International Journal of Law, Crime and Justice
Volume.2, Number.1 Year 2025
e-ISSN: 3047-1362; p-ISSN: 3047-1370, Pages 108-121
DOI: https://doi.org/10.62951/ijlcj.v2i1.440
Available online at: https://international.appihi.or.id/index.php/IJLCJ

Application of Criminal Law in Online Gambling Case
(Case Study Decision No. 02/Pid.B/2022/PnPwk)

Wendi Darman Laia[1] , Martono Anggustin[2] , Lesson Sihotang[3]
[123] Faculty of Law, HKBP Nommensen University, Medan, Indonesia
wendidarman.laia@student.uhn.ac.id[1], martono.anggustin@uhn.ac.id[2], lesson.sihotang@uhn.ac.id

Abstrak : *This research discusses the application of criminal law in online gambling cases in Indonesia, with a focus on decision No. 02/Pid.B/2022/PnPwk. The development of information technology has led to the emergence of cybercrime, including online gambling, which has a negative impact on society. Through a normative research approach, this study analyzes the challenges faced in law enforcement related to cybercrime, as well as legal protection for victims. The results show that despite regulations such as the Electronic Information and Transaction Law (EIT Law), many provisions are considered ambiguous, resulting in legal uncertainty. Law enforcement is also hampered by a lack of technological understanding among law enforcement and limited international cooperation. Therefore, it is necessary to update regulations and increase technological capacity to strengthen efforts to handle online gambling in the digital era. This research is expected to provide insights for the development of legal policies that are more effective and responsive to the challenges of cybercrime.*

Keywords: *Criminal Law, Online Gambling, Cybercrime*

1. INTRODUCTION

Globally, information and communication technology has altered human civilization and societal behavior. Furthermore, the rapid advancement of information technology has led to profound societal transformations and the erasure of international borders. Nowadays, information technology is a double-edged sword because, while it advances civilization and improves human welfare, it also serves as a powerful platform for illegal activity. The rise of a new kind of crime called cybercrime is one consequence of technological advancement.

Cybercrime is a type of criminal activity that is typically committed online and involves computers. Online gambling is one type of cybercrime. According to Article 303, paragraph (3) of the Criminal Code, gambling is defined as any game in which the player's talent or experience has an impact, but luck is typically the only factor that determines the likelihood of making money. This definition covers all rules pertaining to the outcomes of contests or other games that are played by people other than the competitors, in addition to a number of other pertinent rules.

"Cybercrime is now rampant in five major cities in Indonesia and at a fairly high level of concern and is carried out by hackers who are mostly young people who seem creative but in fact they steal credit card numbers via the internet," according to research by information technology specialist Roy Suryo. There are two types of cybercrime: cybercrime in the broad sense and cybercrime in the limited meaning. The restricted definition of cybercrime is a crime

Received: January 10, 2024; Revised: January 25, 2025; Accepted: February 12, 2025; Online Available: February 17, 2025

against a computer system, whereas the broad definition include crimes against a computer system or network as well as crimes involving the use of computer facilities.[1]

Given the current state of the law, it is crucial to consider the effects of scientific advancements and technological advancements that have been abused as criminal tools in order to predict the direction of legal policy. Therefore, criminal law can be used to combat cybercrime, especially in this instance with regard to the contents of reliable evidence.

The evidence needs to be organized in such a way that it can be used in the legal process, ensuring that every action taken by cybercriminals can be accounted for. Clear and firm legal policies are needed to provide protection to the community and encourage effective law enforcement in facing new challenges arising from technological developments.

