THE ROLE OF CYBER LAW IN ADDRESSING CYBERCRIME IN INDONESIA

Junaidi Lubis[1*], Muhammad Koginta Lubis,[1] Haris Dermawan[1]
[1]Battuta University, Medan City, Indonesia
*Correspondent Email: junaidilubis67@yahoo.co.id

Abstract
Cybercrime has become a real threat in today's digital age. Technological developments cannot be stopped, including legal issues. The law must also be able to anticipate that technological developments must be supervised so as not to cause new crimes in the digital world. Technological developments do not necessarily always have a bad impact on people's lives, therefore it needs to be limited for the comfort and safety of the community in the digital space so as not to take new victims. Method in this study is normative legal research and the approach carried out is a conceptual approach. The results of the study indicate that with the existence of cyber law in Indonesia, every crime that occurs in the digital world can be solved with cyber law whose function is as a legal umbrella in handling cybercrimes that befall every citizen.
Keywords: Cyber, Cyber Law, The Role of Law.

Abstrak
Kejahatan siber telah menjadi ancaman yang nyata diera digital pada saat ini. Perkembangan tekhnologi memang tidak dapat dibendung termasuk dalam soal hukum. Hukum juga harus mampu mengantisipasi agar perkembangan tekhnologi harus diawasi agar tidak menimbulkan kejahatahan baru dalam dunia digital. Perkembangan tekhnologi tidak serta merta selalu membawa dampak buruk bagi kehidupan Masyarakat maka dari itu perlu dibatasi demi kenyamanan dan keamanan Masyarakat dalam ruang digital tidak sampai memakan korban baru. Adapun metode dalam penelitian ini ialah penelitian hukum normatif (normative legal research) dan pendekatan yang dilakukan ialah pendekatan konsep. Tujuan dari penelitian ini ialah untuk menganalisa bagaimana peranan hukum cyber law dalam mengatasi kejahatan siber yang ada di Indonesia. Hasil penelitian mengindikasikan bahwasannya dengan adanya hukum cyber law di Indonesia setiap kejahatan yang terjadi dalam dunia digital dapat diselesaikan dengan hukum siber law yang fungsinya ialah sebagai payung hukum dalam penanganan kejahatan cyber yang menimpa setiap warga negara.
Kata Kunci: Siber; Hukum Siber; Peranan Hukum.

DOI: 10.24252/aldev.v7i3.60482

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

INTRODUCTION

The digital world must be understood as something commonplace in the context of contemporary society. The rapid enhancement of the digital world has brought many people to new knowledge, transforming what was once manual into digital or virtual. With the rapid advancement of technology, the use of electronic media has also seen a significant increase, that in turn has gradually influenced various aspects of society, comprising culture, social life, politics, and the legal system, all of that are evolving in tandem with the changing times (Labib 2010).

The shift by the real world to the digital world has increased significantly, so that in the future this issue must receive special attention by the state so that technological advances do not have a negative impact on people's lives, especially in the use of digital technology. There is an adage in society that crime arises by society itself, so that the shift to the digital world must be interpreted properly in the lives of society and the legal world. Crime will also increase if the law does not take part in addressing issues that arise in society in the increasingly widespread enhancement of the digital world (Afitrahim 2012). A society has values that thrive in togetherness amid differences, so this must be able to bring about many changes that can transform the paradigm of society for the better, comprising the shift in the virtual world as mentioned above.

The values that exist in society are to protect society itself by disturbances that can disrupt order in civilization so that the remains secure by incorporating these principles into specific laws, that is referred to as cyber law. In this case, the state gives security to every citizen so that they do not become victims of cybercrime in Indonesia (J Remmelink 2014). The term "cyber" is often associated with computer systems and networks connected to the internet. As a outcome, the term "cyber" has a broad correlation, and the exact meaning of the word "cyber" itself has not yet been definitively established. The word "cyber" can function as a noun or an adjective, and different countries interpret it differently. At least 26 definitions of the term "cyber" exist, comprising (Azmi 2020).

