Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

CYBER-SABOTAGE FROM THE PERSPECTIVE OF INFORMATION AND ELECTRONIC TRANSACTIONS REGULATION

Dirga Agung[1*], Andi Dewi Pratiwi[2]
[1]Universitas Atmajaya, Indonesia
[2]Univeritas Sulawesi Barat, Indonesia
*Correspondent Email: dirlen_alexander@yahoo.com

Abstract

Most cyber criminals on the internet will be ensnared by Law Number 11 of 2008 concerning Electronic Information and Transactions. The law should offer protection to internet users with good intentions, and provide strict action for cybercrime, especially cyber sabotage actors who disrupt electronic systems and even cause electronic systems to not work properly. Similarly, in Article 5, namely obtaining evidence, there are many obstacles, especially against perpetrators of crimes in Article 33 of Law Number 11 of 2008. Based on the results of the study, it can be concluded that in addition to creating good laws, it also builds the skills of law enforcers to especially find evidence of cybercrime (cybercrime) which is not easy because the crime is in cyberspace by sabotaging the electronic system. In addition, the perpetrators of crimes also hide their identity and the actions they take in cyberspace which is a form of protection.

Keywords: Cyber-sabotage; Electronics; Information; Regulation.

Abstrak

Sebagian besar pelaku kejahatan siber di internet akan terjerat oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang harus menawarkan perlindungan kepada pengguna internet dengan niat baik, dan memberikan tindakan tegas terhadap kejahatan dunia maya, terutama pelaku sabotase dunia maya yang mengganggu sistem elektronik bahkan menyebabkan sistem elektronik tidak berfungsi dengan baik. Demikian pula dalam Pasal 5 yaitu memperoleh barang bukti banyak kendala terutama terhadap pelaku tindak pidana dalam Pasal 33 Undang-Undang Nomor 11 Tahun 2008. Berdasarkan hasil penelitian dapat disimpulkan bahwa selain menciptakan hukum yang baik juga membangun ketrampilan penegak hukum khususnya menemukan bukti kejahatan dunia maya (cybercrime) yang tidak mudah karena kejahatannya ada di dunia maya dengan menyabotase sistem elektronik. Selain itu, para pelaku tindak pidana juga menyembunyikan identitas diri dan tindakan yang mereka lakukan di dunia maya yang merupakan bentuk perlindungan.

Kata Kunci: Sabotase siber; Elektronik; Informasi; Regulasi.

Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

INTRODUCTION

As technology and science develop, the condition of human civilization also develops in a positive direction. For example, internet technology, where this technology was initially only used in the fields of research and education, has now penetrated various fields, such as business. Business people use internet technology to make it easier to promote products, recruit employees and other programs from local to global levels.[1] This is intended to achieve the era of society 5.0. So it could be said that the existence of internet technology makes it easier for large and small scale business people to carry out economic activities. Not only that, internet technology also provides new opportunities for online businesses.[2]

The development of internet technology certainly has positive and negative impacts. The positive impact of the development of the internet is that it makes it easier to get the information you need just by entering keywords in the search engine section; make it easier for people to make transactions via e-commerce; shorten transaction time; make it easier to purchase products from abroad; supports communication activities without being limited by area or time; and supports electronic commerce.[3]

Meanwhile, the negative impact of internet technology is increasing crime in cyberspace in the form of cybercrime. Most of the perpetrators of this crime are late teenagers who have knowledge in the fields of informatics and telecommunications. The most common form of cybercrime is hacking illegal systems via the internet. The definition of cybercrime is an act of violating the law committed by an individual by utilizing internet or telecommunications technology related to internet applications. Another definition of cybercrime according to Barda Nawawi Arief is a series of activities carried out by individuals or groups of individuals in the form of cyber crimes in cyberspace. Another example of Cybercrime is Cyber Sabotage.[4]

Cyber Sabotage is one of the most vulnerable cybercrimes that occurs in cyberspace. This was stated by industry experts that cyber sabotage poses a serious threat to institutional electronic systems. This crime can attack anyone and of course causes huge losses to the victim.[5] An example of a case of cyber sabotage is the case that ensnared Bjorka in the form of hacking the Republic of Indonesia Government system. The hacking of this system indicates that the security system of the Republic of Indonesia Government institutions is relatively weak. If this condition is not followed up properly, there is a high possibility that the system will be hacked and damaged again. This case made researchers interested in studying further about cybercrime crimes by carrying out research entitled "Cyber Sabotage in the Perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions".