It is considered to be of utmost importance because, in the application of criminal law, the basis for determining whether or not an individual is guilty of a crime is whether or not his actions can be held accountable (the element of guilt) and whether or not they are supported by legitimate evidence (the principle of legality). According to the Criminal Code's Article 1 paragraph (1), "Nullum delictum nulla poena sine praevia lege poenali"—or, to put it another way, "no criminal act, no punishment, without prior criminal law regulations"—this way of thinking is consistent with the application of the principle of legality in criminal law (KUHP).[2]

There is actually no legal vacuum when it comes to cybercrime; this is what happens when the legal science interpretation approach is applied, and this is what law enforcement officials should do when handling novel conduct that are not expressly covered by the law. The problem becomes different if there is a political decision to determine *cyber crime* in separate legislation outside the Criminal Code or other special laws [3]. However, in the issue of this interpretation, the judges who interpret it fall into the category of fraud, some also include it in the category of theft. For that, it is actually necessary to develop an understanding of information technology for judges so that the interpretation of a form of *cyber crime* into articles in the Criminal Code or other laws is not confusing.

The application of criminal law in handling *Cybercrime cases* in Indonesia faces various challenges. Although there are regulations that govern it, such as the Electronic

---

[1] Muhammad Anthony Aldriano . " *Cyber Crime in the perspective of criminal law* ". Jakarta: Citizenship Journal Vol. 6 No. 1 June 2022 p.

[2] Republic of Indonesia Law N o. 1 of 2023 concerning the Criminal Code (KUHP)

[3] Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia 2008 Number 58

Information and Transactions Law (UU ITE) No. 11 of 2008, many provisions in the law are considered ambiguous. This often causes confusion in law enforcement and different interpretations among law enforcers [4]. For example, several articles in the ITE Law are considered unclear in defining the types of cybercrime , which can result in legal uncertainty for perpetrators and victims.

Criminal law as a law enforcement tool has an important role in dealing with this crime. However, the application of criminal law in the context of cyber crime, especially online gambling, faces various challenges. Although Indonesia already has regulations such as the Electronic Information and Transactions Law (UU ITE), many provisions in the law are considered ambiguous and difficult to implement. The lack of understanding among law enforcement officers regarding information technology is also a significant obstacle, resulting in difficulties in investigating and prosecuting cases related to cyber crime.

In this study, the formulation of the problem is the criminal law process against *Cyber* perpetrators and the legal protection provided to victims of *Cyber crime.* Therefore, the author wants to discuss more deeply about the problem of online gambling. Thus, the purpose of this study is to determine the criminal law process against *Cyber perpetrators* and the legal protection provided to victims of *Cyber crime* is important to understand how criminal law is applied in handling cases like this, especially considering the complexity of digital evidence, jurisdictional boundaries, and the development of the perpetrators' modus operandi. This title is also relevant to identifying possible legal loopholes and formulating more effective law enforcement strategies in the digital era.

2. METHOD

The object of this research is the application of criminal law in *cyber crime cases* , especially in the context of decision No. 02/Pid.B/2022/PnPwk issued by the Pangkalan Brandan District Court. This study will analyze how criminal law is applied to violations that occur in the *cyber realm* , as well as to identify the challenges and effectiveness of the application of law in these cases. The main focus will be given to the legal, procedural aspects, and the consequences of the decision on law enforcement in Indonesia.

The research method used in this study is normative research. According to Soejorno Soekanto, the normative legal research method studies or analyzes primary legal materials and

[4]Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions.

secondary legal materials by understanding law as a set of regulations or positive norms in the Legislation system that regulates human life (Soekanto & Mamuji, 2004).[5]

Data were collected through two sources, namely: **Primary Data** : Obtained through semi-structured interviews with legal experts, legal practitioners, and law enforcement officers involved in cyber crime cases. **Secondary Data** : Includes legal documents, literature related to criminal law and cyber crime, and relevant court decisions. This data was collected from court archives, libraries, and trusted online sources.

3. RESULTS AND DISCUSSION

1. Concept and Types of Cybercrime Based on (Case Study of Decision No. 02/Pid.B/2022/PnPwk)

Cybercrime is a term that encompasses various forms of crime committed through information and communication technology, especially the internet. With the advancement of technology, these types of crimes are increasingly diverse and complex. Cybercrime not only harms individuals, but can also cause wider losses to society and the state. These crimes include a variety of illegal activities, such as identity theft, online fraud, and the distribution of illegal content.

