JURNAL HUKUM Khaira Ummah

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

Master of Law, UNISSULA

Application of Elements of Illegal Access Criminal Act Via Social Media by Investigators at the Directorate of Special Criminal Investigation of the West Sumatera Regional Police

Muhammad Subran Ardatul Putra[1)] **& Andri Winjaya Laksana**[2)]
[1)]Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia, E-mail: M.Subranardatul07@Gmail.com
[2)]Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia, E-mail: AndriWinjayaLaksana@unissula.ac.id

Abstract. *The more advanced the development in the field of technology, the more crimes that emerge, one of which is in the cyber world. Information Security and Electronic Transactions (ITE) is currently always overshadowed by the high level of ITE crimes, causing many people to become victims of cyber crimes. This study aims to determine the application of elements of the crime of illegal access through social media by investigators at the Ditreskrimsus Polda Sumbar. In this study, the approach method used is: a normative legal approach or an approach through literature study. The research specification used is Descriptive Analytical, which is an effort to analyze and explain legal problems related to objects with a comprehensive and systematic description of everything related to the application of elements of illegal criminal acts of access through social media by investigators at the Ditreskrimsus Polda Sumbar. The application of the elements of the crime of illegal access via social media by investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Police is by applying the elements contained inArticle 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Transaction Information.Obstacles in the Application of Illegal Criminal Act Elements of Access Through Social Media by Investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Police especially in terms of collecting evidence to fulfill the elements of the crime*

Keywords: *Criminal; Electronic; Transactions.*

1. Introduction

The development of computer technology and internet networks has created a new world called cyberspace, which is a network/container for someone where they can communicate with each other based on the internet network on their computer. However, the development of this information technology can also be a double-edged sword, because in addition to having a positive impact, namely making it easier for humans to carry out their activities, on the other hand it also has a large negative impact and seems to provide a gap for criminals to carry out their actions. One of them is the crime of Illegal Access or illegal access.

Access is the activity of interacting with an electronic system that stands alone or in a network. Article 1 paragraph (15) of Law Number 19 of 2016 concerning Amendments to Law

Number 11 of 2008 concerning Electronic Information and Transactions, states that Access is a number, letter, symbol, other character or a combination of them, which is the key to accessing a Computer and/or other Electronic System. In the general explanation of the ITE Law, it is stated that what is meant by "making accessible" is all actions other than distributing and transmitting through an electronic system that cause electronic information and/or electronic documents to be known to other parties or the public. Meanwhile, Illegal in the broad sense according to the Big Indonesian Dictionary (KBBI) is invalid, without rights, without permission, not according to the Law. The idea of being without rights and not according to the law takes a clear form in the thinking pioneered by LJ van Apeldoorn. Without rights, there is a terminology called "wederrechtelijk" in criminal law which means contrary to the law in strijd met het rech or violating the rights of others met krenking van eens anders recht and not based on law niet steunend op het recht.[1]

Regulations regarding the crime of Illegal Access are regulated in Article 35 of Law Number 11 of 2008 concerning Information and Electronic Transactions, which states:

Any person who intentionally and without authority or against the law manipulates, creates, changes, removes, or destroys Electronic Information and/or Electronic Documents with the aim of making the Electronic Information and/or Electronic Documents appear to be authentic data.

The mode of crime in Illegal Access is not uncommon in society, various methods are used such as manual methods to sophisticated technology. Done using elements of coercion and violence to being done with elements of caution. Various incidents that occur, in general the mode used by criminals. Illegal Access by utilizing sophisticated technology is by stealing or breaking into data with elements of fraud or asking for data for example from credit card holders when getting it to make fake transactions. This type of crime is known as carding. There are several modes that are usually carried out in credit card crimes including Phishing, Carding, Hacking, Skimming and Extrapolation of these modes that are most common in society.[2]

Currently, a new legal regime has been born, known as cyber law or telematics law. Cyber law or cyber law, is internationally used for legal terms related to the use of information and communication technology. Likewise, telematics law is the embodiment of the convergence of telecommunications law, media law, and informatics law. Other terms that are also used are information technology law (law of information technology) and virtual world law.[3]

According to data from the West Sumatra Regional Police, cybercrime until mid-2020 reached 126 cases. These cases include defamation, hate speech, spam, misuse of information technology networks, and carding. One of the crimes is Illegal Access which is highly dependent on lifestyle patterns or technological advances that are developing in society which is more popularly known as cyber crime. The crime of Illegal Access is a crime of intentionally and unlawfully accessing computers and electronic systems belonging to other