[1] Harwood, S., & Eaves, S. (2020). Conceptualising technology, its development and future: The six genres of technology. *Technological forecasting and social change*, *160*, 120174. https://doi.org/10.1016/j.techfore.2020.120174

[2] Andi Sofyan, Nur Azisa, *Hukum Pidana*, Pustaka Pena Mas, Makassar, 2016.

[3] Barda Nawawi Arief, 2010, Kapita Selekta Hukum Pidana, Citra Aditya Bakti, Bandung

[4] Andi Hamzah, *Hukum Pidana Indonesia,* Sinar Grafika, Jakarta, 2017.

[5] Michael L. Pittaro, *Cyberstalking: An Analysis of Online Harassment and Intimidation", International Journal of Cyber Criminology*, 1 (2), 2007, Hal. 180.

Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

METHOD

A technique implemented in research involving scientific theory and logical and systematic stages to make it easier to search, process, analyze and conclude research data in order to obtain answers to previously determined problem formulations is called a research method. Research methods can also be defined as the techniques and instruments implemented to obtain research data. The implementation of this research is of the library type, namely utilizing written sources in the entire series of research carried out.[6] Then the nature of this research is qualitative. Based on the opinion expressed by Sutrisno Hadi, library research has the same meaning as general research. Furthermore, the method implemented to collect data in library research is the documentation method by utilizing sources from articles, theses, books, journals, magazines, transcripts, notes, and the like.[7]

The approach used in this research is normative juridical based on the regulations "UU No.11 of 2008" regarding "Electronic Information and Transactions". The definition of normative is legal research whose aim is to obtain normative knowledge regarding the correlation between regulations, especially those related to "Cyber Sabotage in the Perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions". Researchers implemented data collection methods to obtain two types of data sources, where the data sources used included: 1) Secondary data defined as a type of data obtained through intermediaries from other parties or not obtained by researchers directly from research respondents. Secondary data is needed by researchers to support primary data. Researchers obtain secondary data from the internet, journals, books, articles, and the like related to cyber sabotage; and 2) Primary data defined as a type of data that researchers obtain from fundamental sources. In this research, primary data comes from statutory regulations no. 11 of 2008 regarding "Electronic Information and Transactions".

RESULT AND DISCUSSION

A crime using internet technology carried out by an individual or group of individuals against another individual as a target so that the target individual experiences losses while the perpetrator obtains a profit from his actions is called cybercrime. If defined briefly, cybercrime is behavior that is contrary to law based on internet technology. Technological developments in the field of communication do not all have positive impacts but there are also negative impacts. Even though technology used wisely can change human lifestyle or behavior in a positive direction. However, as technology develops, the number of crime cases increases. For example, crimes using electronic systems are called cybercrime. This crime takes the form of system hacking carried out by hackers.[8] Hackers will try to break into a company's system that claims its electronic system is complicated and difficult to penetrate to prove and inform the public that the company's system is very weak. Then, in terms of the type of crime, there are two types of internet technology crimes, namely:[9]

Cyber Sabotage defined as a series of activities to destroy, damage or disrupt network systems and computer programs connected to the internet. This form of crime takes the form of injecting a logic

[6] Teguh Prasetyo, *Hukum Pidana*, PT Raja Grafindo Persada, Jakarta, 2013.
[7] Irwansyah dan Ahsan Yunus, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*, Mirra Buana Media, Yogyakarta, 2020.
[8] Barbara A. Ritter, "*Deviant Behavior in Computer-Mediated Communication: Development and Validation of a Measure of Cybersexual Harassment*", Journal of Computer-Mediated Communication, 2014, 19 (2).
[9] Warren Chik, *Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking*, Journal of International Commercial Law and Technology, 3 (1), 2008.

bomb virus into a computer system which ultimately results in the original owner of the system being unable to control or being controlled and the system will be controlled by the perpetrator according to his motives. Cyber Sabotage is classified as the act of inserting a logic bomb virus into a computer network system so that the system cannot operate normally. This case often occurs and under certain conditions cyber saboteurs will offer themselves to help handle and repair abnormal computer network systems.[10]

Illegal access/unauthorized access to computer systems and services, this crime takes the form of infiltrating or hacking computer network systems illegally or without the permission of the owner of the network system in question.