One of the most well-known forms of cybercrime is online gambling. Online gambling has become increasingly popular as internet accessibility increases in Indonesia. These unregistered gambling platforms use technology to attract players with the promise of big profits, often at the expense of user safety and comfort. Online gambling is not only illegal, but can also damage the morals and society of society, especially among the younger generation.

In addition to online gambling, phishing is another form of cybercrime that often occurs. In phishing, the perpetrator tries to obtain sensitive information from the victim, such as passwords and credit card information, by deceiving them. Usually, the perpetrator uses an email or website that looks like an official site to trap the victim. This crime shows how important it is for the public to be aware of information security and how to protect themselves from such threats.

Hacking is also included in the category of serious cybercrime. Hackers can access other people's computer systems or networks without permission, often with the aim of stealing data or damaging the system. This crime not only harms individuals or companies, but can also

[5] Soekanto, S., & Mamuji, S. (2004). Normative Legal Research "A Brief Review". Jakarta: Raja Grafindo Persada.

cause major losses to a country's economy. Therefore, a deep understanding of the types of cybercrime is essential to formulating effective prevention and law enforcement policies.

With the development of technology, forms of cybercrime continue to evolve, creating new challenges for law enforcement. Therefore, it is important for the community and government to continue to monitor these developments and update existing regulations. A comprehensive understanding of the concept and types of cybercrime will help in formulating better strategies to combat this crime.

The Development of Cybercrime in the World

Cybercrime has its origins in hacking endeavors that have been present for over a hundred years. In the 1870s, youths caused disruptions to the technological infrastructure, notably altering the authority behind a newly established telephone system

In the early 1960s, there were university facilities such as the MIT artificial intelligence laboratory, using computers as their main tool, this was a trial stage for hackers. Hackers assume that someone who masters computers can create a program. By designing the program, it can carry out its tasks.

By adding the appropriate tones to the phone to instruct the phone system to open the line, John Draper made long-distance phone calls free in the early 1970s. The whistle was created by John Draper as a complimentary gift in a box of kid's cereal. "Captain Crunch" was Draper's nickname. Later, in the 1970s, he was arrested multiple times for vandalizing telephones. YIPL/TAP (Youth International Party Line/Technical Assistance Program) magazine was founded by the Yippie social movement to assist phone phreaks in making free long-distance calls.

In the beginning of the 1980s, a writer known as William Gibson introduced the concept of cyberspace, signifying an online realm. This term appeared in his science fiction book titled Neuromancer. During the inaugural effort to apprehend cybercriminals, the FBI conducted a raid on 414 headquarters located in Milwaukee, which refers to a specific site. This operation took place because hackers infiltrated a total of 60 computers, ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory.

The Comprehensive Crime Control Act is an organization tasked with carrying out comprehensive crime control measures, by providing Secret Service through credit card and computer fraud.

Computer fraud and misuse increased the authority of federal authorities in the late 1980s. The United States Defense Department established the Computer Emergency Response

Team at Carnegie Mellon University in Pittsburgh with the goal of looking into the increasing number of computer network threats.

At the age of 25, Kevin Mitnick was a veteran hacker who carried out his mission secretly by monitoring e-mail from MCI and digital equipment security employees. Mitnick damaged computers and stole software. Based on the case, Mitnick was sentenced to one year in prison.

In October 2008, a new virus called Conficker (also known as Downup, Downandup and Kido) emerged, categorized as a worm. Conficker attacks Windows and is most commonly found on Windows XP. Microsoft released a patch to stop the worm on October 15, 2008. Heinz Heise estimated that Conficker had infected 2.5 million PCs by January 15, 2009, while The Guardian estimated that 3.5 million PCs were infected. By January 16, 2009, the worm had infected nearly 9 million PCs, making it the fastest-spreading infection in a short period of time.[6]

The Development of Cybercrime in Indonesia

The development of technology in today's society is increasingly rapid, this can also increase the form of crime that must be addressed seriously, if this crime is not addressed seriously it will have an impact and influence on people's lives.

