JURNALLIGAHUKUM
Volume 1: Number 2: January 2021 / P-ISSN 2085-577X
Published by Faculty Of Law
Universitas Pembangunan Nasional Veteran Jawa Timur

Legal Protection For Victims Of Crime Of Hacking

Adhek Inarania Salsabila[1], Sri Maharani MTVM[2]
[1]*Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia, Email: Inaran19@gmail.com*
[2]*Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia.*

Abstract

Cybercrime has become a threat to stability, so the government has difficulty to handle the crime that have been carried out with computer technology, especially the internet and internet networks. The Government issued Law Number 11 of 2008 concerning Information and Electronic Transactions which was later updated with Act Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Technology, which is expected to be able to anticipate developments and problems, including the impact negative abuse of the Internet with various motivations that can cause victims such as material and non-material losses. The research method that I use is empirical juridical, namely research that examines the applicable legal provisions and what happens in reality in the community. The data source is taken from the results of field observations at the DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police, applicable laws, legal journals, and Indonesian dictionaries and legal dictionaries. This study uses descriptive analytical research methods, the analysis data method is a qualitative approach to primary data and secondary data. Descriptive includes the content and structure of positive law, which is an activity carried out by the author to determine the content or meaning of the rule of law which is used as a reference in solving legal issues that are the object of study.

Keywords : legal protection, hacking

I. Introduction

Technology from time to time is always experiencing development. Along with the development of existing technology, resulting in the world more easily accessible. Nothing is impossible to do with the help of today's technology. The technological advancements in question can help humans to carry out daily activities. The presence of modern technology such as the internet has changed humanity's view of life. The human communication paradigm in managing economic, business, social interaction, and political activities is different. Entering the technological era 4.0 human life depends a lot on technology. For example, economic actors conduct businesses ranging from promotional activities to payment transactions utilizing technology both by transfer, EDC machines, to M-Banking.

The internet, if likened to a double-edged sword, because in addition to bringing positive benefits, but the negative impact also arises with the human shrewdness to use technology as a medium to commit crime. Negative impacts can occur when an error occurs caused by a computer device that will result in large losses for users or interested

*Coresponding Author

parties. These intentional errors lead to misuse of computers, so that it has the potential to use computer media and the internet to commit various criminal acts

Various crimes that use computer technology and the internet as a medium, have recently shown significant figures, both in terms of quantity and in terms of quality. The use of computer media and the internet as a medium for committing crimes is generally known as cybercrime.

Various kinds of crimes are started from a mild scale to the heaviest. As stated by Dimitri Mahayana, director of the Telecommunications Sharing Vision research institute conducting research in 2013, said Indonesia could get 42,000 cyber attacks per day. This tends to undermine the security of companies and the state, and hinder the development of individuals (the community at large) given the mobility of internet use which tends to increase from day to day.

Various types of cybercrime cases recorded in the East Java Regional Police include: hate speech, hacking, online fraud, spreading false news, spreading viruses, and others. According to the Head of Sub Directorate Siber DITRESKRIMSUS East Java Regional Police, the situation and condition of the community affected the number of cases received. For example at the time of the democratic party season, the number of cybercrime cases received was the most cases of hate speech and spreading false news. But there are also criminal acts which are not influenced by the situation of the community. Like hacking. Crime hacking always happens all the time.

The crime of hacking from time to time always develops along with the development of increasingly sophisticated technology. Because of hackers, other computer or electronic companies will always improve their security systems. But hackers will always try to find loopholes in the security system and break in.

The actions of the hackers are not always based on malicious intentions or called mens rea. But sometimes there are also hackers who try to hack because of curiosity and challenged to try to find a loophole of a security system. But whether based on mens rea or just curious, these actions still cannot be justified before the law.

Therefore the government issued Law Number 11 Year 2008 Regarding Information and Electronic Transactions which was later updated with Act Number 19 Year 2016 concerning Amendments to Law Number 11 Year 2008 Regarding Electronic Information

and Technology, which is expected to be able to anticipate developments and problems , including the negative impact of misuse of the Internet with various motivations that can cause victims such as material and non-material losses. Law Number 11 Year 2008 which is then updated with Law Number 19 Year 2016 Regarding Information and Electronic Transactions can be used as a Judge in imposing prison sentences on all perpetrators of cybercrime in Indonesia.