1. Cyber Sabotage Case Motive

Hackers as perpetrators of Cyber Sabotage have strong principles and work processes by hiding their identity so that nicknames are often used when mentioning a hacker's name. Identity for a hacker is an absolute thing that must be hidden even from his closest friends. This is a particular strength for hackers as well as a form of self-protection from the activities they have carried out. This is a form of monitoring any risks that threaten him. There are five types of ways to carry out cyber sabotage, including:[11]

a. Bombard website data until the system runs abnormally.
b. Shutting down, delaying and stopping computer machines. One example of this is the shutdown of the Nuclear Power Plant system that occurred in Iran in 2011 by hackers.
c. Using information in the computer network system illegally.
d. Providing false information regarding an individual's identity to the authorities or the public as a form of concealing a criminal identity or destroying one's good name.
e. Disseminate hoax, negative or dangerous information through blogs, social media and websites.

2. Cyber Sabotage Case Motive

Hackers as perpetrators of Cyber Sabotage have strong principles and work processes by hiding their identity so that nicknames are often used when mentioning a hacker's name. Identity for a hacker is an absolute thing that must be hidden even from his closest friends. This is a particular strength for hackers as well as a form of self-protection from the activities they have carried out. This is a form of monitoring any risks that threaten him. There are five types of ways to carry out cyber sabotage, including:[12]

a. Bombard website data until the system runs abnormally.
b. Shutting down, delaying and stopping computer machines. One example of this is the shutdown of the Nuclear Power Plant system that occurred in Iran in 2011 by hackers.
c. Using information in the computer network system illegally.

[10] Tjaden, P., & Thoennes, N. *Full report of the prevalence, incidence, and consequences of violence against women: U.S. Department of Justice*, Office of Justice Programs, 2000.

[11] National Centre for *Cyberstalking* Research, *A Practical Guide to Coping with Cyberstalking*, Andrews UK Limited, 2015.

[12] Utin Indah Permata Sari, *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cybercrime yang dilakukan Oleh Virtual Police Di Indonesia*, Mimbar Jurnal Hukum, 2 (1), 2021.

d. Providing false information regarding an individual's identity to the authorities or the public as a form of concealing a criminal identity or destroying one's good name.
e. Disseminate hoax, negative or dangerous information through blogs, social media and websites.

3. Examples of Cyber Sabotage Cases

Based on information from Tribunnews.com, with the topic "This Teenage Hacker Successfully Hacked the Tiket.com Site on the Citilink Server, Losses Estimated at IDR 4.1 Billion" which was published on Thursday, March 30 2017, at 18.25 WIB, reporting on the actions of three teenagers Those who broke into the tiket.com site were arrested by the National Police Criminal Investigation Unit at Jakarta Police Headquarters. The hacking of the tiket.com site with the Citilink server was led by a 19 year old teenager named Haikal with the initials SH. The tiket.com site is classified as an online ticket buying and selling website. As a result of the actions of the three teenagers, Citilink and Tiket.com suffered losses of up to billions of rupiah, where Citilink lost IDR 2 billion while Tiket.com lost IDR 4.1 billion. When met by media crew on Thursday, March 30 2017, Brigadier General Pol Rikwanto as Karopenmas (Head of Public Information Bureau) Public Relations Division together with Head of Unit 1 Sub-Directorate III Directorate VI of Cyber Crime (Dittipidsiber) Bareskrim said, "This case was revealed after the ticket. com, PT Global Network, reported a breach of its online buying and selling site to Bareskrim Polri on November 11 2016."

The hacking process of the tiket.com site occurred from 11 – 27 October 2016 using the airline server PT Citilink Indonesia (www.citilink.co.id). Hackers took and sold airline ticket deposits on the Citilink Indonesia server. The hacker's actions resulted in tiket.com losing up to IDR 4,124,000,982.00 as well as the Citilink airline, where the hacker canceled and made a refund for the ticket purchase that had been made. The total loss received by Citilink airline reached IDR 1,973,784,434.00. Based on the results of the investigation, it seems that the hacker syndicate led by SH is selling the tickets they stole from tiket.com at a discount of 30 to 40 percent. They made a profit of around IDR 1 billion. From the results of the investigation, MKU played a role in offering airplane ticket sales using Hairul Joe's Facebook account. "He has a user name and password to enter the Citilink server which he obtained by hacking the Tiket.com site with suspect SH (19)," explained Rikwanto to the media crew.