Cybercrime is a type of crime that is difficult to overcome because it is different from ordinary crimes in general. In Indonesia itself, various types of cybercrime have occurred, such as pornography, defacing sites, hacking, cyber gambling, and others.[7]

2. Legal Regulation Based on (Case Study of Decision No. 02/Pid.B/2022/PnPwk)

In Indonesia, regulations governing cybercrime are regulated in Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). This law is the legal basis for law enforcement against various forms of cybercrime. In the ITE Law, there are various provisions governing the prohibition of defamation, unauthorized access to electronic systems, and fraud committed through electronic media. However, even though the ITE Law has existed, there are still many challenges faced in its implementation.

[6]Editorial. Getting to Know the History of Cybercrime in the World, https://jurnalsecurity.com/mengenal-sejarah-cybercrime-didunia/ . Uploaded (November 17, 2016). Accessed August 14, 2021.

[7]Adami Chazawi, "Criminal Acts of Politeness", (Rajawali Press, Jakarta, 2005). p.,169

The existence of clear and comprehensive laws on online gambling can provide a strong legal basis for law enforcement. Unclear or inadequate regulations can make it difficult to punish perpetrators of online gambling crimes.

From a positive legal perspective, the criminal content of gambling is regulated in Article 303 of the Criminal Code, namely:

"Anyone who gambles is threatened with a criminal penalty of 10 years in prison, or a fine of Rp. 25 million, unless they have permission from the authorities."

The Electronic Information and Transactions Law's Article 27 paragraph (2) and Article 45 paragraph (1) then regulate online gambling, specifically: "Any person who intentionally and without the right distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing gambling content." This conduct is a criminal violation that carries a maximum penalty of IDR 1 billion in fines and/or 6 years in prison. Additionally, the restriction against issuing gambling permits is stated in Article 1 of Law No. 7 of 1974 concerning the Implementation of Gambling Control.

In the context of legal regulation, the effectiveness of law enforcement against online gambling crimes can depend on a number of the following factors:

1. Accuracy and Adequacy of Regulation. Good legal regulation should be carefully designed to cover various aspects of online gambling, including the definition of online gambling activities, the types of games that are permitted or prohibited, and licensing requirements. Clear and comprehensive regulation provides a strong legal basis for enforcement.
2. Compliance with Technology. As online gambling evolves along with technological developments, legal regulations must be able to adapt to these changes. The involvement of new technologies such as blockchain or artificial intelligence in online gambling requires regulations that can accommodate these dynamics.
3. Operator Licenses and Supervision. The licensing mechanism for online gambling operators must be strict and involve a careful process. In addition, supervision of licensed operators must be carried out regularly to ensure compliance with regulations and protect consumer interests.
4. Strict Sanctions and Punishments. Effective legal regulations must establish adequate and effective sanctions and penalties as a form of deterrence. The threat of serious punishment can reduce the motivation of perpetrators to engage in illegal gambling activities.

5. Inter-Agency Cooperation. The importance of cooperation between government agencies in implementing regulations cannot be ignored. Collaboration between law enforcement agencies, financial institutions, and regulatory authorities can improve enforcement efficiency and strengthen control over illegal gambling activities.
6. Responsiveness to Change. Regulations must be designed with the ability to respond quickly to new developments in the online gambling industry. Mechanisms for changing rules and adapting to new trends are essential to maintaining the relevance and effectiveness of regulations.

By taking these factors into account in developing legal regulations, enforcement of online gambling crimes can be more effective and responsive to changes in the digital environment. Good regulations will provide a solid foundation for law enforcement officers to carry out their duties efficiently and effectively.

In the context of regulation, cooperation between various parties is also very important. The government, internet service providers, and the community must work together to create an environment that is safe from cybercrime. Internet service providers, for example, have an important role in monitoring and removing illegal content and reporting suspicious activity to the authorities. Good cooperation between these parties can help in detecting and preventing cybercrime.

