

**JLPH:**
Journal of Law, Politic
and Humanities<https://dinastires.org/JLPH> ✉ dinasti.info@gmail.com ☎ +62 811 7404 455E-ISSN: 2962-2816
P-ISSN: 2747-1985DOI: <https://doi.org/10.38035/jlph.v6i6>
<https://creativecommons.org/licenses/by/4.0/>

Received: 21 September 2026 | Revised: 13 Oktober 2026 | Accepted: 18 Oktober 2026

Cybercrime in Indonesia: a Legal Perspective and Countermeasures

Muhammad Ikramullah Romandita Utama¹¹Universitas Bengkulu, Bengkulu, Indonesia, muhammadikramullah.im@gmail.comCorresponding Author: muhammadikramullah.im@gmail.com¹

Abstract: The rapid advancement of information and communication technology in the era of globalization has significantly transformed modern society's activities while simultaneously triggering the emergence of cybercrime. Cybercrime refers to unlawful acts utilizing electronic systems or the internet as a means or object of crime, characterized by its borderless nature, anonymity, and broad impact on economic, social, and national security dimensions. This study aims to analyze the development and forms of cybercrime in Indonesia, as well as to examine its legal perspective and countermeasure strategies. Employing a normative legal research method, this paper analyzes relevant statutory regulations and legal literature. The findings indicate that cybercrime in Indonesia manifests in various modes, including hacking, cracking, phishing, online scams, cyberbullying, ransomware, and personal data theft. The rise of these crimes is driven by high internet usage unmapped by digital literacy, system vulnerabilities, and economic motives. From a legal perspective, Indonesia has established a legal framework through the Electronic Information and Transactions (EIT) Law and the Personal Data Protection Law. However, law enforcement continues to face complex hurdles, such as cross-border jurisdictional conflicts, digital evidence verification, limited human resource capacity, and inadequate digital forensic infrastructure. Therefore, tackling cybercrime requires a comprehensive blend of penal and non-penal approaches, encompassing adaptive regulatory updates, law enforcement capacity building, enhanced national cybersecurity, community digital literacy education, and international cooperation.

Keywords: Cybercrime, Criminal Law, EIT Law, Law Enforcement, Cybersecurity

Abstrak: Pesatnya perkembangan teknologi informasi dan komunikasi di era globalisasi telah membawa perubahan signifikan dalam aktivitas masyarakat modern sekaligus memicu munculnya kejahatan siber (cybercrime). Cybercrime merupakan tindakan melawan hukum yang memanfaatkan sistem elektronik atau jaringan internet sebagai sarana maupun objek kejahatan, yang berkarakteristik borderless, anonim, serta berdampak luas pada aspek ekonomi, sosial, hingga keamanan nasional. Penelitian ini bertujuan untuk menganalisis perkembangan dan bentuk-bentuk cybercrime di Indonesia, serta mengkaji perspektif hukum dan upaya penanggulangannya. Penelitian ini menggunakan metode pendekatan yuridis normatif dengan menganalisis peraturan perundang-undangan dan literatur hukum terkait.

Hasil penelitian menunjukkan bahwa cybercrime di Indonesia berkembang dalam berbagai modus seperti hacking, cracking, phishing, penipuan daring (online scam), cyberbullying, ransomware, dan pencurian data pribadi. Peningkatan kasus ini didorong oleh tingginya penggunaan internet yang tidak diimbangi dengan literasi digital, kelemahan sistem keamanan, serta motif ekonomi. Dalam perspektif hukum, Indonesia telah memiliki kerangka regulasi utama seperti UU ITE (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016) dan UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022). Namun, proses penegakan hukum masih menghadapi kendala kompleks, seperti masalah yurisdiksi lintas negara, pembuktian dan validitas alat bukti digital, keterbatasan sumber daya manusia serta sarana digital forensik. Oleh karena itu, penanggulangan cybercrime membutuhkan kombinasi pendekatan penal dan non-penal secara komprehensif, mencakup penguatan regulasi adaptif, penguatan kapasitas aparat, peningkatan keamanan siber nasional, edukasi literasi digital masyarakat, serta kerjasama internasional.