One of the hackers with the initials AI was tasked with inputting data into the Citilink Indonesia server to order plane tickets via the tiket.com application on Citilink which had previously been successfully accessed by MKU. Then NTM acted as the party who bought plane tickets on Citilink Airlines using a Facebook account with the name Nokeyz Dhosite Kashir whose plane ticket booking code was sent by MKU. Then the purchase data will be sent back to AI to re-input the purchase data to the tiket.com site on the Citilink server. Based on the results of the investigation, the brain of this hacking scenario is SH or Haikal. However, during the arrest process, SH was not found at the scene. Rikwanto explained, "SH hacked at a place in Jakarta. "After the tiket.com site was successfully hacked, SH handed over the account and password for the online ticket booking site tiket.com to MKU." "You could say their boss is SH, who opens the sites and the three of them continue. If they are successful, the results are divided by two," added Rikwanto.[13]

[13] Siemieniecka & Skibinska, "*Stalking and Cyberstalking a Form of Violence*", Proceeding of The International Scientific Conference, 2019, Vol. 3.

Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

4. Cyber-sabotage According to the ITE Law

An indication that an individual has committed a criminal offense is that the behavior he or she commits is classified as an offense and is contrary to the law. The definition of "criminal act" is based on the Dutch language, namely "strafbaarfeit", where the vocabulary that forms it, namely "strafbaar" means "can be punished" and "feit" means "part of a reality". Meanwhile, according to legal experts, the definition of strafbaarfeit is:

a. In Simons' opinion, the definition of strafbaarfeit is behavior that violates the law carried out by an individual intentionally and can be punished in accordance with applicable laws and regulations.
b. In Hazewinkel Suringa's opinion, the definition of strafbaarfeit is an individual's actions that are contrary to norms in society and must be subject to criminal law in accordance with the violation.

Scope and material factors make it no secret that technological developments have made major changes to the scope of hacker operations, and vice versa. The ability and intelligence of hackers play a role in the development of information technology (mutualistic symbiosis). Because technological developments are always directly proportional to the habits and knowledge of hackers. In general, it can be concluded that technological development is always influenced by the scope and material of hackers, this is very clear because technology is a result of human thought, while hackers are actors in this case human resources (HR). These technological developments will then influence other aspects of life, including legal aspects. The relationship between technological developments and the needs of society has a unique cycle, which begins with increasing human skills and knowledge, then technology is created which successfully influences human life.[14] The easier it is to access needs, the higher the possibility of getting something, including material things (money), and this is where the law is required to play a role in creating boundaries for technology and humans.

This explanation forms the conclusion that technology comes from humans and is used to help humans.[15] Meanwhile, laws were created by humans to limit the use of technology and regulate abuse and violations that may occur in the cycle. That is the importance of law, in this case criminal law which resolves and even prevents perpetrators of crimes in cyberspace (cybercrime) which is balanced with developing and ordering the criminal law system both in the scope of economics, culture, structural development and the substance of criminal law. Criminal law policy occupies the top position which binds everyone to achieve the welfare and security of society.

One of the legal policies in Indonesia is the regulations regarding behavior in cyberspace which are explained in the regulation "UU no. 11 of 2008" regarding "ITE (Electronic Information and Transactions)". However, this regulation does not yet strictly bind crimes in cyberspace or cybercrime. So that every case regarding the evidentiary process and the legal force of crimes in cyberspace cannot resolve the cases that occur. Based on the regulations of Law no. 11 of 2008 article 33 relating to "Electronic Information and Transactions" regulates criminal acts for individuals who destroy or damage computer systems, where the contents of the article read: "Every person intentionally and

[14] Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, Myeshia Price-Feeney, "*Online Harassment, Digital Abuse, And Cyberstalking in America*", Center for Innovative Public Health Research.
[15] Achmad Ali, *Menguak Tabir Hukum*, edisi kedua, Citra Aditya Bakti, Bogor, 2008

Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

without right or against the law carries out any action which results in disruption of the Electronic system and/or causes the Electronic System to not work properly."

Then the sanctions imposed for the actions described in article 33 are explained in article 49, which reads: "Every person who meets the elements as intended in article 33, shall be punished with imprisonment for a maximum of 10 (ten) years and/or a fine of a maximum of IDR 10,000,000,000.00 (ten billion rupiah)." The definition of an electronic system is a collection of electronic devices that support the process of disseminating, sending, announcing, displaying, storing, analyzing, processing, collecting and preparing electronic information data. The electronic system can be used by anyone, including the public, business entities, government and state institutions.