With clear regulations and consistent implementation, it is hoped that law enforcement against cybercrime can be more effective. In addition, the public also needs to be given a better understanding of existing laws so that they can protect themselves from potential cybercrime. With these steps, it is hoped that Indonesia can create a safer and more protected digital environment from cybercrime.

3. Forms of Unlawful Acts in (Case StudyDecision No. 02/Pid.B/2022/PnPwk)

Unlawful acts refer to actions taken by individuals or groups that are contrary to applicable legal rules. These actions not only harm others but can also damage social order and create injustice. In the context of criminal law, these acts can be violations regulated in the Criminal Code (KUHP) and other laws and regulations.

In Decision No. 02/Pid.B/2022/PnPwk, Defendant Tita Devita was charged with committing illegal gambling through the Gacor93 site. The existence of this site and the activities carried out by the Defendant indicate that these actions are not only against the law but also have the potential to cause widespread negative impacts, such as gambling addiction among the community.

Gambling crimes are one of the most common forms of unlawful acts faced by the justice system. In this case, gambling is defined as an activity in which an individual risks money or something of value in the hope of gaining a profit based on an uncertain outcome.

The crime of gambling is regulated in Article 303 of the Criminal Code which states that anyone who offers or provides an opportunity to gamble can be subject to criminal sanctions. In this case, the Defendant Tita Devita was involved in operating the online gambling site Gacor93, which did not have an official permit. This violation also involves Article 27 paragraph (2) of Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), which expressly prohibits the distribution of information related to gambling.

One very interesting aspect in the context of unlawful acts is the distribution of illegal content. In this case, the Defendant was not only involved in gambling itself, but also in actively promoting gambling sites through various social media platforms, including Instagram and Facebook.

Article 27 paragraph (2) of the ITE Law prohibits every individual from distributing information that contains gambling content. By promoting, the Defendant contributed to the spread of information that is detrimental to society and opened up opportunities for other individuals to engage in illegal activities. The spread of this content not only includes information about gambling sites, but also creates a social network that can reach more people, especially those who are vulnerable to the negative influence of gambling.

In this case, the involvement of many parties is a form of collusion that worsens the legal situation. The defendant Tita Devita did not commit this act alone; she collaborated with several other individuals, including witnesses who also acted as admins on the Gacor93 site. This collusion shows that this unlawful act was the result of organized cooperation.

In the verdict, there is an explanation that the Defendant acted as a coordinator, who recruited and organized admins to run the gambling site operations. The involvement of many parties in this crime shows that the act is not only an individual responsibility, but is a collective activity that can have greater legal consequences. This shows that supervision and law enforcement must be stricter to overcome the criminal network involved in online gambling.

The consequences of this unlawful act can be seen from the verdict that was handed down. The defendant was sentenced to 1 year and 6 months in prison, and a fine of Rp 125,043,750. This sanction reflects the seriousness of the actions taken by the defendant and the impact caused by illegal gambling.

In addition, evidence used in the crime, such as laptops and mobile phones, were confiscated for destruction. This shows that the justice system is trying to enforce the law firmly and prevent similar crimes from happening in the future. Strict law enforcement is needed to protect the public from the negative impacts of illegal gambling and create a safer environment.

4. Law Enforcement Based on (Case Study of Decision No. 02/Pid.B/2022/PnPwk)

The availability of resources, including manpower and technology, affects the ability of law enforcement to detect and prosecute online gambling perpetrators. Lack of resources can be a major obstacle to law enforcement efforts. For law enforcement to be more effective, support from all parties involved is needed.

The success of law enforcement in online gambling cases depends heavily on the existence of clear and comprehensive legal regulations. These regulations must be able to accurately determine the types of violations related to online gambling, provide adequate authority to law enforcement officers, and determine appropriate sanctions. Law enforcement must be supported by adequate technology and investigative expertise to identify and track illegal online gambling activities. A quick and appropriate response to information related to illegal activities is a key factor in law enforcement. Solid cooperation between law enforcement agencies, authorities, and other related parties is essential. Good coordination can facilitate the exchange of information, speed up investigations, and maximize the use of existing resources.