The hackers in launching their actions sometimes have targeted victims first. Like the case of hacking to Sony Pictures which caused losses due to the leaking of their valuable files. But many hacking victims are also chosen at random. As is the case at this time, which is hacking someone's social media account which is then used for fraud. After the social media account is hacked, the hacker will claim to be the original owner of the account and borrow money from the friend of the original owner of the account. The original owner of the account often does not feel that he has been a victim of hacking. They only realize that they have become victims of hacking after reports from friends who are victims of fraud.

II. Method

The type of research used by the author is Juridical-Empirical, the research method that the author uses is empirical juridical, namely research that examines the applicable legal provisions and what happens in reality in the community. The data source is taken from the results of field observations at the DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police, applicable laws, legal journals, and large Indonesian dictionaries and legal dictionaries. This study uses descriptive analytical research methods, data analysis used is a qualitative approach to primary data and secondary data. Descriptive includes the content and structure of positive law, which is an activity carried out by the author to determine the content or meaning of the rule of law which is used as a reference in solving legal issues that are the object of study

III. Main Heading of the Analysis or Result

Various crimes that use computer technology and theinternet as a medium, have recently shown significant figures, both in terms of quantity and in terms of quality. In 2017, Sub Directorate of Siber DITRESKRIMSUS East Java Regional Police received 3 public

complaints about hacking against social media. The most targeted social media hacking is blackberry massanger.

Public complaints in 2018 increased to 4 cases. Unlike in 2017, the most targeted social media is Facebook. As many as 2 facebook accounts were hacked and then used to commit fraud against the friends list contained in the facebook account. While 2 other cases were carried out on Tokopedia and Instagram accounts.

In 2019, Sub SIT V Siber received the most complaints from the public regarding the crime of testing when compared to the previous 2 years. In 2019, hacking is the most targeted e-commerce account. A total of 4 criminal acts of hacking were carried out on Tokopedia, OLX, Bukalapak, and Lazada accounts. Whereas 2 other cases were carried out on Instagram accounts.

Factors of hacking are certainly different from those of other criminal acts. Because criminal acts generally occur in the real world and can be seen in plain sight, felt, or heard. While the crime of hacking (hacking) occurs in cyberspace using a technology or computer system. so that the crime of hacking (hacking) can not be seen or heard directly but can be felt in real terms as a result of these actions.

These factors are divided into 2 (two). Namely internally and externally. The following will describe the factors that also influence the occurrence of criminal acts of hacking.

Internal factor is a factor in the occurrence of a hacking crime (hacking) that comes from within a perpetrator of a hacking crime (hacking). Internal factors of hacking (hacking) include:

1. Hacking is done by perpetrators based on revenge motives. Relationships between family, friends, and relationships are factors that cause a person to become a victim of hacking because the victim has previous problems with his social environment, which can trigger anger of the perpetrators hacking.
2. Hacking is carried out on the basis of personal interests both material and non material. A hacker is able to make a program for his own benefit and is destructive or destructive and make it a profit.

3. Hacking is carried out because the motive is fun and aims to explore and penetrate an operating system and computer security code. This action does not result in damage to a system, because it is only based on curiosity about a system.

While external factors are factors of criminal hacking (hacking) that come from outside a hacker. External factors for hacking can be described as follows:

1. Lack of knowledge of law enforcement in the Republic of Indonesia in overcoming hacking problems. In general law enforcement officers still lack knowledge in the mastery of computer operations and an understanding of computer hacking and the ability to conduct investigations into cyber crime cases. This allows hackers or so-called hackers to be far more powerful than law enforcement officials which results in increasing intensity of hacking crimes in Indonesia.
2. Network security systems that have not been able to prevent hacking. The lack of an internet security system allows anyone to try to hack into someone's social media account.
3. The absence of a special body formed by the government that can provide assistance against the occurrence of criminal acts of hacking (hacking).

Based on the factors of the occurrence of hacking crimes (hacking) that the authors get from library studies, the authors then conduct research directly in the DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police in order to know firsthand the factors of the crime of hacking (hacking) associated with the theory of the factors causing the occurrence of acts of hacking criminal hacking (hacking) that the author has described above.

The most factor that causes the crime of hacking (hacking) is the perpetrators of committing crimes (hacking) for profit. In 2017, DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police received 3 illegal access complaints and all of the 3 complaints were due to the same factors. Namely for profit. In 2017, the most targeted social media hackers were Blackberry Messenger or BBM.