In general, the formulation of a criminal act includes several things, namely: 1. The target of the norm is the subject of law; 2. Prohibited production that causes consequences; and 3. Criminal threats as a means of enforcing the implementation or compliance of these provisions. The formulation in Book I of the Criminal Code explains that criminal acts must have 3 main elements, namely legal subject, prohibited creation and criminal threat. If discussed briefly, prohibited acts have 2 different forms, namely concrete acts, namely criminal acts that occur in the field and abstract, namely planned acts. Legal processing will apply if the legal subject of the prohibited act and the threat of punishment are clear. These three elements are very clearly related, if there is no legal subject, then the criminal act is just a threat. Likewise, vice versa, if the subject of the law and the action are clear but the threat of punishment is not yet clear, then the legal process will become dull and powerless.

In the criminal formulation, legal issues related to Cyber Sabotage are included in the category of prohibited acts because these activities are included in criminal acts which are definitely subject to legal threats as explained in Book I of the Criminal Code. In short, criminal acts depend on the formulations contained in Article 1 of the Criminal Code, while the punishment system depends on the rules that are applied for a certain action at a certain time. Good law without being accompanied by good and competent law enforcers clearly still creates obstacles. As with the lack of firmness in implementing the regulations of Law no. 11 of 2008 regarding "Electronic Information and Transactions" regarding cybercrime cases.

In article 5, a statement is summarized, namely "regarding the expansion of new evidence in accordance with procedural law in force in Indonesia, accepting electronic information and electronic data or printouts as valid evidence". This statement proves that the legal regulations related to cybercrime were not previously included in the Criminal Procedure Code (KUHP). The rise in acts of cyber sabotage is due to the limited skills and competence of law enforcers in eradicating crackers in cyberspace even though laws regarding cyber sabotage have been established. The lack of competent law enforcement means that perpetrators of cyber sabotage can escape criminal law. In general, there are two obstacles that hinder the enforcement of cyber sabotage laws, namely:

a. Inadequate legal instruments based on the legal policies stated in the Criminal Code, legal instruments (investigators) such as the National Police provide the analogy that cybercrime acts must have their own legal regulations.

b. Level of investigator competency, another obstacle to law enforcement in dealing with cyber sabotage is the low competence of investigators such as the National Police in investigating cases of crimes in cyberspace committed by hackers, moreover, most of the National Police are not

Alauddin Law Development Journal (ALDEV)
Vol. 6, No. 1, 2024

skilled in operating computers: When carrying out an investigation there are several components that the National Police must find or law enforcement when investigating cases, including:"Every person intentionally and without right or against the law carries out any action which results in disruption of the Electronic system and/or causes the Electronic System to not work properly."

Then the sanctions imposed for the actions described in article 33 are explained in article 49, which reads: "Every person who meets the elements as intended in article 33, shall be punished with imprisonment for a maximum of 10 (ten) years and/or a fine of a maximum of IDR 10,000,000,000.00 (ten billion rupiah)." The definition of an electronic system is a collection of electronic devices that support the process of disseminating, sending, announcing, displaying, storing, analyzing, processing, collecting and preparing electronic information data. The electronic system can be used by anyone, including the public, business entities, government and state institutions.

In general, the formulation of a criminal act includes several things, namely: 1. The target of the norm is the subject of law; 2. Prohibited production that causes consequences; and 3. Criminal threats as a means of enforcing the implementation or compliance of these provisions. The formulation in Book I of the Criminal Code explains that criminal acts must have 3 main elements, namely legal subject, prohibited creation and criminal threat. If discussed briefly, prohibited acts have 2 different forms, namely concrete acts, namely criminal acts that occur in the field and abstract, namely planned acts. Legal processing will apply if the legal subject of the prohibited act and the threat of punishment are clear. These three elements are very clearly related, if there is no legal subject, then the criminal act is just a threat. Likewise, vice versa, if the subject of the law and the action are clear but the threat of punishment is not yet clear, then the legal process will become dull and powerless.

In the criminal formulation, legal issues related to Cyber Sabotage are included in the category of prohibited acts because these activities are included in criminal acts which are definitely subject to legal threats as explained in Book I of the Criminal Code. In short, criminal acts depend on the formulations contained in Article 1 of the Criminal Code, while the punishment system depends on the rules that are applied for a certain action at a certain time. Good law without being accompanied by good and competent law enforcers clearly still creates obstacles. As with the lack of firmness in implementing the regulations of Law no. 11 of 2008 regarding "Electronic Information and Transactions" regarding cybercrime cases.