1. Physical infrastructure is closely connected to communication networks and the internet.
2. Systems are closely connected to business data systems, infrastructure systems, and services.
3. Devices typically refer to hardware such as computers, servers, and routers connected to the internet
4. The virtual world is the digital world connected to the flow of national activities.

The term "cyber" is now more accurately applied to physical infrastructure, computer networks, and data systems in the virtual world, that include data or non-data relationships among individuals, organizations, governments, and society, as well as interconnected hardware devices on a broader scale.

Cybercrime has become a new dimension in the world of crime, so the law must be specific to deal with crimes of this nature. According to Barda Nawasi Arif, "the new form of anti-social behavior refers to the evolution of crime into cybercrime, such as digital crimes like cybercrime (Barda Nawawi Arif 2017). Etymologically, cybercrime is real crime that can disrupt economic growth and social enhancement in a country. data technology touches various aspects of human life and has led to the emergence of electronic-based crime (Adinda Evita Puspa 2024). According to Rene L. Pattiradjawane, the concept of cyberlaw evolved by computers, creating a space accessible to all through the internet with unlimited reach. This has caused concern among the public and law enforcement agencies, prompting the establishment of special rules as a form of protection for every citizen to ensure they are protected when

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

they become victims of cybercrime.

According to Jhon Sipropoulus, cybercrime is characterized by efficiency and quick access, posing a unique challenge for law enforcement agencies when it comes to handling cybercrime cases, as it is difficult to uncover the perpetrators who rely on data systems and the internet to carry out their crimes (Galuh Kartiko 2013). The handling of cybercrime by the National Cyber and Encryption Agency differs by the handling of general crimes, so this type of crime receives special attention because it requires the use of devices that must be connected to the internet for detection purposes.

In Indonesia itself, the term used to refer to cybercrime or computer misuse is computer crime or cybercrime. This is because computers are tools used for or as a means of committing crimes or criminal acts. However, in reality, computers and computer data are also objects of criminal acts. Therefore, in this context, computer crime has a much broader meaning than simply cybercrime, that is closely connected to the objects of criminal acts themselves (Peradilan 2004). Cybercrime is defined as computer crime committed in cyberspace, that is a separate space that emerges in various commercial transactions and other valuable data in cyberspace. The concept of cyberspace itself is defined as a space that is connected and communicates utilizingthe internet to carry out activities (Rahmawati 2017).

The term cyberspace comes by the word cybermetics, that initially did not describe the relationship among internet networks. Cyber and technology, when traced back to their origins, come by the Greek word technikos, that means art or skill in a logical sense, i.e., the science or principles found in the word cyber (software) (Brantas 2014). Cybercrime is becoming increasingly diverse alongside the enhancement of internet technology, so cyber law must also be able to give answers to the technological advancements in question. No matter how advanced technology becomes, cyber law must serve as a shield to protect every citizen who navigates the internet in accessing data, all in accordance with existing laws and regulations.

The latest enhancement in cyber law is attacks through open source, that have become quite common among cybercriminals after malware. The method used is to find weaknesses in users who do not trust search applications, commonly referred to as open source (Muhammad Danuri dan Suharnawi 2017). A survey conducted in 2016 by the Indonesian Internet Service givers Association (APJII) revealed that 132.7 million people in Indonesia have access to the internet. The number of internet users in Indonesia is reported to continue increasing every year. The number of internet users in Indonesia continues to grow due to the ease of access to the internet and the affordability of internet-enabled devices. Seventy percent (70%) of internet users in Indonesia access the internet utilizingmobile devices. This indicates that internet usage at home is very low, while internet usage on mobile phones is very high.