[1]Jan Remmelink, Criminal Law Commentary on the Most Important Articles of the Dutch Criminal Code and Their Equivalents in the Indonesian Criminal Code, Gramedia Pustaka Utama, Jakarta 2003, p. 5.
[2]Asril Sitompul, Internet Law: Introduction to Legal Issues in Cyberspace, First Edition, Citra Aditya Bhakti, Bandung, 2001, p. 19.
[3]Ika Riswanti Putranti, Copyleft Licenses and Open Source Software Protection, First Edition, Gallery Ilmu, Yogyakarta, 2010, p. 21.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

people in any way that results in losses for others. The case can be understood that this activity is illegal access. Such as the investigation carried out by investigators at the West Sumatra Regional Police's Directorate of Criminal Investigation where there was a fake or bogus Facebook account claiming to be an official at an agency in West Sumatra. Through this account, the perpetrator asked for money from the treasurer at the agency and close friends of the official. The treasurer at the agency and close friends of the official believed it because the profile on the account was the same as the official's original account. The posts and language used were also the same as the original. As a result, the victims suffered losses of around Rp. 60,000,000 (sixty million Rupiah).

Starting from the conditions that occurred above, for that reason, in an effort to find out and analyze the investigation of the crime of Illegal Access, the researcher is interested in conducting research which will be written in the form of a thesis with the title "Application of Elements of the Crime of Illegal Access Through Social Media by Investigators at the Directorate of Criminal Investigation of the West Sumatra Regional Police"

2. Research methods

This study uses normative legal research, namely using norms in laws with a conceptual approach and a special approach. The method used in this study is normative juridical. This study goes through the stages of literature study, the data obtained is then analyzed through a qualitative analysis approach. Qualitative data processing and analysis generally emphasizes its analysis on the process of deductive and inductive conclusions and the dynamics of the relationship between observed phenomena using scientific logic.

3. Results and Discussion

3.1 Implementation of the Elements of the Criminal Act of Illegal Access Through Social Media by Investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Police

Illegal access is increasingly popular from year to year, a shortcut for fraudsters to get money from fraud because they don't have to bother to work, where they only rely on social media as a medium to deceive their targets. With the capital of sweet words to gain the trust of their targets. This illegal access can be in the form of fake accounts that use other people's names to facilitate their actions. These fraudsters will not be deterred, and will commit fraud again after successfully deceiving their targets.

Illegal access is a very despicable act and can harm many people. However, often illegal access actions that occur in society are not reported to the police. So that makes the owners of these fake accounts continue to commit fraud continuously. The creation of fake accounts in the name of other people can cause defamation for others because they have spread false information that is detrimental to other parties.

Considering that due to the virtual nature of cyberspace, illegal content such as Information and/or Electronic Documents that contain content that violates morality, gambling, insults or defamation, blackmail and/or threats, the spread of false and misleading news resulting in consumer losses in Electronic Transactions, as well as acts of spreading hatred or hostility based on ethnicity, religion, race, and class, and sending threats of violence or intimidation that are aimed personally can be accessed, distributed, transmitted, copied, stored for re-dissemination from anywhere and at any time, then in order to protect the public interest

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

from all types of disturbances resulting from the misuse of Electronic Information and Electronic Transactions, an affirmation of the role of the Government is needed.

The role of the government is intended to prevent the spread of illegal content by taking action to terminate access to Electronic Information and/or Electronic Documents that have unlawful content so that they cannot be accessed from the jurisdiction of Indonesia and the authority is needed for investigators to request information contained in the Electronic System Organizer for the benefit of enforcing criminal law in the field of Information Technology and Electronic Transactions. Illegal content that is spread through electronic media and is commonly found in the community includes false information, blasphemy and defamation.

Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is the first law in the field of Information Technology and Electronic Transactions as a much-needed legislative product and has become a pioneer that lays the foundation for regulations in the field of utilization of Information Technology and Electronic Transactions. However, in reality, the implementation of the ITE Law has experienced various problems.

Based on the Constitutional Court Decision Number SO/PUU-VII2OOS and Number 2/PUUVII 2OO9, the criminal act of insult and defamation in the field of Electronic Information and Electronic Transactions is not merely a general crime, but also a complaint offense. The affirmation of the complaint offense is intended to be in line with the principle of legal certainty and the sense of justice of the community.