Kata Kunci: *Cybercrime, Hukum Pidana, UU ITE, Penegakan Hukum, Keamanan Siber*

INTRODUCTION

The development of information and communication technology in the current era of globalization has profoundly impacted human life. Technological advancements have brought about significant changes in societal activities across various sectors, including the economy, education, social life, governance, and communication. The advent of the internet as part of the evolution of digital technology has become a primary means of supporting the needs of modern society. Activities previously conducted through conventional methods have shifted to electronic-based systems; examples include banking transactions, online commerce (e-commerce), learning systems, public services, and social interaction via digital media. These developments demonstrate the vital role information technology plays in enhancing the effectiveness and efficiency of daily life (Budi Suhariyanto, 2014).

Advances in information technology essentially offer immense benefits to human life. However, these developments also bring about various new consequences, including the emergence of crimes that utilize information technology as a means to commit illegal acts. Rapid technological progress is often not matched by a corresponding increase in public awareness regarding the safe and responsible use of technology. Consequently, technology originally created to simplify human life is instead exploited by certain parties to engage in unlawful activities. This phenomenon has given rise to a new form of crime known as cybercrime (Abdul Wahid dan Mohammad Labib, 2010).

Cybercrime is an unlawful act committed using computers, the internet, electronic systems, or other digital devices either as the means or the object of the crime. It differs from conventional crime in that it can be perpetrated without regard for geographical or temporal boundaries. Perpetrators can carry out their actions from any location, even across national borders, thereby creating complex issues regarding jurisdiction and law enforcement. Furthermore, the perpetrator's identity is often difficult to ascertain due to the use of fake accounts, the masking of digital identities, and specific technologies capable of erasing traces of their activity (Maskun, 2013).

The prevalence of cybercrime has shown a significant increase over time. Common forms of cybercrime include hacking, cracking, personal data theft, online scams, cyberbullying, malware distribution, carding, and the spread of hoaxes via social media. These various forms of crime demonstrate that the evolution of digital technology has created new challenges that both society and the state must confront. As internet usage grows, the potential for cybercrime also rises, evolving alongside increasingly sophisticated (Widodo, 2013).

Indonesia is among the countries experiencing rapid growth in the number of internet users. High levels of public engagement with digital technology have led to an increased risk of cybercrime. Indonesians currently rely heavily on the internet for various daily activities a dependency that cybercriminals often exploit for illicit gain. Low levels of digital literacy, weak data security systems, and a lack of cybersecurity awareness are factors contributing to the rise of technology-based crimes in Indonesia (Josua Sitompul, 2012).

Cybercrime not only causes individual losses but can also have broader impacts on society and the state. Economically, it can result in significant financial losses. Socially, it can foster a sense of insecurity and erode public trust in the use of digital technology. On an even larger scale, cyberattacks targeting government institutions or critical national infrastructure can threaten national security stability. Consequently, cybercrime is no longer viewed merely as an ordinary offense; it has become a serious threat in modern society (Didik M. Arief Mansur dan Elisatris Gultom, 2009).

From a legal perspective, the evolution of cybercrime necessitates a legal system capable of keeping pace with social changes and technological advancements. Conventional criminal law was fundamentally designed to address tangible offenses with clearly defined territorial boundaries, whereas cybercrime operates within a virtual realm characterized by features distinct from those of traditional crimes. Consequently, there is a need for a legal framework that ensures legal certainty while guaranteeing effective law enforcement against cybercriminals (Sigid Suseno, 2013).

The increasingly complex evolution of cybercrime demonstrates that it is no longer merely a technical issue related to the use of information technology; rather, it has developed into a multidimensional problem touching upon legal, economic, social, cultural, and national security aspects. Due to this complexity, combating cybercrime cannot rely solely on repressive measures such as law enforcement; it also requires preventive steps—including education, the enhancement of digital literacy, the strengthening of technological security systems, and inter-agency cooperation at both national and international levels. Such measures are crucial because the borderless nature of cybercrime often complicates the identification of perpetrators, the determination of legal jurisdiction, and the effective execution of law enforcement actions (Rika Ratna Permata, 2020).

Furthermore, the rapid pace of digital technology advancement necessitates continuous legal updates. The law cannot afford to lag behind societal developments, as its fundamental function is to establish order, certainty, justice, and protection for the public. If technological progress outpaces regulatory development, a legal gap emerges one that criminals can exploit to commit acts detrimental to society. Consequently, the state is required to implement regulations that are adaptive to information technology advancements without compromising the protection of public rights.

Furthermore, successfully combating cybercrime requires the active participation of the public as technology users. The public is not merely a subject of legal protection but also plays a vital role in fostering a secure digital environment by raising cybersecurity awareness, exercising caution when using digital media, and complying with applicable laws. Public legal awareness is a crucial factor in minimizing the potential for cybercrimes, which are increasingly evolving with diverse forms and new.