The effectiveness of law enforcement can be strengthened by the application of strict penalties, so that it can provide a deterrent effect for online gambling perpetrators. The threat of severe penalties can be a deterrent for people to engage in illegal activities. Training and capacity building of law enforcement officers to face the specific challenges related to online gambling is very important. The ability to understand technology, analyze data, and skills in digital investigations will strengthen the capacity of law enforcement. Law enforcement must also be able to quickly adapt to changes in technology and online gambling trends. Regulatory flexibility and the ability of law enforcement officers to respond to these changes will ensure the success of law enforcement in the long term.

Public awareness of the dangers of illegal online gambling can strengthen law enforcement efforts. Public education through outreach and information campaigns can help the public identify and report illegal activities, and encourage active participation in maintaining public safety. By considering all these factors, law enforcement against online gambling crimes will be more effective and responsive to evolving legal challenges.

Then, the law enforced in this case study is:

TO JUDGE:

1. The defendant, TITA DEVITA, SST. Par Binti Endang Rukanda, has been found legally and convincingly guilty of engaging in "Participating in Gambling using Information and Electronic Transactions (ITE)" as defined by Article 27 paragraph (2), Article 45 paragraph (1), and Article 55 paragraph (1) ke-1 of the Criminal Code, which carries criminal penalties;
2. The defendant was sentenced to 10 (ten) months in prison and a fine of Rp 125,043,750,- (one hundred twenty-five million forty-three thousand seven hundred and fifty rupiah), with the clause that, should the payment not be paid, 11 (eleven) days in prison would be substituted;
3. Ascertain that the entire amount of the defendant's punishment is subtracted from the time spent in arrest and custody;
4. Ascertain if the defendant is still being held;
5. Constructing proof
6. Demand that the defendant pay Rp 3,000.00 (three thousand rupiah) in court fees;

Obstacles in Law Enforcement against Cybercrime

1. The Absence of Specific Regulations on Online Gambling One of the main obstacles in handling online gambling cases is the absence of regulations that specifically regulate online gambling or cyber gambling. Existing regulations, such as the Criminal Code and the ITE Law, have not been fully able to overcome the characteristics of this crime, which is cross-border, complex, and uses sophisticated technology. Without specific regulations, law enforcement has difficulty effectively regulating and controlling the ever-growing online gambling activities.
2. Technology and Law Enforcement Capacity Limitations Law enforcement efforts against online gambling are greatly influenced by the limitations of existing technology. Although the Ministry of Communication and Information has blocked online gambling sites, this blocking is still ineffective because online gamblers can easily create new sites or move their servers to other countries. In addition, law enforcement agencies such as the police and prosecutors often experience technological limitations in tracking and identifying perpetrators who use sophisticated security systems and anonymous networks.

3. Difficulties in Proving and Investigating Online Gambling Cases Investigations into online gambling cases face obstacles in collecting evidence, especially in tracing the flow of funds and identifying perpetrators who often use cross-border electronic transactions. Identification of the main perpetrators and parties involved is a major challenge, especially since online gambling activities often involve foreign operators with strong encryption systems.
4. Lack of International Cooperation Online gambling crimes are often cross-border and involve foreign operators, so law enforcement in such cases requires strong international cooperation. Without cooperation with other countries, the process of prosecuting and executing laws against online gambling perpetrators outside Indonesia's jurisdiction becomes difficult and limited.