Illegal access is set onArticle 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Transaction Information and its criminal threats are contained in Articles 51 and 45 of the law. The elements applied by investigators are the first subjective elementthat is "Any person who intentionally and without rights or against the law" this is fulfilled by the existence of evidence, namelyThe witness's statement stated that he had sent a certain amount of money because of...whatsapp with someone claiming to be Kombespol Joko Sadono, SH, SIK, MHand other evidence is expert testimony and electronic evidence in the form of account screenshotsFacebook on behalf of Joko Sadono with URL Link https://www.facebook.com/joko.sadono.165. All evidence indicates the suspicion that the crime was committed by an individual legal subject.

Every Person, according to the definition of Article 1 point 21 of the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions, what is meant by a Person is an individual, whether an Indonesian citizen, a foreign citizen,or legal entity. The person in question is the perpetrator sending Electronic Information and/or Electronic Documents containing content as referred to in Articles of the Republic of Indonesia Law Number 11/2008 concerning Electronic Information and Transactions.

Intentionally, the element referred to as "intentionally" is the existence of evidence of a will to realize an element in a crime according to the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions, namely an active perpetrator or someone who is proven to have carried out an action that can be interpreted as a legal act, including technical actions in the use oftechnology, but without considering the motive and reason – as formulated by Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions and the perpetrator has known or realized or

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

intended the consequences of the act. Evidence of intent can be shown, among other things, by the actions of the perpetrator recorded in the electronic system, from the activity records of his account or which is currently under his control or which is currently being used and/or which is carried out repeatedly so that it is known by the Witness.

Next is the element Without Rights, while what is meant by "without rights" is an act that is not based on a right or authority based on the Law or permission and other legitimate legal basis; including if the actThis is done beyond the rights or authority granted by law or other legitimate permits and legal bases; or violates the rights of others or is against the law. Subjectively, this element has been proven to have been carried out by the suspect whoexplained that the suspect created 2 (two) Facebook accounts in the name of Kombespol Joko Sadono, SH, SIK, MH, including:

1. Joko Sadono is a suspect for using a black Samsung J3 brand cellphone, which is the suspect's Facebook for using the cellphone number082275120505 with password Joko78;

2. Joko Sadono II, the suspect, used a black Samsung J3 brand cellphone, which the suspect created or registered using the cellphone number on Facebook.085264696765 with password Joko73.

The objective elements applied are "manipulating, creating, changing, removing, destroying Electronic Information and/or Electronic Documents" this elementaccording to the evidence of the witness's statement who was friends on the Facebook account and received the messagewhatsapp as if it were true from the person concerned. Other evidence is a letter or electronic document in the form ofElectronic letter/documentScreenshot printout of WhatsApp conversation with someone claiming to be Kombespol Joko Sadono, SH, SIK, MH.

Manipulation, which is the process of engineering through the addition or reduction or removal or obscuring or hiding part or all of a reality, reality, facts or history and/or material (objects) carried out using a design system tool or a value system, without the recipient of the information and/or electronic document being aware of it; so that something will appear to have a meaning, substance/content, that is different from the original (not authentic) or directed at another meaning desired by the sender.

The act of manipulation is carried out with the aim of making the Electronic Information and/or Electronic Documents appear to be authentic data.Based on the agreement between witness statements, experts, and electronic documents, it is known that there is a fake Facebook and WhatsApp in the name of Kombespol Joko Sadono, SH, SIK, MH, which is strongly suspected of being manipulated by Ganda Hirahman Wahyu by creating the fake Facebook and WhatsApp in the name of Kombespol Joko Sadono, SH, SIK, MH.

Furthermore, the element "with the aim that the Electronic Information and/or Electronic Documents are considered as if they were authentic data" is in accordance with the evidence of witness statements who suspect that the electronic information is authentic and expert statements.

Article 35 of the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions is regulated alternatively, meaning that it is sufficient to prove that the perpetrator intentionally committed one or more of the acts in question. Through these acts, illegitimate rights arise for himself or others. Where the use of the rights in

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

question is without legal basisor authority so that it becomes invalid or violates the rights of others. In this case the act carried out was data manipulation.

The suspect's actions are also linked to the provisionsArticle 45 paragraph (4)Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008on Electronic Information and Transactions "Any person who intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain extortion and/or threats". Where the elements are fulfilled "Any person intentionally and without rights or against the law" Based on the statements of witnesses, experts and electronic documents, it was found that there was a match that the suspect on behalf of Ganda Hirahman Wahyu Pgl Ganda used a Facebook and WhatsApp account in the name of Joko Sadono, where with the Facebook and WhatsApp the suspect asked for help from Yon Friadi to send money amounting to Rp. 20,000,000,- (twenty million rupiah) and this was confirmed by the suspect's statement.