Based on the preceding discussion, it is evident that cybercrime is a phenomenon that evolves alongside advancements in information and communication technology. Cybercrime impacts not only individuals but also the interests of the broader public and even national security. Therefore, a deeper examination of cybercrime in Indonesia viewed through a legal lens and considering countermeasures is crucial. Such an analysis fosters an understanding of the evolution of cybercrime, its regulation within the Indonesian legal system, and the strategies required to combat it effectively and sustainably.

METHODS

This study employs a normative legal research method (juridical-normative), involving the examination and analysis of legal norms concerning cybercrime within the Indonesian legal system and the measures taken to address it. The approaches utilized include the statute approach to examine various legal provisions governing cybercrimes and the conceptual approach to understand the concept of cybercrime and the policies for addressing it. The legal materials employed consist of primary sources (legislation related to cybercrime and information technology), secondary sources (books, scholarly journals, research findings, and expert legal opinions), and tertiary sources (legal dictionaries and other supporting materials). Data collection was conducted through library research, while the analysis was performed using a qualitative-descriptive method; this involved elaborating upon, interpreting, and interrelating relevant legal provisions to analyze the evolution and forms of cybercrime in Indonesia, as well as the legal perspectives and the preventive and repressive measures employed to combat it.

RESULTS AND DISCUSSION

Forms and Evolution of Cybercrime in Indonesia

The rapid advancement of information technology has brought about significant changes in the lifestyles of the Indonesian people. The use of the internet across various aspects of life such as communication, economic transactions, education, banking, and public services has created an increasingly expansive digital landscape. However, this development has also been accompanied by a rise in the misuse of technology by certain parties to commit unlawful acts. As internet usage grows, the forms and methods of cybercrime are evolving rapidly and becoming increasingly complex (Budi Suhariyanto, 2014).

Cybercrime in Indonesia has grown rapidly due to the public's extensive use of digital technology. Technological advancements enable perpetrators to exploit vulnerabilities in digital security systems and the public's low level of technological literacy to gain unlawful profits. Unlike conventional crimes, which typically involve direct interaction, cybercrime utilizes electronic devices and internet networks, allowing offenses to be committed from anywhere without the need for physical contact with the victim (Abdul Wahid dan Mohammad Labib, 2010).

The evolution of cybercrime in Indonesia demonstrates that such offenses are no longer simple in nature; instead, they have developed into forms of crime characterized by increasingly diverse patterns, methods, and targets. Perpetrators target not only individuals but also corporations, financial institutions, educational establishments, and government agencies. This indicates that cybercrime has a broad scope and poses a threat to various sectors of society (Maskun, 2013).

In addition to hacking, there is another form of cybercrime known as "cracking." While hacking focuses primarily on unauthorized system access, cracking involves breaching security systems or modifying programs for specific purposes. Crackers typically aim to gain personal profit by compromising the security of a device or computer network. Such actions can result in significant financial losses and compromise the security of user data (Josua Sitompul, 2012).

Another form of cybercrime that occurs quite frequently in Indonesia is online fraud. Online fraud is perpetrated by utilizing the internet, social media, or electronic applications to deceive victims for financial gain. The methods employed vary widely, ranging from the sale of non-existent goods, fake investments, and lottery scams to identity misuse via social media. High levels of public engagement in digital transactions have made online fraud one of the most prevalent forms of cybercrime.

Another form of cybercrime that has seen significant growth is personal data theft. Personal data currently holds high economic value, making it a frequent target for cybercriminals. Perpetrators can obtain such data through various methods, including system hacking, phishing, the dissemination of malicious links, or the misuse of specific digital applications. The stolen data is subsequently used for various illicit activities, such as compromising bank accounts, creating fake accounts, and committing other criminal offenses (Abdul Kadir Muhammad, 2004).

In addition to data theft, technological advancements have also given rise to phishing. Phishing is a fraudulent method that lures victims into disclosing personal information such as passwords, account numbers, OTP codes, or other sensitive data via fake websites or electronic messages. This type of crime often mimics legitimate institutions, making it difficult for victims to distinguish between authentic and fraudulent information. Consequently, many people fall victim to these schemes due to a lack of understanding regarding such digital threats.