4. CONCLUSION

The rise of internet gambling due to technological advancements has become a significant obstacle for Indonesia's criminal justice system. The intricacy and dynamics of online gambling are still not adequately addressed by current legal laws, such as those included in the Criminal Code, the ITE Law, and the Ministry of Communication and Information's attempts to restrict gambling websites. Inequality and injustice provide significant obstacles to Indonesia's current legal rules pertaining to internet gambling offenses. The Criminal Code (KUHP), Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 19 of 2016 (a revision of the ITE Law), and Article 303 paragraph 1 of Law Number 9 of 1981 concerning gambling are among the regulations that govern these policies in this instance. However, the issue of gambling offenses in cyberspace has not been adequately addressed by current legal restrictions, raising questions about how effective their enforcement will be. Law enforcement is confused by the ambiguity in defining moral norm violations, which might be construed differently, as well as by differences in jurisdiction. Furthermore, the vagueness in the classification of crimes that do not expressly address online gambling and the absence of precise definitions of terms connected to cyber gambling in current legislation suggest that they need to be revised.

Thus, to effectively address the problem of cyber gambling in Indonesia, it is necessary to update and improve existing regulations in order to provide better legal certainty and justice for the community, as well as ensure that the law can function efficiently in addressing the increasingly growing online gambling activities. Therefore, special regulations, technological

capacity development, international cooperation, and ongoing socialization are needed to strengthen efforts to prevent and handle online gambling crimes in Indonesia.

5. BIBLIOGRAPHY

Abdulkadir Muhammad. (2004), *Law and Legal Research,* Bandung : Citra Aditya Bakti, p. 134

Adami Chazawi, 2005. *"Criminal Acts of Politeness",* Jakarta : Rajawali Press p.169

BJ Corbett . (2019). *Understanding Cybercrime: A Guide for Law Enforcement and Legal Professionals* . New York: Routledge.

Bruce Schneier . (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* . New York: Norton & Company.

David S. Wall **.** (2007). *Cybercrime: The Transformation of Crime in the Information Age* . Cambridge: Polity Press.

Didik M. Arief Mansur and Elisatris Gultom. (2009), *Cyber Law Legal Aspects of Information Technology*, Bandung: PT Radika Aditama, p. 8

Editorial. Getting to Know the History of Cybercrime in the World, https://jurnalsecurity.com/mengenal-sejarah-cybercrime-didunia/ . Uploaded (November 17, 2016). Accessed August 14, 2021.

Evelyn H. Wang & David MSK Lam **.** (2020). *Cybersecurity and Cybercrime in the Digital Age* . New York: Routledge.

Hamzah Andi. (1990), Criminal Aspects in the Computer Sector , Jakarta : Sinar Grafika, p. 26.

Kevin D. Mitnick . (2002). *The Art of Deception: Controlling the Human Element of Security* . Indianapolis: Wiley Publishing.

Law N o. 1 of 2023 concerning the Criminal Code (KUHP)

Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia 2008 Number 58

Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions.

MA Schaffer . (2018). *Cybercrime and Cybersecurity: The Role of Law in the Digital Economy* . New York: Palgrave Macmillan.

Mark A. Rothstein & Elizabeth S.H.D. Lee . (2017). *Cybercrime and Digital Forensics: An Introduction* . New York: Wiley.

Ministry of Communication and Information of the Republic of Indonesia. National Security Strategy *cyber (*2022-2024).

Muhammad Anthony Aldriano (2022). *" Cyber Crime from a Criminal Law Perspective".* Jakarta: Citizenship Journal, Vol. 6 No. 1 June, p.2

Muhammad Anthony Aldriano. (2022). " Cyber Crime in the perspective of criminal law ", Jakarta: Citizenship Journal (Vol. 6 No. 1) p.1

Rahmawati, H. (2021), *Cybersecurity: Challenges and Solutions in Indonesia . National Security Journal* .

Richard A. Clarke . (2019). *Cyber War: The Next Threat to National Security and What to Do About It* . New York: HarperCollins.

Samson Garfinkel & Abhi Shelat . (2003). *Understanding Digital Forensics* . Boston: Addison-Wesley.

Soekanto, S., & Mamuji, S. (2004), *Normative Legal Research,* "A Brief Review". Jakarta: Raja Grafindo Persada.

Thomas J. Holt, Adam M. Bossler, & Kathryn C. Seigfried-Spellar . (2015). *Cybercrime and Digital Forensics: An Introduction* . New York: Routledge.