The next element is "distributing and/or transmitting and/or making accessible Electronic Information and/or Electronic Documents that contain blackmail and/or threats"The suspect named Ganda Hirahman Wahyu Pgl GANDA explained that the suspect's motivation in creating Facebook and WhatsApp in the name of Kombespol Joko Sadono, SH, SIK, MH was only to scare Syamsul Ridwan because the suspect's intention to scare Syamsul Ridwan was successful, so the suspect continued and tried to find other victims to give some money.

Another issue that often causes debate in society is related to the elements of distribution or dissemination of electronic information. According to the explanation of Article 27 paragraph (1) as contained in Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning ITE, what is meant by "distributing" is sending and/or disseminating Electronic Information and/or Electronic Documents to many people or various parties through the Electronic System. Meanwhile, what is meant by "transmitting" is sending Electronic Information and/or Electronic Documents addressed to one other party through the Electronic System. Furthermore, regarding the word "making accessible" is all other actions other than distributing and transmitting through the Electronic System that cause Electronic Information and/or Electronic Documents to be known to other parties or the public. The word "making accessible" is the most potential to cause debate because in practice, electronic information on social media can sometimes be spread and can be accessed by other parties even without the intention to spread it. For example on Facebook, sometimes just by clicking like, information can be spread and can be accessed by other parties. In this case, if there is an allegation that a criminal act has occurred, then usually the party who first spread it is designated as the suspect, although in fact if we pay attention to the explanation of Article 27 paragraph (1) of Law No. 19 of 2016, then all parties who make the information known to other parties should be able to be made suspects of the criminal act. Provisions like this are prone to being used as rules to ensnare other parties selectively according to the interests of certain parties.

In relation to the process of examining digital evidence both during investigation and examination in court, there needs to be adequate capability from law enforcement. In handling electronic data, special steps are needed so that the digital evidence does not change. Therefore, investigators must understand the initial handling of electronic evidence on computers at the scene of the crime, physical sector-by-sector duplication (forensic

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

imaging), file system analysis of Microsoft Windows programs, searching and displaying files even though they have been deleted and formatted, or data that has never been saved and only printed (file recovery), mobile phone analysis (mobile forensics), audio recording analysis (audio forensics), video recording analysis (video forensics), and digital image analysis (image forensics).

Cybercrime cases are special cases whose investigation methods can be different from investigations in general cases. In carrying out its duties and roles, the function of the investigators, especially the cybercrime unit, is based on several laws related to cybercrime crimes that occur. One of them is as a guideline for evidence, namely the provisions in Article 184 of the Criminal Procedure Code, where the evidence referred to is witness testimony, expert testimony, letters, instructions, and defendant's testimony. In addition, investigators can use cybercrime investigators using evidence, namely Electronic Information and/or Electronic Documents and/or printouts. However, electronic information and/or electronic documents are declared valid if they use an electronic system in accordance with the provisions stipulated in the ITE Law.

Furthermore, according to the provisions of Article 6 of Law No. 11 of 2008, it is also regulated that in the event that there are other provisions that require that information must be in written or original form, electronic information and/or electronic documents, then it will be considered valid as long as the information contained therein can be accessed, displayed, guaranteed its integrity, and can be accounted for so that it explains a situation. In the provisions of Article 44 of the ITE Law, it is regulated that, evidence for investigation, prosecution and examination in court according to the provisions of this law are as follows: a. other evidence in the form of Electronic Information and/or Electronic Documents as referred to in Article 1 number 1 and number 4 and Article 5 paragraph (1), paragraph (2), and paragraph (3). Based on these provisions, the evidence in cybercrime is as follows:

a) Electronic Information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are able to understand them. This is in accordance with the provisions of Article 1 number 1 of Law No. 11 of 2008.

b) Electronic Documents are any electronic information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, which can be viewed, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs or the like, letters, signs, numbers, Access Codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand them. This is based on the provisions of Article 1 number 4 of Law No. 11 of 2008.