The enhancement of internet technology has led to the emergence of a new type of crime known as cybercrime, that exploits the internet network. Fraud, hacking, data interception, email spamming, and data manipulation utilizingcomputer programs to access other people's data are some examples of cybercrime that have emerged in Indonesia. Victims, the economy, and the dignity of the Indonesian state have suffered greatly by cybercrime. To address these internet violations, specialized institutions are needed, both government and non-government (NGOs). In Indonesia, the Indonesian Computer Emergency Response Team (IDCERT) has been established. To report computer security issues, individuals can contact this unit. However, to achieve its objectives quickly, support by all parties is required.

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

METHOD

The author employs the normative legal research method (Muhaimin 2020). This method is used to examine legislation, legal literature, and other documents connected to cyber law policies in Indonesia in addressing cybercrime (Zainuddin Ali 2016). This method involves a comprehensive analysis of relevant legal elements. The conceptual approach used is to examine relevant legal theories (Sugiyono 2013). The data collected in this study were obtained through the analysis of legislation, court decisions, legal journals, textbooks, and other relevant documents. To conduct this analysis, a descriptive analytical approach was applied (Hardani, Nur Hikmatul 2020). This method describes the current cyber law policy and analyzes its effectiveness in handling cybercrime.

RESULT AND DISCUSSION

1. *The Role of Cyber Law*

Legal aspects originating by cyberspace law, that covers every aspect connected to individuals or legal entities that use and utilize internet technology, beginning when a person first accesses the internet and enters the virtual world. According to Jonathan Rosenoer in his book Cyber Law - Internet Law, the scope of cyber law includes:

a. Copyright
b. Trademarks
c. Defamation
d. Hate Speech
e. Hacking, Viruses, Illegal Access
f. Internet Resource Management
g. Privacy 8. Liability
h. Criminal Offenses
i. Procedural Issues (Jurisdiction, Investigation, Evidence, and Others)
j. Electronic Contracts
k. Pornography
l. Robbery
m. Consumer Protection
n. E-Commerce, E-Government
o. The importance of cyber law regulation in Indonesia is:
p. Legal certainty
q. To address the impacts arising by the use of data technology due to
r. The existence of global factors, namely free competition and open markets (Darmawan Napitupulu 2017).

Law has the purpose of adapting to various activities of society that continue to evolve over time. According to Sudarto, the main objective of law is to achieve the welfare of society, both physically and spiritually, so that actions that harm society can be avoided. Cybercrime falls under the category of criminal acts that can have a negative impact on society, both materially and spiritually. Due to legal and judicial constraints in Indonesia, cybercriminals are often difficult to apprehend. These criminal acts usually involve perpetrators by other countries, even though they have legal implications in Indonesia. There are three types of jurisdiction that play an crucial role in international law, namely legislative jurisdiction, enforcement jurisdiction, and judicial jurisdiction (Saputra 2023).

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

Indonesian legislation has regulated various provisions regarding crimes connected to cybercrime in some different articles. The Criminal Code (KUHP) is not yet fully capable of dealing with cybercrime because it does not cover all crucial aspects of crimes in the virtual world. In terms of evidence, the KUHP adheres to the principle of legality, that means that an act cannot be considered a crime if it is not regulated by law. However, Law No. 48 of 2009 on Judicial Power states that courts are obligated to examine and adjudicate a case devoid of rejecting it due to legal uncertainty (Sunaryo 2014).

The legal world has adopted the practice of expanding the interpretation of legal principles and norms to address cybercrime. In essence, such crimes can be prosecuted utilizinganalogies or examples by some articles of the Criminal Code (KUHP), such as Article 362 relating to carding cases, Article 378 relating to fraud, and Article 311 relating to defamation, that can be applied in handling various types of cybercrimes.[1] Therefore, there is no need for new legislation to address crimes committed through the internet; the provisions of the KUHP remain applicable. In such cases, judges may employ a broad interpretation of the relevant provisions of the KUHP pertaining to cybercrimes devoid of explicitly referencing them. Additionally, it is crucial for judges to uphold the principles of justice and the legal standards prevailing in society (M Nanda Setiawan, Mariani Safitri 2022).

