dollars in losses worldwide. This case demonstrated that digital crime not only affects individuals but also large corporations and the global economy. Such threats encouraged many countries to begin formulating cybersecurity laws to combat increasingly complex digital crimes (Knight, 2000).

To this day, digital crime continues to evolve in line with technological advancements and changes in societal behavior that increasingly depend on the digital world. The emergence of social media, cloud computing, and blockchain technology has introduced new forms of digital crime, such as the spread of hoaxes, cloud data theft, and cryptocurrency fraud. These developments indicate that digital crime constantly adapts to technological innovations. The long history of digital crime from past to present underscores the importance of vigilance and dynamic regulations to address the ever-growing threats in cyberspace.

The Development of Cyber Law Regulations in Indonesia

The rapid advancement of information and communication technology has significantly transformed how people interact, work, and conduct transactions. In this digital era, the internet is not only a means of communication but also a public space that enables various economic, social, and cultural activities. However, despite its conveniences and benefits, the digital world also presents new challenges in the form of increasingly complex and diverse cyber threats. Digital crimes such as hacking, personal data theft, online fraud, and the spread of false information pose real threats that can disrupt social and economic stability (Simorangkir, 2024). Therefore, effective legal regulations are necessary to protect society from cyber threats and create a safe and trustworthy digital ecosystem. In

Indonesia, the development of cyber law regulations has been dynamic, evolving in response to the need to address the ever-growing threats in cyberspace.

The evolution of cyber law regulations in Indonesia is a response to the rapid growth of information and communication technology, which has significantly impacted various aspects of life. As society becomes increasingly connected through the internet, the need for legal protection in the digital world has become more urgent. Online activities involving financial transactions, the exchange of personal information, and social interactions give rise to various potential threats such as hacking, data theft, online fraud, and the spread of fake news. Therefore, cyber law regulations are needed to protect the rights and interests of the public in cyberspace while ensuring national digital security and stability. Acknowledging this importance, Indonesia has started formulating various regulations to address threats and regulate cyber governance within the country.

The journey of cyber law regulations in Indonesia began with the introduction of Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE). This law serves as the first legal foundation specifically governing activities in cyberspace, covering aspects such as electronic transactions, personal data protection, and the prosecution of cybercrimes. The UU ITE aims to provide legal certainty and security for internet users in Indonesia (Ferdiansyah et al., 2025). However, since its initial implementation, the law has faced criticism for containing ambiguous provisions that could potentially restrict freedom of expression. One of the most controversial articles is Article 27(3), which regulates defamation in the digital sphere and has often been used to prosecute social media users on charges of defamation or insult.

In response to these criticisms and the increasing complexity of technology, the Indonesian government revised the UU ITE in 2016 through Law No. 19 of 2016. This revision aimed to refine existing regulations and address various societal concerns. Some key changes in the revised UU ITE include reducing criminal penalties for defamation offenses and adding provisions that allow the accused to clarify the context of statements deemed defamatory (Idris & Supandi, 2024). Additionally, the revision strengthened the government's role in monitoring and blocking electronic information deemed unlawful. Despite these changes, the revised UU ITE is still considered insufficient in fully addressing issues related to freedom of expression and fair law enforcement in the digital space.

Apart from the UU ITE, Indonesia has also enacted various supporting regulations related to cyber law, such as Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP PSTE). PP PSTE regulates the governance of electronic systems, including the obligations of electronic system providers to protect users' personal data and ensure the security of managed information systems. This regulation aims to enhance public trust in digital services and prevent personal data breaches, which have become increasingly common. PP PSTE also requires foreign electronic system providers to register and comply with Indonesian regulations if they offer services to Indonesian citizens. This provision is intended to safeguard Indonesia’s digital sovereignty amid the dominance of global technology companies.

To further protect internet users' personal data, Indonesia has also enacted Law No. 27 of 2022 on Personal Data Protection (UU PDP). The UU PDP is a specific regulation governing the collection, processing, storage, and destruction of personal data. This law is expected to provide legal certainty in protecting individuals' privacy rights and preventing the misuse of personal data for commercial or criminal purposes (Suari & Sarjana, 2023). The UU PDP also requires electronic system providers to obtain user consent before collecting or utilizing personal data. This regulation is seen as a significant step forward in personal data governance in Indonesia and is expected to increase public trust in digital services.