The evolution of cybercrime in Indonesia is also marked by a rise in cases of cyberbullying. Cyberbullying involves acts of intimidation, humiliation, threats, or attacks against an individual via digital channels such as social media, electronic messaging, or other online platforms. Unlike traditional bullying, cyberbullying has a broader impact because the disseminated information can be accessed by a large number of people in a very short time. Such actions can inflict serious psychological harm on the victim.

In addition, there are crimes involving the dissemination of malware and ransomware. Malware refers to malicious programs designed to damage computer systems or steal user information. Ransomware, meanwhile, is a type of malware that locks a victim's system or data and demands a ransom in exchange for restoring access. Such attacks currently pose a serious threat, as they can target both individuals and critical state institutions.

Another form of cybercrime emerging in Indonesia is "carding" the theft and misuse of another person's credit card data to conduct illegal transactions. Indonesia once experienced a high incidence of carding cases due to weak digital transaction security systems and a lack of public awareness regarding personal data protection.

Given these various forms of cybercrime, it is evident that such offenses are on the rise in Indonesia, both in terms of the number of cases and the diversity of **modus operandi** employed by perpetrators. Cybercrime evolves alongside advancements in information technology and the activity patterns of the digital society. Therefore, a solid understanding of the various forms of cybercrime is essential to enable the public to heighten their vigilance and to allow the government to formulate more effective countermeasures.

Legal Perspective and Efforts to Combat Cybercrime in Indonesia

1. A Legal Perspective on Cybercrime in Indonesia

The rapid advancement of information technology has brought about changes in modern legal systems, including Indonesian criminal law. Shifts in societal lifestyles characterized by an increasing reliance on digital technology have given rise to new forms of criminal offenses previously unknown in conventional criminal law. Cybercrime has evolved alongside the growing use of the internet in various aspects of daily life. This situation presents new challenges for the national legal system, as the characteristics of cybercrime differ from the conventional crimes traditionally addressed by criminal law (Edmon Makarim, 2005).

From a criminal law perspective, cybercrime is viewed as an unlawful act that causes harm to individuals, society, and the state. Cybercrime possesses unique characteristics because it is committed within a virtual space (cyberspace) that transcends national borders. These characteristics often give rise to issues regarding legal jurisdiction, evidence,

perpetrator identification, and law enforcement processes. Consequently, the evolution of cybercrime necessitates a legal system capable of adapting to advancements in information technology (Dikdik M. Arief Mansur dan Elisatris Gultom, 2005).

Theoretically, the law serves to establish order, certainty, justice, and public protection. In the context of cybercrime, the law functions not only to impose sanctions on offenders but also as an instrument to prevent various forms of information technology misuse. The law must be capable of safeguarding public interests regarding the use of digital technology, thereby ensuring security and legal certainty within cyberspace (Satjipto Rahardjo, 2006).

Cybercrime can essentially be examined through the perspective of modern criminal law. Modern criminal law emphasizes that societal evolution must be accompanied by legal development to ensure the law does not lag behind social realities. Shifts in criminal patterns driven by technological advancements demonstrate that criminal law can no longer focus solely on conventional offenses; it must also be capable of addressing crimes that emerge within the digital realm. Consequently, the reform of criminal law is crucial in addressing the evolution of cybercrime (Barda Nawawi Arief, 2011).

In Indonesia, the legal framework governing cybercrime initially relied on provisions within the Criminal Code (KUHP). However, the Criminal Code was deemed inadequate for addressing various forms of technology-based crime, as the majority of its provisions were designed to regulate conventional offenses. For instance, the elements of criminal offenses in the Code largely focus on physical objects, whereas the targets of cybercrime can include electronic data, information systems, or digital identities (Adami Chazawi dan Ardi Ferdian, 2015).

In response to technological advancements and the rise of cybercrime, the Indonesian government established specific regulations through Law Number 11 of 2008 concerning Electronic Information and Transactions, which was subsequently amended by Law Number 19 of 2016. The enactment of this law represents a significant step toward providing legal certainty for various electronic activities while also serving as the legal basis for combating cybercrime in Indonesia (Ahmad Ramli, 2010).

The Electronic Information and Transactions Law regulates various forms of criminal offenses related to the use of information technology. Acts categorized as criminal offenses under the law include, among others, illegal access to electronic systems, illegal interception, electronic data manipulation, the dissemination of prohibited information, and the destruction of electronic systems. The enactment of this law demonstrates the state's effort to align the legal system with advancements in information technology (Siswanto Sunarso, 2009).