In response to current enhancements, to address and prevent cybercrime, regulations have been established specifically governing criminal offenses in the field of data technology, as contained in Law No. 1 of 2024 amending Law No. 11 of 2008 on data and Electronic Transactions. It is hoped that this Law on data and Electronic Transactions will serve as a source of strength to regulate and enforce order in activities connected to the use of data technology (I Gusti Bagus Agung Kusuma Atmaja 2025).

According to Widodo, cybercrime is defined as actions carried out by individuals, groups, or legal entities that utilize computers as tools to commit crimes, as well as being the target of such crimes. Various types of crimes commonly occurring in cyberspace include:

a. Illegal access to computer systems and services is a type of crime that occurs when someone attempts to hack or enter a computer network devoid of authorization, or devoid of the consent or knowledge of the computer network owner.

b. Illegal content refers to activities that constitute cybercrime through the dissemination of data or data on the Internet regarding matters that are untrue, contrary to norms, and may be considered unlawful or disruptive to public order.

c. Falsified data is a form of crime in the digital realm that is carried out by manipulating data in crucial documents stored as unscripted documents via the internet. This criminal act generally targets e-commerce documents by creating the impression of "typing errors" that ultimately benefits the perpetrator, as victims tend to enter personal data and credit card numbers that are likely to be misused by the perpetrator.

d. Cyber espionage is a form of crime that uses the internet as a tool to monitor others. This is done by infiltrating the computer network systems of the target.

e. Cyber sabotage and extortion: This type of crime usually involves disrupting, damaging, or destroying data, programs, or computer networks connected to the internet. This is typically done by infiltrating logic bombs, viruses, or specific programs that render data, programs, or computer

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

networks unusable or unable to function as intended.

f. Intellectual property rights violations, this method of crime targets the intellectual property rights of others on the internet. For example, copying the appearance of someone else's website is illegal.

g. Privacy violations, this type of crime usually focuses on personal data stored in digital personal data forms. If this data is known by others, it can cause material and immaterial losses to the victim. Examples include the leakage of credit card numbers, ATM PINs, and so on (Antoni 2017).

Specific regulations governing crime are necessary to combat crime. This also applies to cybercrime; cyber law is needed to deal with cybercrime. Cyber law in Indonesia does not yet have a clear official term. However, data law is one of the many terms used (Lita Sari Marita 2015). The enforcement of laws against violations of technology and data is regulated by cyber law. These penalties are necessary to regulate people's actions in various internet-based activities. In addition, because activities on the internet can be carried out freely and are not limited by national borders, cyber law also serves as a restriction. Although virtual in nature, cyber activities have an impact on people's daily lives (Ahmad Ramli 2010).

In today's trade practices, people tend to prefer shopping online rather than visiting physical stores. This shift became even more prominent during the COVID-19 pandemic, when the government imposed restrictions on gatherings to break the chain of virus transmission. With the growing public interest in online shopping, many online stores began offering a payment system where the payment is made only when the order arrives, commonly known as the Cash on Delivery (COD) system.

2. *Handling Cybercrime in Indonesia*

With the advancement of technology, Indonesia must implement specific cyber law. Experts in this field argue that conventional laws cannot anticipate the rapid enhancement of technology (Riko Nugraha 2021). The level of cybercrime in Indonesia continues to increase, according to a report by cybersecurity company Kaspersky. In the first quarter of 2022, there were around 12 million cybercrime threats in Indonesia, a significant increase by the same period in 2021. Cyber law, also known as cyber law, is a legal aspect derived by "Cyberspace Law" and covers every aspect connected to individuals or legal entities that use and utilize internet or electronic technology, beginning when they go online and enter the cyber or virtual world. In countries that have advanced in the enhancement of their cyber laws, this law is crucial for addressing cybercrime (Lubis et al. 2024).