Beyond general cyber law regulations, Indonesia has also issued several specialized rules to combat the growing complexity of cybercrimes. One such regulation is Chief of the Indonesian National Police Regulation No. 6 of 2019 on Cybercrime Investigations. This regulation provides technical guidelines for law enforcement officers in investigating and handling cybercrimes such as hacking, identity theft, online fraud, and the distribution of illegal content. Its implementation encourages the use of digital technology in investigative processes and promotes international cooperation in tackling cross-border cybercrimes. This regulation demonstrates the Indonesian government's commitment to enhancing the capabilities of law enforcement in addressing increasingly sophisticated and organized cybercrimes.

The history of cyber law regulation development in Indonesia cannot be separated from global efforts to combat cybercrime. Initially, Indonesia lacked specific regulations governing the digital world. However, as cybercrimes and data breaches became more prevalent worldwide, Indonesia recognized the importance of comprehensive regulations. This development has also been influenced by international agreements such as the Budapest Convention on Cybercrime, which has served as a reference for many countries in formulating cyber law regulations (Najwa, 2024). Although Indonesia has not ratified the Budapest Convention, its principles have gradually been incorporated into various cyber law regulations in the country.

The development of cyber law regulations in Indonesia has also been driven by major cases that have shaken national digital security. One notable incident was the 2020 e-commerce hacking and data breach case, which exposed the personal data of millions of Indonesians. This incident sparked public concern and prompted the government to accelerate the enactment of the UU PDP. Additionally, the widespread dissemination of fake news and hate speech on social media has pushed the government to tighten regulations concerning digital content. These events illustrate that the evolution of cyber law regulations in Indonesia is often influenced by the dynamics of cyber threats occurring in real-world situations.

International Regulations: A Comparison with Indonesia

International cyber regulations have become a crucial issue amid the rapid development of information and communication technology that transcends national borders. The global nature of the internet creates a boundless space for users worldwide to interact and conduct transactions quickly and efficiently.

However, this borderless nature also provides opportunities for transnational cybercrimes, such as hacking, data theft, digital fraud, and cyberattacks that can threaten national security and economic resilience (Suharto & Apriyani, 2021). These cybercrimes do not only target individuals or corporations but can also threaten critical infrastructures such as banking systems, power grids, and national defense security. Therefore, a comprehensive and integrated international regulation among countries is urgently needed to address increasingly complex and dynamic cyber threats. However, differences in political, economic, and legal systems across countries make the harmonization of international cyber regulations a highly complex challenge, requiring a prudent and flexible approach.

In general, international cyber regulations aim to create secure, reliable, and fair internet governance for all global users. This includes efforts to regulate online activities, protect personal data, prevent cybercrimes, and ensure that human rights in the digital world remain protected. International organizations such as the United Nations (UN), the International Telecommunication Union (ITU), and the Internet Governance Forum (IGF) have actively contributed to formulating regulations and policies governing internet use and handling cybercrimes (Susila & Salim, 2024). One of the primary challenges in formulating international cyber regulations is how to balance cybersecurity and freedom of expression, considering that the internet also serves as a space for information democratization and free speech. In pursuit of this balance, some countries engage in bilateral and multilateral cooperation to enhance cybersecurity through intelligence information exchanges and cross-border cyber law enforcement collaboration.

At the international level, the Budapest Convention is the first legal instrument specifically addressing cybercrimes. Adopted in 2001 by the Council of Europe, this convention aims to combat cybercrime through the harmonization of national legislation, enhancement of international cooperation, and provision of effective tools for cybercrime investigation and prosecution. The Budapest Convention also provides a clear legal framework for handling various types of cybercrimes, such as unauthorized access to computer systems, data interception, cyber fraud, and the distribution of illegal content. Although initially signed by European countries, the Budapest Convention has now been adopted by over 60 countries worldwide, including the United States, Japan, and Australia. However, the convention has also faced criticism for being perceived as favoring Western countries' interests while excluding developing nations from the drafting process, leading to inequalities in the global implementation of cyber regulations.