Electronic Information and/or Electronic Documents and/or printouts are valid legal evidence. Electronic Information and/or Electronic Documents or printouts are an extension of valid evidence in accordance with the applicable Procedural Law in Indonesia. However, printouts of electronic documents do not apply to: a). letters that according to the Law must be made in written form; and b). letters and documents that according to the Law must be in the form of a notary deed or a deed made by a deed-making official. In the event that there are other

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

provisions that require that information must be in written or original form, Electronic Information and/or Electronic Documents are considered valid as long as the information contained therein can be accessed, displayed, its integrity is guaranteed, and can be accounted for so that it explains a situation.

Regarding the subject of the perpetrator of the crime, criminal responsibility in the ITE Law can be imposed on individuals and corporations. This can be seen from the subject of the crime contained in its criminal provisions, namely every person. The definition of a person in the General Provisions of Article 1 paragraph (21) is an individual, whether an Indonesian citizen, a foreign citizen, or a legal entity. Even explicitly, corporate responsibility in criminal acts in the ITE Law is stated firmly in Article 52 paragraph (4).

In the ITE Law, corporations are also subjects of criminal acts. Therefore, a clear and detailed corporate accountability system should also be regulated, especially regarding when a corporation is said to have committed a crime, who is responsible and the criminal sanctions that can be imposed. However, this law does not regulate these three main things. Regarding criminal sanctions, for example, it only mentions the principal penalty plus two-thirds. Other types of sanctions that are more appropriate for corporations are not regulated, such as temporary or permanent closure.

Criminal provisions in the ITE Law adopt an alternative-cumulative formulation system. This can be seen from the use of the formulation "...and/or...", except in Article 52 which is of a nature that contains aggravating criminal penalties. Meanwhile, for the types of criminal sanctions (strafsoort), there are 2 (two) types, namely imprisonment and fines. Both types of sanctions are threatened for all types of crimes, whether committed by individuals or corporations. In fact, corporations certainly cannot be subject to imprisonment. The determination of corporations as subjects of criminal acts should only be threatened with fines and additional/administrative/disciplinary actions. The formulation system for the amount/duration of criminal penalties (strafmaat) in the ITE Law is a special maximum system, namely a special maximum for imprisonment ranging from 6 years to 12 years and a special maximum for fines ranging from IDR 600,000,000 to IDR 12,000,000,000.

From the law that is the legal umbrella, it has been correct and implemented by law enforcers, only law enforcers are required to educate and socialize more about this illegal access to the public so that the public can distinguish between real accounts and fake accounts that can deceive the public. From the data above, we know that there are many perpetrators of illegal access cases, but it is quite difficult and takes a long time to prove the perpetrators of this illegal access because there are several syndicates and may be spread throughout Indonesia due to the vastness of cyberspace that is the target of the perpetrators.

3.2 Obstacles in the Application of Illegal Criminal Act Elements of Access Through Social Media by Investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Police

In cybercrime cases, investigations are faced with complex problems, especially in terms of evidence. Many witnesses and suspects are outside the jurisdiction of Indonesian law, so that conducting examinations and taking action is very difficult, not to mention the constraints of very complex evidence related to information technology and digital codes that require good Human Resources and forensic computer equipment.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

Cybercrime case prosecution often encounters obstacles, especially in the arrest of suspects and confiscation of evidence. In the arrest of suspects, we often cannot determine for sure who the perpetrator is because they do it simply through a computer that can be done anywhere without anyone knowing so that there are no witnesses who know directly. The results of the tracking can only find the IP Address of the perpetrator and the computer used. The confiscation of evidence often encounters problems because usually the reporter is very slow in reporting, this causes the attack data in the server log to be deleted, usually occurs in deface cases, so investigators have difficulty in finding the statistical logs contained in the server because usually the server automatically deletes the existing logs to reduce the server load. This makes investigators unable to find the data needed to be used as evidence while the statistical log data is one of the vital pieces of evidence.

The examination of witnesses and victims often encounters obstacles, this is because at the time the crime took place or was committed there was not a single witness who saw it (testimonium de auditu). They only found out after the incident occurred because they received the impact of the attack that was launched. The role of expert witnesses is very large in providing information in cybercrime cases, because what happens in cyberspace requires specific skills and expertise. Expert witnesses in cybercrime cases can involve more than one expert witness according to the problems faced, for example in deface cases, in addition to expert witnesses who master graphic design, expert witnesses are also needed who understand network problems and expert witnesses who master programs.