For preventive measures, cyber law is vital in addressing cyber crimes and controlling them. In the process of enforcing the law against crimes committed utilizingelectronic and computer means, comprising money laundering and terrorism, cyber law will serve as the foundation. In Indonesia itself, cyber law is urgently needed in addressing cybercrime, as such crimes cannot be stopped due to the rapid advancement of technology. Supporters of cyber law believe that Indonesia must have cyber law because conventional law cannot anticipate the rapid enhancement of the virtual world (Haris Dermawan, Junaidi Lubis 2025).

At the United Nations Conference X/2000 in Vienna, Austria, the term cybercrime was divided into two categories. The term cybercrime is used in a narrow sense to refer to computer offenses, and the term cybercrime is used in a broad sense to refer to offenses connected to computers. The document states:

a. Cybercrime narrow computer crime: any legal behavior directed by electronic operations that targets the security of computer systems and data processed by them.

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

b. Cybercrime in a broader sense (computer-connected crime): any illegal act done in connection with a computer system or network, comprising illegal possession, offering, or distribution by means of a computer system or network.(Barda and Arif 2001)

c. computer system or network. utilizingthe means of a computer system or network (by means of a computer system or network) within a computer system or network (in a computer system or network).

d. Against computer systems or networks. by this definition, in a narrower context, cybercrime is computer crime directed at computer systems or networks. In a broader sense, cybercrime encompasses all new types of crime targeting computers, computer networks, and users, as well as various forms of traditional crime now committed with the aid of or utilizingcomputer devices.

Digital transactions are legal actions carried out utilizingcomputers, computer networks, or various other electronic media (*Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.*, n.d.). Furthermore, a computer is an electronic data processing device that can be used for typing, calculating, or running systems that perform logical and arithmetic functions in its storage. With this definition, electronic transactions have a very broad scope, both in terms of their subjects—every individual or entity that uses computers, computer networks, or other electronic media—and their objects, that include various products and services.

In practice, electronic transactions are conducted through the use of a connected network, also known as the internet, that consists of various sizes of computer networks that are interconnected through electronic communication media and have the ability to access all services offered by other networks.(Daniel H Purwadi 2005) The ITE Law will serve as the legal basis for enforcing laws against crimes committed utilizingelectronic and computer means, comprising money laundering and terrorism-connected crimes, both in terms of prevention and the handling of criminal acts.(Nasrullah 2003)

The following will describe the components that influence law enforcement against cybercrime. Legal factors greatly influence law enforcement against cybercrime. Because cybercrime falls under the category of transnational crime, the laws applied in this discussion are Indonesian laws. International legal principles and principles are used if not regulated by national law. The handling of cybercrime by law enforcement officials is greatly influenced by the existence of regulations. There are some laws connected to data technology, particularly regarding crimes involving the internet prior to the enactment of the ITE Law. The enforcement of cybercrime laws before the enactment of the ITE Law was carried out by interpreting cybercrime within the context of the Criminal Code (KUHP) and other laws connected to the enhancement of data technology, comprising:

a. Law No. 14 of 2008 on Public data Disclosure

b. Law No. 36 of 1999 on Telecommunications

c. Law No. 19 of 2002 as amended by Law No. 28 of 2014 concerning Copyright

d. Law No. 25 of 2003 on Amendments to Law No. 15 of 2002 on Criminal Acts

e. Money Laundering as amended by Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering

f. Law No. 15 of 2003 on the Eradication of Terrorism-connected Criminal Acts

g. And so on.

In its enhancement, regulations on cyberspace and cybercrime are governed by Law No. 11 of 2008 on Electronic Data and Transactions, as amended by Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Data and Transactions, which serves as the legal basis. It is hoped that this ITE Law can serve as a tool for controlling and enforcing order for all activities that utilize data technology, not only limited to internet activities, but also encompassing all activities that use computers and other electronic devices.