In contrast to the Budapest Convention’s focus on legislative harmonization, China and Russia have adopted different approaches to cyber regulations. These two countries emphasize the concept of cyber sovereignty, which is the right of a state to regulate internet activities within its territory independently, without foreign intervention. China, for example, implements strict regulations to control internet access and content through the Great Firewall, which restricts access to foreign platforms such as Google and Facebook (Fadhillah et al., 2023). Additionally, China requires technology companies to cooperate with the government by providing user data access as part of national security measures. Russia also enforces laws requiring the storage of internet user data on local

servers and grants broad authority to the government for cyber surveillance. This approach highlights the differing paradigms in cyber governance between democratic nations that emphasize information freedom and authoritarian regimes that prioritize control and political stability.

Meanwhile, the European Union (EU) is known for its stringent data protection regulations through the General Data Protection Regulation (GDPR). Implemented in 2018, GDPR grants individuals strong rights over their personal data and mandates companies to uphold high-security standards in data protection. This regulation has a global reach, as it applies to any company processing data of EU citizens, even if the company operates outside Europe. GDPR also imposes severe penalties on companies that violate data protection provisions, encouraging businesses worldwide to enhance their data security standards. Furthermore, GDPR governs the right to be forgotten, data portability rights, and transparency obligations in data collection and usage (Aisya et al., 2017). This policy reflects the EU's commitment to protecting privacy and human rights in an increasingly complex digital era.

Compared to Indonesia, cyber regulations in Indonesia are still in the development and refinement stage. The Electronic Information and Transactions Law (UU ITE) serves as the primary legal basis governing cyber activities in Indonesia. The UU ITE covers various aspects, including electronic transactions, online defamation, the dissemination of illegal content, and threats to cybersecurity. However, the UU ITE has often sparked controversy due to its vague provisions, which are prone to misuse in restricting freedom of expression online. Additionally, the unclear definitions of hate speech and defamation have led to legal uncertainty and the potential criminalization of criticism against the government (Jahriyah et al., 2021). Consequently, revising and refining the UU ITE is an essential agenda in strengthening Indonesia's cyber regulations.

From an international perspective, comparing Indonesia's cyber regulations with other countries shows that global harmonization of cyber regulations remains a significant challenge. Each country has different approaches to cyber governance, tailored to their political, economic, and cultural interests. However, international cooperation in tackling cybercrimes is still necessary to create a secure and trustworthy digital ecosystem. Indonesia needs to continue strengthening its cyber regulations by adopting best practices from international regulations, such as the Budapest Convention and GDPR, while still considering local contexts. Additionally, Indonesia should enhance international cooperation in addressing cross-border cyber threats through extradition agreements and intelligence information exchanges. By doing so, Indonesia can more effectively safeguard its national cybersecurity and protect citizens' rights in the digital realm.

Case Study of Digital Crime in Indonesia

Digital crime in Indonesia has been on the rise along with the rapid development of information and communication technology. The ongoing digitalization in various aspects of life, from the economy and education to public services, has transformed how people interact and conduct transactions. However, behind the convenience and efficiency offered by digital technology, the threats of

cybercrime have also become increasingly complex and diverse. Indonesia, as one of the countries with the largest number of internet users in the world, has become an attractive target for digital criminals who exploit security vulnerabilities to carry out various illegal activities. Various types of digital crimes have emerged, including online fraud, personal data theft, and cyber-attacks that threaten national security. As society becomes increasingly dependent on digital technology, understanding the various forms of digital crime in Indonesia is crucial as an initial step in preventing and addressing them.

One of the most common types of digital crime in Indonesia is online fraud. Online fraud is carried out through various methods, including phishing, scams via social media, and fraudulent e-commerce transactions. Phishing is an attempt to steal personal data such as usernames, passwords, and credit card information by deceiving victims through emails or fake websites that appear legitimate. In Indonesia, phishing cases often target users of digital banking services and e-wallets who are unaware of suspicious links (Hibar et al., 2025). Additionally, social media scams are rampant, involving fake buying and selling schemes or bogus investment offers that promise large profits in a short period. This type of fraud exploits victims' trust and the lack of verification of sellers' accounts on social media platforms. Many victims suffer significant financial losses due to scammers who are difficult to trace. In some cases, perpetrators use fake identities to erase their tracks, making legal prosecution more challenging.