In addition to the Law on Electronic Information and Transactions, the regulation of cybercrime is supported by various other statutes such as the Personal Data Protection Law and the Telecommunications Law as well as certain provisions within the Criminal Code that remain relevant for addressing cyber offenses. The existence of these various regulations demonstrates that combating cybercrime requires a multidisciplinary legal approach and cannot rely solely on a single piece of legislation (M. Hamdan, 2012).

Although Indonesia has various regulations addressing cybercrime, law enforcement still faces numerous challenges in practice. A primary issue is the transnational nature of cybercrime; perpetrators can commit offenses from another country without being physically present at the victim's location. This situation complicates the determination of which jurisdiction has the authority to handle the case. Furthermore, proving cybercrimes requires digital evidence, which possesses characteristics distinct from those of conventional evidence (Sinta Dewi Rosadi, 2018).

Beyond jurisdictional issues, another challenge lies in the rapid pace of technological advancement relative to the evolution of the law itself, the of cybercrime constantly evolves

alongside digital technological innovations, often causing existing regulations to lag behind in addressing new forms of crime. Consequently, continuous legal reform is essential to ensure the law keeps pace with societal and technological developments (Agus Rahardjo, 2013).

Based on the foregoing, it is evident that, from a legal perspective, cybercrime constitutes a modern form of criminal offense requiring an adaptive legal approach. The law must be capable of keeping pace with technological advancements to ensure legal certainty, justice, and public protection. Strengthening regulations, updating criminal laws, and fostering inter-agency cooperation are crucial factors in achieving effective law enforcement against cybercrime.

2. Efforts to Combat Cybercrime in Indonesia

The rising trend of cybercrime in Indonesia indicates that it has become a serious issue requiring special attention from various stakeholders. While rapid advancements in information technology have positively impacted society, they have simultaneously created opportunities for various forms of technological misuse. Cybercrime is currently evolving not only in terms of the number of cases but also regarding the increasingly complex nature, methods, and targets of these offenses. Perpetrators target not only individuals but also corporations, educational institutions, financial entities, and even government systems. Consequently, efforts to combat cybercrime cannot be piecemeal; instead, they require a comprehensive approach that integrates legal, technological, and institutional aspects alongside public participation (Muladi dan Barda Nawawi Arief, 2010).

From the perspective of criminal law policy, crime control can essentially be pursued through two primary approaches: penal and non-penal. The penal approach involves addressing crime through the application of criminal law to offenders; this is implemented via the enactment of legislation, investigation and prosecution processes, and the imposition of criminal sanctions. Conversely, the non-penal approach employs preventive measures aimed at eliminating the factors that give rise to criminal acts. In the context of cybercrime, a balanced application of both approaches is essential, given the distinct complexities inherent in cybercrime compared to conventional offenses (Barda Nawawi Arief, 2010).

Efforts to address the issue through a legal approach have been undertaken by establishing regulations that serve as the legal basis for handling cybercrime in Indonesia. The state enacted Law Number 11 of 2008 concerning Electronic Information and Transactions subsequently amended by Law Number 19 of 2016 to serve as the primary legal framework governing various electronic-based activities. These regulations represent the state's response to advancements in information technology, which have given rise to new forms of criminal offenses in cyberspace. The law defines various acts as criminal offenses, including illegal access to electronic systems, illegal interception, electronic data manipulation, the dissemination of prohibited information, and interference with electronic systems. The existence of these regulations marks a crucial step toward providing legal certainty and protection for the public in their use of digital technology (Adami Chazawi dan Ardi Ferdian, 2015).

In addition to establishing regulations, strengthening the capacity of law enforcement officials is a crucial component of efforts to combat cybercrime. Handling cybercrimes requires a different set of skills compared to handling conventional crimes. Law enforcement personnel are not only expected to understand criminal law aspects but must also possess technical expertise in information technology, digital forensics, network security, and electronic system analysis. This is because evidence in cybercrime cases largely consists of electronic data and digital traces, which require specialized methods for identification and substantiation. Therefore, enhancing human resource quality, providing

continuous training, and ensuring adequate technological facilities are essential to supporting effective law enforcement against cybercrime (M. Ali Zaidan, 2015).