In essence, this regulation meets the criteria for legal implementation by legal, sociological, and philosophical perspectives. by a philosophical perspective, the presence of Law No. 11 of 2008 on data and Electronic Transactions, as amended by Law No. 19 of 2016 on Amendments to LawLaw Number 11 of 2008 on data and Electronic Transactions, is based on the mandate contained in Article 28F of the 1945 Constitution of the Republic of Indonesia. (Pasal 28F UUD 1945 bahwasannya Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi d n.d.)

This law regulates all matters relating to activities on the internet, computer devices, and other electronic instruments. by a sociological perspective, Law No. 11 of 2008 on data and Electronic Transactions, as amended by Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on data and Electronic Transactions, is of great importance in regulating various activities of individuals interacting with one another in the virtual world. The need for regulations to protect the interests of internet users in accessing various data has been driven by the dynamics of global data. The Constitution of Law No. 11 of 2008.

Simply put, cybercrime can be defined as a criminal act committed with the intention of gaining personal profit while harming others through a computer network or the internet.(Rafi Septia Budianto Pansariadi 2023) The cyber world still needs regulations to govern all activities involving technology. The purpose of these regulations is not only to protect the interests of society but also to prevent criminal acts. These regulations also give law enforcement officials with a basis for handling cybercrime cases in Indonesia. Criminal law policy, also known as criminal policy, is a combination of art and science, according to Marc Ancel. Its ultimate goal is to help courts and lawmakers make better decisions about how to apply criminal laws. The supremacy of the law and the individuals responsible for enforcing court decisions are central to this policy (Pristiono 2020).

The purpose of policy in combating crime is to improve criminal law rules, so criminal law policy is included in crime prevention policy (criminal policy). If cybercrime is truly considered a unique criminal activity that requires a different set of laws and regulations by the Criminal Code, then special regulations will be needed.(Ismail Koto 2021) Because computer forensic laboratories must operate abroad, the investigation and prosecution of cybercrime is hampered by these limitations. In addition, the image of judicial institutions is still poor, despite various efforts to encourage victims of cybercrime to report their cases to the police. This has led to an increase in the number of unreported cases in the handling of cybercrime. To create a society with an data culture, the enhancement of data technology, especially the internet, is very crucial to combat cybercrime.

Given the many obstacles that hinder the implementation of criminal law related to cybercrime, the

government and law enforcement agencies, comprising elements of society, especially universities, are responsible for working together to overcome these obstacles. By overcoming various existing problems, we can at least make progress in supporting the enforcement of criminal law connected to cybercrime. The author believes that identifying issues in the enforcement of criminal law against cybercrime can be done both within and outside the criminal justice system.

Internally, examples include reducing the likelihood of various issues arising within the criminal justice system, both formal and material. Officially, the challenges in the investigation, inquiry, and prosecution stages are that law enforcement officials have some limitations in understanding the problems of cybercrime case disclosure, which are certainly connected to the use of advanced technology and science (such as the internet and computers), as well as perpetrators who have special expertise that law enforcement officials do not have.

Given the rapid escalation of cybercrime in both quantity and quality, it is crucial to immediately address the shortage of resources for law enforcement officials. In addition, we must consider the process of proving cybercrime, which requires a complex system of evidence similar to that required for conventional crimes. Therefore, the author believes that one of the fastest steps law enforcement can take to address cybercrime is to resolve the various issues associated with these limitations, rather than focusing solely on problems from upstream to downstream.

Cyberattacks in Indonesia have increased every year. The types and variations of attacks differ by previous years, but some remain consistent. There are several factors that contribute to cybercrime, including the presence of perpetrators, their methods of operation, opportunities to commit crimes, crime targets, public responses to criminal acts, and existing regulations. Perpetrators who are more skilled in technology are usually able to illegally access other people's computer networks. Therefore, the tendency for perpetrators of cybercrime clearly involves individuals who are proficient in and understand aspects of the internet.