Aside from online fraud, identity theft is also a concerning form of digital crime in Indonesia. Identity theft occurs when an individual's personal information, such as identification numbers, credit card details, or social media account information, is stolen and misused by irresponsible parties. This stolen data can be used for identity fraud, bank account theft, or other crimes that cause financial and psychological harm to victims. In Indonesia, identity theft often occurs through fake applications, unsecured websites, or vulnerable public Wi-Fi networks (Nuranisa & Lukitasari, 2024). Additionally, data breaches from government institutions and private companies have exacerbated this issue. The lack of security in personal data management highlights the weak data protection regulations in Indonesia, encouraging digital criminals to continue exploiting these vulnerabilities. This situation raises public concern about the security of their personal data, especially in an era where online information is heavily relied upon.

Cyber-attacks also pose a serious threat in Indonesia's digital landscape. These attacks aim to damage information systems, steal data, or disrupt digital services on a large scale. One of the most frequent types of cyber-attacks is Distributed Denial of Service (DDoS), where attackers flood servers with massive amounts of data traffic, causing systems to slow down or become completely inaccessible. DDoS attacks often target government websites, banking services, and e-commerce platforms. In addition to DDoS, malware attacks such as ransomware are also prevalent in Indonesia. Ransomware works by encrypting victims' important data and demanding ransom payments in digital currency to unlock it (Lestari & Taufik, 2024). Many institutions in Indonesia, including hospitals and educational institutions, have fallen victim to ransomware, suffering substantial operational losses. These cyber-attacks reveal the vulnerability of Indonesia's digital infrastructure to increasingly sophisticated cyber threats.

Additionally, cyberbullying has become a concerning form of digital crime in Indonesia, particularly among teenagers. Cyberbullying involves intimidation, insults, or harassment through digital media such as social media, instant messaging apps, or online forums. The impact of cyberbullying is not only psychological but can also affect victims' mental health, leading to depression and suicidal tendencies. In Indonesia, cyberbullying cases frequently occur among students and university students who are active on social media. The lack of education on internet ethics and weak parental supervision further aggravates this phenomenon. Although Indonesia's Electronic Information and Transactions Law (UU ITE) regulates online defamation and insults, its enforcement remains ineffective in addressing cyberbullying cases. A more holistic approach is needed, including digital education and increased public awareness, to tackle cyberbullying effectively.

Another prevalent form of digital crime is the dissemination of illegal content, such as child pornography, hate speech, and hoaxes. The spread of illegal content not only violates social and moral norms but also threatens national security. In Indonesia, the spread of hoaxes and hate speech often escalates during election periods and sensitive issues involving religion and politics. These hoaxes mislead the public and can trigger broader social conflicts. Meanwhile, the distribution of child pornography is a particularly severe crime as it involves the exploitation of children who should be protected (Andaryuni, 2012). The Indonesian government, through the Ministry of Communication and Information Technology (Kominfo), has blocked websites that distribute illegal content. However, these efforts are often ineffective as digital criminals continuously find new ways to bypass these restrictions.

The phenomenon of digital crime in Indonesia highlights the need for stronger regulations and law enforcement in the cyber world. The UU ITE, as the main legal framework governing digital crimes in Indonesia, is often deemed insufficient to accommodate the growing complexity of cybercrime. Therefore, the government must revise and refine regulations while enhancing international cooperation to combat cross-border digital crimes. Educating the public about cybersecurity and internet ethics is also crucial in preventing digital crimes from an early stage. With a good understanding of various digital crimes, society can be more cautious and responsible when using digital technology, contributing to a safer and healthier digital ecosystem in Indonesia.