In addition to repressive measures involving law enforcement, combating cybercrime also requires preventive steps through the enhancement of digital system security. Various sectors of society ranging from banking, government, and education to public services now rely on electronic systems. This reliance makes the security of electronic systems a critical factor. Attacks on digital systems can result in significant losses, impacting both the economy and national security. Therefore, it is essential to strengthen cybersecurity systems by upgrading security tools, enhancing the monitoring of digital systems, and developing information security technologies capable of anticipating the ever-evolving range of cyber threats (Edmon Makarim, 2010).

Furthermore, enhancing public digital literacy is a crucial component of efforts to combat cybercrime. Rapid technological advancements are often not matched by public understanding of how to use technology safely and responsibly. Many people still lack awareness regarding the dangers of cybercrime such as online fraud, personal data theft, phishing, and other forms of digital attacks. Low levels of digital literacy often leave individuals vulnerable to victimization due to a lack of caution when using information technology. Therefore, educational programs, outreach initiatives, and digital security campaigns are essential to foster public awareness regarding the importance of personal data protection and wise internet usage. These educational efforts can be implemented through educational institutions, mass media, and government programs aimed at improving public digital security (Ridwan Mansyur, 2019).

The transnational nature of cybercrime necessitates international cooperation in efforts to combat it. Cybercriminals can commit offenses from another country without being physically present where the victim is located. This situation creates challenges regarding the identification of perpetrators, the determination of legal jurisdiction, and the enforcement of the law. Consequently, inter-agency and international cooperation is essential, involving information exchange, mutual legal assistance, the development of cybersecurity technologies, and international law enforcement coordination. Such international cooperation is crucial for effectively addressing cybercrime, given that these offenses transcend national borders.

In addition to the various efforts already undertaken to combat cybercrime, it is essential to establish an integrated and sustainable national cybersecurity system. In today's digital era, cybersecurity is no longer understood merely as the protection of computer devices or internet networks; rather, it encompasses the protection of all electronic systems, data, information, and digital infrastructure utilized in the activities of both society and the state. Rapid technological advancements have created a situation where nearly every sector of life ranging from the economy, education, government, healthcare, banking, and transportation to national defense relies on digital systems. This reality demonstrates that the security of cyberspace has become a crucial element in maintaining national stability and ensuring the continuity of modern societal activities (Andi Hamzah, 2012).

The widespread advancement of digital transformation has also heightened the risk of attacks on strategic digital infrastructure. Digital infrastructure currently serves as the backbone for various public services utilized by the community; electronic banking systems, communication networks, government data centers, hospitals, and modern transportation systems all rely heavily on information technology. Should such infrastructure suffer disruptions due to cyberattacks, the consequences could extend beyond economic losses to disrupt public services and undermine social stability. Consequently, protecting digital infrastructure has become a top priority in national cybersecurity policy (M. Arsyad Sanusi, 2011).

Recent developments indicate that cyber threats are no longer perpetrated solely by specific individuals but also by organized groups, international networks, and even entities driven by specific political or economic agendas. Contemporary cyberattacks range from large-scale data theft, the sabotage of electronic systems, and security network breaches to the deployment of malicious software (malware) designed to damage specific systems. These threats demonstrate that cybercrime has undergone significant evolution regarding the perpetrators, methods, and targets involved. Consequently, cybersecurity systems must be continuously developed to adapt to the increasingly complex nature of these threats (Efa Laela Fakhriah, 2019).

In addition to strengthening digital security systems, enhancing the quality of human resources is a crucial factor in combating cybercrime. Technological advancements necessitate a workforce possessing the requisite skills and competencies in information technology. Addressing cybercrime requires professionals with specialized expertise such as digital forensics, computer network security, information systems analysis, programming, and digital footprint identification. These capabilities are essential because the process of handling cybercrime differs significantly from that of conventional criminal offenses (Sutan Remy Sjahdeini, 2009).

Improving the quality of human resources can be achieved through various means, such as developing information technology-based educational curricula, providing technical training, facilitate professional certification, conducting cybersecurity research, and fostering collaboration with educational and related institutions. Beyond law enforcement personnel, capacity building is also essential for other sectors, including government employees, electronic system operators, and the general public. With a workforce possessing adequate capabilities, the prevention and handling of cybercrime can be carried out more effectively (M. Yahya Harahap, 2010).

Beyond institutional and technological aspects, public participation plays a crucial role in efforts to combat cybercrime. The public is not merely an object of legal protection but also an active participant in safeguarding the digital space. Low public awareness regarding information security is often a contributing factor to the rising number of cybercrime victims. Many people still fail to grasp the importance of protecting personal data, using digital security systems correctly, or understanding the risks associated with unsafe internet usage.