CONCLUSION

The ease of obtaining data through the internet has made everyone smarter. It is no longer necessary to read books and other learning materials to gain knowledge; now, you can find new knowledge by searching the internet at. However, even though knowledge can be easily obtained on the internet, it is crucial to note that the knowledge gained on the internet must be used wisely. This means that knowledge must be used for good, not for evil. It turns out that the virtual world can become a breeding ground for crime when used by irresponsible individuals. This has led to the emergence of the term cybercrime, that refers to illegal acts committed by irresponsible people when utilizingthe internet, or generally considered criminal acts that use computers and computer networks in the process. Along with the increase in internet usage, various types of crimes have also emerged.

If there are criminal acts, there should be sanctions for the perpetrators. This is the reason behind the emergence of cyber law, that regulates anyone who commits crimes in cyberspace. Almost all countries have established rules to deal with cybercrime. In the United States, there is the Uniform Electronic Transactions Act (UETA), while Singapore has the Electronic Transactions Act (1998) and the Electronic Communications Privacy Act (1996). In Indonesia, the ITE Law has been implemented since 2008. The government needs to pay serious attention to cybercrime because this issue is very common worldwide, especially in Indonesia, that appears to have a fairly high rate of cybercrime.

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

REFERENCES

Adinda Evita Puspa. 2024. "Peran Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia." Universitas Islam Sultan Agung.

Afitrahim. 2012. "Yurisdiksi Dan Transfer Of Preceeding Dalam Kasus Cybercrime." Universitas Indonesia.

Ahmad Ramli. 2010. *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.

Antoni. 2017. "KEJAHATAN DUNIA MAYA (CYBER CRIME)DALAM SIMAK ONLINE." *Nurani* 17 (02): 261–74. https://doi.org/https://doi.org/10.19109/nurani.v17i2.1192.

Azmi, Riza. 2020. "Sejarah Dan Konteks Terminologi Siber Majalah Cyber Defenze Community." Cybermagazine.Com. Jakarta. 2020.

Barda, and Nawawi Arif. 2001. "Laporan Konfrensi PBB X/2000." In *The Term Computer Related Crime Had Been Developed to Encompass Both the Entirely New Forms of Crime That Were Directed at Computers, Net Work and Their Users, and the More Traditional Form of Crime That Were Now Being Commited Whit Use or Assistence of C*, 249–50. Bandung: Ctra Aditya Bakti.

Barda Nawawi Arif. 2017. *Sari Kuliah Perbandingan Hukum Pidana*. Cetakan 1. Jakarta: Raja Grafindo Persada.

Brantas, Sugeng. 2014. "Defence Cyber Dalam Konteks Pandangan Bangsa Indonesia Tentang Perang Dan Damai." *Pertahanan Dan Bela Negara* 2 (2): 55. https://doi.org/10.33172/jpbh.v7i2.179.

Daniel H Purwadi. 2005. *Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia*. Jakarta: PT. Elex Media Komputindo.

Darmawan Napitupulu. 2017. "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional." *Deviance Jurnal Kriminologi* 1 (1): 107. https://doi.org/https://doi.org/10.36080/djk.595.

Galuh Kartiko. 2013. "Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau Dari Hukum Internasional." *Rechtldee* 8 (2): 1.

Hardani, Nur Hikmatul, dkk. 2020. *Metode Penelitian Kualitatif Dan Kuantitatif*. CV. Pustak. Yogyakarta.

Haris Dermawan, Junaidi Lubis, Muhammad Koginta Lubis. 2025. "Proteksi Hukum Dalam Peretasan (Pencurian) Data Pribadi Nasional." *Rio Law Jurnal* 6 (1): 347–61. https://doi.org/https://doi.org/10.36355/rlj.v6i1.1603.

I Gusti Bagus Agung Kusuma Atmaja. 2025. "PERANAN CYBER LAW DALAM PENEGAKAN HUKUM TERHADAP TINDAK PIDANA DUNIA MAYA (CYBER CRIME)." *AKTUAL JUSTICEJURNAL ILMIAH MAGISTER HUKUM PASCASARJANA UNIVERSITAS NGURAH RAI* 10 (01): 45. https://doi.org/https://doi.org/10.70358/aktualjustice.v10i1.1507.