The Role of the Indonesian Government in Combating Digital Crime

The rapid development of digital technology in Indonesia has brought numerous benefits across various sectors of life, including the economy, education, and public services. However, alongside this progress, digital crimes or cybercrimes have also become increasingly prevalent. Digital crime encompasses various illegal activities that exploit information and communication technology, such as online fraud, personal data theft, hacking, and the dissemination of illegal content. In addressing this threat, the role of the government is crucial in creating a safe and reliable digital ecosystem (Kasim, 2024). The Indonesian government recognizes that digital crimes not only harm individuals but can also threaten

economic stability and national security. Therefore, various efforts have been made to curb digital crimes in Indonesia through legal regulations, strengthening cybersecurity infrastructure, and educating and raising public awareness.

One of the primary roles of the Indonesian government in combating digital crime is the establishment of strict legal regulations that align with technological advancements. The Information and Electronic Transactions Law (UU ITE) serves as the primary legal framework governing digital activities in Indonesia. Initially enacted in 2008 and revised in 2016, the UU ITE aims to provide legal protection for internet users while taking action against perpetrators of digital crimes. Several provisions within the UU ITE regulate the prohibition of spreading illegal content, defamation, online fraud, and unauthorized access to electronic systems. However, the UU ITE has often been criticized for containing vague articles that can be misused, particularly regarding defamation and hate speech. Consequently, the government continues to evaluate the UU ITE to ensure that its implementation does not infringe on the public's right to freedom of expression in the digital sphere.

In addition to the UU ITE, the Indonesian government has also strengthened regulations through Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. This regulation mandates electronic system providers to protect users' personal data, maintain system security, and grant access to law enforcement authorities for legal enforcement purposes. In practice, this regulation aims to curb digital crimes such as identity theft and hacking, which have become increasingly rampant. Moreover, the government is currently drafting the Personal Data Protection Bill (RUU PDP), which is expected to provide more comprehensive protection of digital privacy. With strong regulations in place, digital criminals are expected to think twice before engaging in illegal activities that harm the public (Herdiana, 2022).

Beyond legal regulations, the Indonesian government is actively strengthening cybersecurity infrastructure to combat digital crime. The National Cyber and Crypto Agency (BSSN) was established in 2017 with the primary mission of safeguarding national cybersecurity and protecting critical information infrastructure from cyber threats. BSSN plays a key role in early detection of cyber threats, responding to cyber incidents, and coordinating with relevant agencies to combat digital crime. Additionally, BSSN is responsible for developing cybersecurity standards for both government institutions and the private sector, thereby fostering a more secure digital ecosystem. With strict supervision and security measures implemented by BSSN, the risk of cyberattacks such as hacking and malware is expected to be minimized in Indonesia.

International cooperation is also a strategic measure taken by the Indonesian government in tackling digital crime. Given that digital crime transcends national borders and involves international networks, Indonesia actively collaborates with other countries and international organizations such as INTERPOL and ASEAN. Through these partnerships, the government can exchange intelligence on cyber threats, enhance law enforcement capacity in handling digital crime, and pursue digital criminals operating outside Indonesia. One notable example of Indonesia’s international collaboration is its participation in the Global Forum on Cyber Expertise (GFCE), which focuses on capacity-building and global

cybersecurity enhancement (Fadhillah et al., 2023). By strengthening international cooperation, the Indonesian government can more effectively address digital crime perpetrators who exploit legal jurisdiction loopholes between countries.

On the other hand, the government also recognizes the importance of public education and awareness campaigns as preventive measures against digital crime. Through the Ministry of Communication and Information Technology (Kominfo), the government actively conducts digital literacy campaigns to enhance public awareness of cybersecurity and internet ethics. These digital literacy programs educate people on securing personal data, recognizing online fraud (phishing), and avoiding illegal content that could be harmful to themselves and others (Dinda, 2024). Furthermore, Kominfo collaborates with social media platforms to educate users on responsible social media usage and to prevent them from being easily provoked by hoaxes or hate speech. With a digitally literate society, the prevalence of digital crime is expected to decrease significantly.