Public behavior regarding technology use often creates vulnerabilities that cybercriminals exploit. Factors such as using easily guessable passwords, the habit of opening unknown links, carelessly sharing personal data, and a lack of vigilance regarding digital activities frequently lead to people becoming victims of cybercrime. Therefore, enhancing digital literacy is a crucial preventive measure for creating a secure digital environment. Digital literacy programs can be implemented through formal education, public campaigns, community training, and digital information channels that are easily accessible to the general public (Achmad Ali, 2009).

Furthermore, the rapid evolution of cybercrime necessitates continuous updates to legal regulations. The law is intended to keep pace with societal developments acting as a tool for social engineering yet, in practice, technological advancements often outpace the legal system's ability to accommodate the resulting changes. This situation can create a "legal gap," potentially giving rise to new forms of crime that are not yet clearly addressed by existing legislation. Consequently, regulations must be evaluated and updated periodically to ensure the legal system remains capable of responding to the highly dynamic nature of digital technology.

Legal reform entails not only the enactment of new regulations but also the refinement of law enforcement mechanisms and adaptation to global technological advancements.

Adaptive regulations are essential to provide law enforcement agencies with a robust legal basis for addressing the ever-evolving forms of cybercrime. Furthermore, the formulation of regulations must strike a balance between public protection, legal certainty, and respect for human rights in the use of digital technology.

Thus, it is evident that efforts to combat cybercrime cannot rely on a single approach. Law enforcement must go hand in hand with enhancing technological security, strengthening human resources, raising public awareness, updating legal regulations, and bolstering international cooperation. Such a comprehensive and integrated approach is expected to create an effective protection system against the various cybercrime threats that continue to evolve alongside advancements in information technology.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

1. Cybercrime is a modern form of crime that has emerged as a consequence of the rapid development of information and communication technologies. While technological advancements offer numerous benefits to society such as facilitating access to information, communication, economic transactions, education, and public services they also create opportunities for the misuse of technology to commit criminal acts in cyberspace. Cybercrime manifests in various forms, including hacking, cracking, phishing, personal data theft, online fraud, malware distribution, and cyberbullying, alongside other digital offenses that continue to evolve alongside technological progress. The rise of cybercrime in Indonesia is driven by several factors, such as high internet usage, low levels of digital literacy among the public, weak electronic security systems, and a lack of public awareness regarding the importance of personal data protection. These factors demonstrate that cybercrime is not merely a technological issue but is also linked to social, economic, and educational factors, as well as public behavior regarding the use of information technology.
2. From a legal perspective, cybercrime is a criminal offense with characteristics distinct from conventional crimes, thereby requiring specialized handling. Indonesia has established various regulations to address cybercrime, notably the Law on Electronic Information and Transactions, which serves as the legal foundation for handling cyber offenses. However, law enforcement efforts still face numerous challenges, such as jurisdictional issues, difficulties in establishing proof via digital evidence, limited human resources and technological infrastructure, and the fact that cybercrime often transcends national borders. Consequently, combating cybercrime cannot rely solely on the imposition of criminal sanctions; it must also be supported by enhanced cybersecurity, updated legal regulations, improved public digital literacy, strengthened law enforcement capacity, and sustained national and international cooperation to ensure effective handling of cybercrime.

Recommendations

1. The government and law enforcement agencies are expected to continuously improve the quality of regulations and undertake legal reforms capable of keeping pace with the rapid evolution of information technology. Furthermore, enhancing human resource capabilities through education, training, and skill development in information technology, cybersecurity, and digital forensics must be pursued on an ongoing basis. This is crucial to ensure that law enforcement personnel possess the necessary competence to handle the ever-evolving and increasingly complex forms of cybercrime. The government also needs to strengthen the national digital security system and improve inter-agency coordination to optimize efforts in preventing and enforcing the law against cybercrime.
2. The public needs to raise awareness and deepen their understanding of the importance of digital security in daily life. Information technology must be used wisely and responsibly,

with a clear understanding of the risks associated with internet usage. People need to exercise greater caution in protecting personal data, employ robust account security systems, avoid suspicious links, and stay informed about the evolving nature of cyber threats. Furthermore, efforts to enhance digital literacy through education, public outreach, and training must be sustained; this ensures that the public does not merely use technology but also actively contributes to preventing cybercrime and fostering a digital environment that is safe, secure, and responsible.