After the investigation is complete and poured into the form of a case file, the problem that exists is the problem of evidence because there is no common perception among law enforcement officers, digital evidence is evidence in cybercrime cases that do not have a clear formulation in determining it because digital evidence is not always in real physical form. For example, in a murder case, a knife is the main evidence in committing murder, while in a cybercrime case, the main evidence is a computer, but the computer is only the physical form, while the main thing is the data on the computer's hard disk in the form of a file, which if made real by printing requires a lot of paper to pour it, can the evidence be in the form of a compact disc only, until now there has been no law that regulates the form of digital evidence if presented as evidence in court.

Other obstacles faced by law enforcement in using digital evidence through forensic computers are weaknesses in digital forensic devices, where the West Sumatra Regional Police forensic computer laboratory is not yet available. Examination of digital evidence is carried out by experts as in the case above. The forensic laboratory used is located in the jurisdiction of the West Sumatra Regional Police. The digital forensic laboratory is not yet owned by the Indonesian National Police in every region. In fact, its existence is very important in preventing and handling cases related to Cyber Crime.

Another obstacle is cybercrime which often involves countries (transnational) and knows no borders (borderless), and is outside the jurisdiction of Indonesian law, in this case investigators or Interpol have difficulty in taking action and examining perpetrators/operators who are very clever in carrying out each of their crime modes. Also related to the lack of human resources in terms of knowledge about digital technology, digital codes at the level of the Police, Prosecutors, Judges, so that in handling cybercrime there are obstacles in evidence. Furthermore, the weak regulations of the Law governing cybercrime, and this factor can be

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

exploited by perpetrators of cybercrime to find loopholes in the law to escape the law.

Efforts made in proving using digital evidence with forensic computers include cooperation between POLRI investigators and investigators from other countries to share information and evidence, where with these evidences, they can be used as evidence to create a judge's belief in the truth of a crime that has been committed by the defendant. Furthermore, by using information or opinions from telematics experts who have expertise in their fields, with the information obtained, it can be a consideration for the judge in deciding a case based on the available evidence.

Collecting and securing digital evidence for further analysis so that it can be accounted for in court. By taking a technological approach to law enforcement officers and the community, so that in handling cybercrime cases they are not technologically illiterate and can resolve them with a technological approach.

4. Conclusion

The application of the elements of the crime of illegal access via social media by investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Police is by applying the elements contained inArticle 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Transaction Information. The elements applied by investigators are the first subjective element, namely"Every person intentionally and without rights or against the law" acts carried out by an individual. ElementWhich is Intentionally Fulfilled with Evidence of intention, among others, can be shown by the actions of the Perpetrator recorded in the electronic system, from the activity records of his account or which is currently under his control or which is currently being used and/or which is carried out repeatedly. The objective element applied is "manipulating, creating, changing, removing, destroying Electronic Information and/or Electronic Documents" this element is in accordance with the evidence of the witness's statement who is a friend on the Facebook account and receives the messagewhatsapp as if it were true from the person concerned. Other evidence is a letter or electronic document in the form ofElectronic letter/documentScreenshot printout of WhatsApp conversation with someone claiming to be Kombespol Joko Sadono, SH, SIK, MH. Obstacles in the Application of Illegal Criminal Act Elements of Access Through Social Media by Investigators at the Directorate of Special Criminal Investigation of the West Sumatra Regional Policeespecially in terms of collecting evidence to fulfill the elements of the crime. These obstacles include:isThe examination of witnesses and victims has many obstacles, this is because at the time the crime took place or was committed there was not a single witness who saw it (testimonium de auditu). They only found out after the incident took place because they received the impact of the attack that was launched. The confiscation of evidence has many problems because usually the reporter is very slow in reporting, this causes the attack data in the server log to be deleted, usually occurs in deface cases, so investigators have difficulty finding the statistical logs contained in the server because usually the server automatically deletes the existing logs to reduce the server load. Obstacles to the problem of evidence due to the lack of the same perception among law enforcement officers, digital evidence is evidence in cybercrime cases that does not yet have a clear formulation in determining it because digital evidence is not always in real physical form. The weakness in digital forensic devices, where the West Sumatra Police forensic computer laboratory is not yet available.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 19 No. 3 September 2024

5. References

Asril Sitompul, Internet Law: Introduction to Legal Issues in Cyberspace, First Edition, Citra Aditya Bhakti, Bandung, 2001.

Ika Riswanti Putranti, Copyleft Licenses and Open Source Software Protection, First Edition, Gallery Ilmu, Yogyakarta, 2010.

Jan Remmelink, Criminal Law Commentary on the Most Important Articles of the Dutch Criminal Code and Their Equivalents in the Indonesian Criminal Code, Gramedia Pustaka Utama, Jakarta 2003.