Ismail Koto. 2021. "Cyber Crime According to the ITE Law." *IJRS: Internasional Journal Reglement Society* 2 (2): 103–10. https://doi.org/https://doi.org/10.55357/ijrs.v2i2.124.

J Remmelink. 2014. *Pengantar Hukum Pidana Material Prolegomena Dan Uraian Tentang Teori Ajaran Dasar*. Yogyakarta: Maharsa.

Labib, Abdul Wahib dan Mohammad. 2010. *Kejahatan Mayantara (Cybercrime)*. Cetakan Ke. Bandung: Refika Aditama.

Lita Sari Marita. 2015. "CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA." *Humaniora Universitas Bina Sarana Informatika* 15 (2). https://doi.org/https://doi.org/10.31294/jc.v15i2.4901.

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

Lubis, Junaidi, M H Baginda Harahap, S Pd, and M Kom. 2024. "HUKUM DIGITAL ANTARA TANTANGAN DAN PELUANG."

M Nanda Setiawan, Mariani Safitri, Lidya Lestari. 2022. "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia." *Datin Law Jurnal* 3 (2). https://doi.org/https://doi.org/10.36355/dlj.v3i2.931.

Muhaimin. 2020. *Metode Penelitian Hukum, Mataram: 2020, 56*. Mataram: University Press.

Muhammad Danuri dan Suharnawi. 2017. "Trens Cyber Dan Tekhnologi Informasi Di Indonesia." *Infokam* 8 (2): 58–59. https://doi.org/https://doi.org/10.53845/infokam.v13i2.133.

Nasrullah, T. 2003. "Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-Undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka Tentang 'Keamanan Negara.'" *Indonesia Police Watch Bersama Polda Metropolitan*, 2003.

Pasal 28F UUD 1945 bahwa Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi d. n.d.

Peradilan, Puslitbang Hukum dan. 2004. *Naskah Akademis Kejahatan Internet(Cyber Crime)*. Jakarta: Mahkamah Agung.

Pristiono, Agus. 2020. "KEBIJAKAN KRIMINAL (CRIMINAL POLICY) DENGAN KONSEP MEDIASI DALAM PROSES PENYIDIKAN TINDAK PIDANA UMUM (PENIPUAN DAN PENGGELAPAN) PADA BAGWASSIDIK DITRESKRIMUM POLDA SUMUT." *Ilmu Sosial, Politik Dan Hummanioramaniora* 4 (1): 34. https://doi.org/http://dx.doi.org/10.31604/jim.v4i1.2020.34-43.

Rafi Septia Budianto Pansariadi, Noenik Soekorini. 2023. "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya." *Binamulia Hukum* 12 (02): 287–98. https://doi.org/https://doi.org/10.37893/jbh.v12i2.605.

Rahmawati, Inue. 2017. "Analisis Manajemen Resiko Ancaman Kejahatan Siber." *Pertahanan Dan Bela Negara* 7 (2): 55. https://doi.org/https://doi.org/10.33172/jpbh.v7i2.179.

Riko Nugraha. 2021. "PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA." *ILMIAH HUKUM DIRGANTARA* 11 (02). https://doi.org/https://doi.org/10.35968/jihd.v11i2.767.

Saputra, et al. 2023. *TEKNOLOGI INFORMASI: Peranan TI Dalam Berbagai Bidang.* Jakarta: PT. Sonpedia Publishing Indonesia.

Sugiyono. 2013. *Metode Penelitian Kuantitatif, Kualitatif, Dan RD*. Bandung: Alfabeta.

Sunaryo, T. (n.d.). 2014. *Penemuan Hukum Dalam Proses Peradilan Pidana Di Pengadilan Negeri Pandeglang Berdasarkan Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman.* Jakarta.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. n.d.

Zainuddin Ali. 2016. *Metode Penelitian Hukum, 1st Edn*. Jakarta: Sinar Grafika Offset.