REFERENCES

- Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2010.
- Achmad Ali. *Menguak Teori Hukum dan Teori Peradilan*. Jakarta: Kencana, 2009.
- Adami Chazawi dan Ardi Ferdian. *Tindak Pidana Informasi dan Transaksi Elektronik*. Malang: Bayumedia Publishing, 2015.
- Agus Rahardjo. "Cyber Crime dan Upaya Penanggulangannya dalam Perspektif Teknologi Informasi." *Jurnal Dinamika Hukum*, Vol. 13, No. 2, 2013.
- Ahmad M. Ramli. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama, 2010.
- Andi Hamzah. *Aspek-Aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika, 2012.
- Barda Nawawi Arief. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2011.
- Barda Nawawi Arief. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2010.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers, 2014.
- Didik M. Arief Mansur dan Elisatris Gultom. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2009.
- Dikdik M. Arief Mansur dan Elisatris Gultom. *Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2005.
- Edmon Makarim. *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Jakarta: RajaGrafindo Persada, 2005.
- Edmon Makarim. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: RajaGrafindo Persada, 2010.
- Efa Laela Fakhriah. *Bukti Elektronik dalam Sistem Pembuktian Perdata*. Bandung: Alumni, 2019.
- Hikmahanto Juwana. *Hukum Internasional dalam Perspektif Indonesia*. Jakarta: Obor Indonesia, 2010.
- Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.
- Khairul Umam. "Kebijakan Penanggulangan Kejahatan Siber di Indonesia." *Jurnal Rechtsvinding*, Vol. 9, No. 2, 2020.
- Lilik Mulyadi. *Kapita Selekta Hukum Pidana Kriminologi dan Viktimologi*. Jakarta: Djambatan, 2007.
- M. Ali Zaidan. *Kebijakan Kriminal*. Jakarta: Sinar Grafika, 2015.
- M. Arsyad Sanusi. *Hukum Teknologi dan Informasi*. Bandung: Pustaka Setia, 2011.
- M. Hamdan. *Politik Hukum Pidana*. Jakarta: RajaGrafindo Persada, 2012.
- M. Yahya Harahap. *Pembahasan Permasalahan dan Penerapan KUHAP*. Jakarta: Sinar Grafika, 2010.
- Maskun. *Kejahatan Siber Cyber Crime Suatu Pengantar*. Jakarta: Kencana, 2013.
- Muladi dan Barda Nawawi Arief. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni, 2010.
- Republik Indonesia. *Kitab Undang-Undang Hukum Pidana (KUHP)*.

- Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Ridwan Mansyur. "Penegakan Hukum Tindak Pidana Siber dalam Perspektif Hukum Nasional dan Internasional." *Jurnal Hukum dan Peradilan*, Vol. 8, No. 2, 2019.
- Rika Ratna Permata. "Problematisasi Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *Jurnal Legislasi Indonesia*, Vol. 17, No. 2, 2020.
- Satjipto Rahardjo. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2006.
- Satjipto Rahardjo. *Penegakan Hukum Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing, 2009.
- Sigid Suseno. "Yurisdiksi Tindak Pidana Siber dalam Perspektif Hukum Pidana Indonesia." *Jurnal Hukum IUS QUIA IUSTUM*, Vol. 20, No. 1, 2013.
- Sinta Dewi Rosadi. "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia." *Jurnal Veritas et Justitia*, Vol. 4, No. 1, 2018.
- Sinta Dewi Rosadi. *Perlindungan Privasi dan Data Pribadi dalam Era Digital di Indonesia*. Bandung: Refika Aditama, 2021.
- Sinta Dewi. *Cyberlaw Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjadjaran, 2009.
- Siswanto Sunarso. *Hukum Informasi dan Transaksi Elektronik*. Jakarta: Rineka Cipta, 2009.
- Soejono Dirdjosisworo. *Pengantar Ilmu Hukum*. Jakarta: RajaGrafindo Persada, 2010.
- Soerjono Soekanto. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: RajaGrafindo Persada, 2011.
- Sutan Remy Sjahdeini. *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafiti, 2009.
- Teguh Prasetyo. *Kriminalisasi dalam Hukum Pidana*. Bandung: Nusa Media, 2011.
- Widodo. *Hukum Pidana di Bidang Teknologi Informasi Cybercrime Law*. Yogyakarta: Aswaja Pressindo, 2013.