The Indonesian government also enforces strict legal actions against digital crime perpetrators. Through the Indonesian National Police (Polri) and the Directorate of Cybercrime, the government actively conducts cyber patrols to monitor illegal activities in cyberspace. Cyber police are responsible for detecting and investigating digital crimes, as well as arresting individuals proven to have committed cyber offenses. Additionally, the government collaborates with the judiciary to ensure that digital crime cases are processed transparently and fairly. This initiative aims to deter potential offenders and serve as a warning to the public against engaging in illegal digital activities.

Despite the various efforts undertaken by the Indonesian government to combat digital crime, significant challenges remain. The rapid advancement of digital technology continuously evolves the methods of digital crime, making them increasingly complex. Moreover, low public awareness of cybersecurity remains a major obstacle in preventing digital crime. Therefore, the government must continue updating legal regulations to be adaptive to technological developments, strengthening law enforcement capacities, and improving digital literacy among citizens. With strong synergy between regulations, technology, and education, it is hoped that digital crime in Indonesia can be significantly reduced, leading to a safe and trustworthy digital ecosystem for all.

Conclusion

The existence and regulation of cyber law in Indonesia have evolved in response to the increasing complexity and diversity of digital crime threats. Globally, cyber regulations continue to evolve to address digital security challenges, with various countries implementing stringent and comprehensive laws. Indonesia, through the Electronic Information and Transactions Law (UU ITE) and other related regulations, has made efforts to regulate the use of information technology and combat digital crimes. However, compared to more developed international regulations, such as the GDPR in the European Union or the CCPA in the United States, Indonesia's cyber regulations still face challenges in terms of consistent implementation and adaptation to rapidly advancing technology.

The Indonesian government plays a crucial role in reducing the rate of digital crime through both regulatory and operational approaches. Various measures have been taken, including strengthening the legal framework, enhancing law enforcement capabilities, and raising public awareness of digital security. Additionally, international cooperation has become a key focus in addressing cross-border cyber threats. Nevertheless, the effectiveness of regulations and government policies still needs improvement by aligning with international regulatory standards and reinforcing cybersecurity infrastructure. With strong commitment and adaptive policies, the Indonesian government is expected to combat digital crime more effectively and ensure cybersecurity for its citizens.

References

Aisya, N. S., Putranti, I. R., & Wahyudi, F. E. (2017). Analisis Implementasi Cyber Security di Uni Eropa: Studi Kasus Carbon Credits Hacking dalam European Union Emission Trading Scheme (EU ETS) Tahun 2010-2013. *Journal of International Relations Diponegoro*, *3*(2), Article 2. https://doi.org/10.14710/jirud.v3i2.16612

Andaryuni, L. (2012). UU Pornografi Dalam Perspektif Hukum Islam. *Mazahib*, *10*(1), 26–36. https://doi.org/10.21093/mj.v10i1.107

Balkin, J. M., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (2007). *Cybercrime: Digital Cops in a Networked Environment*. NYU Press. https://www.jstor.org/stable/j.ctt9qfchj

Dinda, A. L. S. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum*, *2*(2), Article 2. https://doi.org/10.58707/aldalil.v2i2.777

Fadhillah, S. A., Matakupan, M. S. A., & Mingga, B. W. B. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest on Cybercrimes. *Journal on Education*, *5*(4), Article 4. https://doi.org/10.31004/joe.v5i4.2822

Ferdiansyah, A., Wahyono, B. A. W., Harahap, A., Gustian, E., & Zaidan, D. (2025). Pengaruh Penerapan Undang-Undang ITE Terhadap Tingkat Kejahatan Siber di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik*, *2*(2), Article 2. https://doi.org/10.62379/bza49768

Fritama, M., & Wibawa, A. (2022). Bioinformatic & Brain-Computer Interface: AIoT & Society 5.0 di Kehidupan untuk Teknologi yang Singular. *Jurnal Inovasi Teknologi Dan Edukasi Teknik*, *2*(3), Article 3. https://doi.org/10.17977/um068v2i32022p144-154

Ghozali, M., Liana, N., Afra, C., Siregar, Z., Nurfahni, Malahayati, & Hatta, M. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *Cendekia: Jurnal Hukum, Sosial Dan Humaniora*, *2*(4), Article 4. https://doi.org/10.5281/zenodo.13883603