The limited tools and capabilities of the police mean that the National Police cannot function properly to eradicate this crime. What should be done is that the National Police can speed up the detection and prediction of the whereabouts of crackers when they are acting in cybercrime laboratories. Apart from that, there are also other things, namely victims who are reluctant to report crimes that have happened to them due to reasons of privacy, economics, or victims who do not trust the expertise and dedication of the police in uncovering the case. Law enforcement action against perpetrators of cybercrime is to protect cyberspace users from crackers who use internet media to commit their crimes. Even though Indonesia does not yet have "cyberlaw" that specifically targets the interests of victims, Indonesia still needs legal action using previously existing laws such as: legislation, jurisprudence and international conventions that have been ratified to protect the interests of cyberspace residents in Indonesia.

Various efforts can be taken to resolve Internet crimes, both preemptively, preventively and repressively. Preemptive efforts can be carried out by ratifying international cybercrime agreements

into the legal system in Indonesia. Preventive handling of cybercrime can be carried out by developing security, increasing energy for computer features, ability and discipline in using these features in cyberspace. These activities can take the form of actions that can be carried out individually, at national or global policies. Meanwhile, repressive cybercrime countermeasures can be implemented by ensnaring the perpetrators of criminal acts to be dealt with in accordance with the law. The law determines the interests of victims by providing restitution, compensation or assistance which is the responsibility of the perpetrator and the state as the provider. The method that law enforcement must implement in handling cybercrime cases is to prioritize a restorative justice system, namely a system that pays attention to the relationship between families, victims and perpetrators of criminal acts in providing solutions or resolving cases..

CONCLUSION

Life will not be free from problems, whether they come from individuals, groups, organizations, even the business world. Apart from wasting energy and thought, it can even cause losses. However, as actors in life, especially as humans, we must be able to approach every problem with broad and open thinking so that the problems we face can be resolved well. It is the same as a crime in the current era of globalization that occurs in cyberspace (cybercrime). For this reason, we must be aware of this as early as possible in order to avoid this crime. With the existence of extensive information facilities, of course we hope that we as individuals and institutions who need it, can make the best use of it in life, at least to avoid before something undesirable happens. Law enforcers should improve their skills, especially in finding evidence of cybercrime, which is not easy because cybercrime perpetrators hide their identities, the actions they take and so on.

REFERENCES

Andi Hamzah, *Hukum Pidana Indonesia*, Sinar Grafika, Jakarta, 2017.

Achmad Ali, *Menguak Tabir Hukum*, edisi kedua, Citra Aditya Bakti, Bogor, 2008

Andi Sofyan, Nur Azisa, *Hukum Pidana*, Pustaka Pena Mas, Makassar, 2016.

Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, Myeshia Price-Feeney, "*Online Harassment, Digital Abuse, And Cyberstalking in America*", Center for Innovative Public Health Research.

Barbara A. Ritter, "*Deviant Behavior in Computer-Mediated Communication: Development and Validation of a Measure of Cybersexual Harassment*", Journal of Computer-Mediated Communication, 2014, 19 (2).

Barda Nawawi Arief, 2010, Kapita Selekta Hukum Pidana, Citra Aditya Bakti, Bandung

Harwood, S., & Eaves, S. (2020). Conceptualising technology, its development and future: The six genres of technology. *Technological forecasting and social change*, *160*, 120174. https://doi.org/10.1016/j.techfore.2020.120174

Irwansyah dan Ahsan Yunus, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*, Mirra Buana Media, Yogyakarta, 2020.

Michael L. Pittaro, *Cyberstalking: An Analysis of Online Harassment and Intimidation", International Journal of Cyber Criminology*, 1 (2), 2007, Hal. 180.

Soerjono Soekanto, *Kriminologi: Suatu Pengantar*, Cetakan Pertama, Ghalia Indonesia, Jakarta, 1981.

Tjaden, P., & Thoennes, N. *Full report of the prevalence, incidence, and consequences of violence against women: U.S. Department of Justice*, Office of Justice Programs, 2000.

Utin Indah Permata Sari, *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cybercrime yang dilakukan Oleh Virtual Police Di Indonesia*, Mimbar Jurnal Hukum, 2 (1), 2021.

U. S. Department of Justice. (2005). *Prosecutors in State Courts*, 2005. 12

National Centre for *Cyberstalking* Research, *A Practical Guide to Coping with Cyberstalking*, Andrews UK Limited, 2015.

Siemieniecka & Skibinska, "*Stalking and Cyberstalking a Form of Violence*", Proceeding of The International Scientific Conference, 2019, Vol. 3.

Teguh Prasetyo, *Hukum Pidana*, PT Raja Grafindo Persada, Jakarta, 2013.

Warren Chik, *Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking*, Journal of International Commercial Law and Technology, 3 (1), 2008.