Hafizah, H., & Muhaimin, M. (2023). Dampak Digitalisasi Pembayaran Zakat Terhadap Peningkatan Penerimaan Zakat pada Baznas Kota Banjarmasin. *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan*, *17*(5), Article 5. https://doi.org/10.35931/aq.v17i5.2661

Hendarto, D. H., & Handayani, R. S. (2024). Pencegahan Kejahatan Siber Terkait Distribusi Perjudian Online di Indonesia dalam Rangka Mewujudkan Keamanan dan Ketertiban Masyarakat. *Jurnal Syntax Admiration*, *5*(5), 1542–1558. https://doi.org/10.46799/jsa.v5i5.1136

Herdiana, R. (2022). *Sanksi Homoseksual melalui Praktik Open Booking Order (BO) Menurut Pasal 45 Ayat (1) UU ITE dalam Perspektif Hukum Pidana Islam* [Other, UIN Sunan Gunung Djati Bandung]. https://digilib.uinsgd.ac.id/56599/

Hibar, U., Jumhana, E., & Arifin, S. (2025). Cybercrime Digital Crime How Technology is Utilized for Crime. *Journal of Law Science*, *7*(1), Article 1. https://doi.org/10.35335/jls.v7i1.5848

Idris, J. I., & Supandi, A. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *Transparansi: Jurnal Ilmiah Ilmu Administrasi*, *7*(1), 149–162. https://doi.org/10.31334/transparansi.v7i1.3709

Jahriyah, V. F., Kusuma, M. T., Qonitazzakiyah, K., & Fathomi, M. A. (2021). Kebebasan Berekspresi di Media Elektronik dalam Perspektif Pasal 27 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Pelayanan Transaksi Elektronik (UU ITE). *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial*, *1*(2), Article 2. https://doi.org/10.15642/sosyus.v1i2.96

Kasim, Z. (2024). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review*, *2*(1), Article 1. https://doi.org/10.32520/ilr.v2i1.22

Knight, P. (2000). ILOVEYOU: Viruses, Paranoia, and the Environment of Risk. *The Sociological Review*, *48*(2_suppl), 17–30. https://doi.org/10.1111/j.1467-954X.2000.tb03518.x

Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, *7*(1), Article 1. https://doi.org/10.33363/sd.v7i1.1243

Lestari, J. A., & Taufik, G. (2024). Penerapan NIST 800-61 REV 2 untuk Analisa Ransomware Attack pada PT. Sembilan Pilar Semesta dengan Berbasis SIEM. *Jurnal Infortech*, *6*(1), Article 1. https://doi.org/10.31294/infortech.v6i1.21767

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), Article 1. https://doi.org/10.32520/albahts.v2i1.3044

Nuranisa, A., & Lukitasari, D. (2024). Tindak Pidana Pencurian Data dan Privasi Pengguna Dalam Transaksi E-Commerce: Studi Kasus pada Aplikasi Tokopedia. *Amandemen: Jurnal Ilmu Pertahanan, Politik Dan Hukum Indonesia*, *1*(2), 115–126. https://doi.org/10.62383/amandemen.v1i2.145

Setiyawan, N. E., Karauwan, D. E. S., Jumiran, & Ghafar, A. A. (2024). The Effect of Digital Technology on Criminal Law Enforcement: An Analysis of Cybercrime and Its Handling. *Mawaddah: Jurnal Hukum Keluarga Islam*, *2*(2), Article 2. https://doi.org/10.52496/mjhki.v2i2.169

Simorangkir, A. S. H. (2024). Peran Pemerintah dalam Penanganan Kejahatan Siber di Era Digital dalam Konteks Hukum Acara Pidana. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *7*(3), Article 3. https://doi.org/10.3783/causa.v7i3.6767

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), Article 1. https://doi.org/10.38043/jah.v6i1.4484

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, dan Cyber Warfare dalam Aspek Hukum Internasional. *Risalah Hukum*, *17*(2), 98–107. https://doi.org/10.30872/risalah.v17i2.705

Susila, M. E., & Salim, A. A. (2024). Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany. *Journal of Law: Padjadjaran Jurnal Ilmu Hukum*, *11*(1), 122–144.