Whereas in 2018, the most targeted social media hackers are facebook. DITRESKRIMSUS SUBDIT V SIBER received 4 illegal access complaints. Namely 2

illegal access to Facebook accounts, 1 to Instagram, and 1 to Tokopedia e-commerce account.

In 2019, hacking cases were mostly carried out against e-commerce accounts as targets. DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police received 6 illegal access complaints. Among Tokopedia, OLX, Bukalapak, Lazada, and 2 others Instagram. Although it is still done together to get profits, hacking of e-commerce accounts is different from social media. If social media is misused for fraud, hacking of an e-commerce account is carried out to drain the remittance balance that is in the account and is used for shopping by the offender. The second most common factor causing hacking is hacking because it is based on revenge or hurt. In the last 3 years, DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police received complaints of hacking cases caused by factors of revenge or hurt as much as 2 complaints.

Internal factors causing hacking (hacking) further are perpetrators of hacking (hacking) only to carry out exploration and penetration of an operating system and other computer security code. Based on the data that the writer got from DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police and interviews with Brigadier Arif W S.H as a member of V Cyber Subdit, hacking due to the desire of exploration by very few perpetrators. Even in the last 5 years, DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police have not received complaints of hacking caused by these factors. The first external factor is the lack of law enforcement in the Republic of Indonesia in overcoming the problem of hacking. According to Brigadier Arif, the theory is not a factor in the crime of hacking in East Java, because every member of the DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police has been equipped with informatics. If a problem is found in the investigation or investigation process, members of the Sub-V Siber will always coordinate with informatics experts. The second external factor is the weakness of the security system that cannot prevent hacking. This theory is also not justified by Brigadier Arif. Because every social media / website / e-commerce has additional security facilities. According to Brigadier Arif, the reason for the hacking is not because of a weak security system so that it cannot prevent hacking, but the low security awareness of the internet user community is a factor in the occurrence of hacking. Many of the people of Indonesia still underestimate and believe that he will not be a victim of hacking. In the International Telecommunication Union (ITU) report in 2017, Indonesia ranked 70th in the category

of cyber security awareness. The third external factor that causes hacking is the absence of a special body formed by the government that can provide assistance against hacking. This theory also cannot be fully justified, because in 2017, President Jokowi has formed a National Siber and Coding Agency (BSSN) whose duty is to oversee and secure the cyber territory of the country and become a coordinating vehicle for all agencies related to cyber security.

Analysis of the causes of hacking in East Java can be related to the teaching of multiple factor theory, that the perpetrators of these crimes are caused by a number of complex factors as stated by Sutherland and Cressey..[1] Different from other criminal acts, hacking can be caused by several factors. Various factors of the occurrence of criminal acts of hacking (hacking) that the authors have described above have links with each other.

In legal protection for victims of cybercrime, there are basically two models, namely the procedural rights model and the service model:

1. The Procedural Rights Model In the procedural rights model, victims of cybercrime crimes are given the right to make criminal charges or assist prosecutors, or the right to be present at all levels of justice where information is needed, implicitly in this model victims are given the opportunity to "Revenge" the perpetrators of crimes that have harmed him.
2. The Service Model
3. This service model focuses on the need to create standard standards for the coaching of victims of cybercrime crime. This model sees the victim as a figure that must be served by the police and other law enforcement agencies, service to victims of cybercrime by law enforcement officials if done well will have a positive impact on law enforcement, especially cybercrime.

In taking action for those who misuse technological development, quality human resources who have the ability and expertise in technology are needed. In law enforcement, at least some factors are influenced by the rule of law itself or the law, the

[1] Widodo, 2007, *Analisis Kriminologis Tentang Penyebab Pelaku Kejahatan Yang Berhubungan Dengan Komputer (Studi Di Unit V Infotek/ , Direktorat Ii Markas Besar Kepolisian Negara Republik Indonesia)*, Hukum dan Dinamika Masyarakat Vol.4 No.2, hlm. 124

implementing apparatus of the rule, namely the law enforcement apparatus and the legal culture itself, namely the community itself which is the target of the law.

The importance of legal protection for victims of cyber crime in order to realize a rule of law. The National Police provides a special e-mail to receive reports of cases related to cybercrime. It aims to facilitate victims in making complaints. But for complaints of hacking cases, the victim must come directly at the police station. For illegal access cases, victims can make complaints both at the Regional Police and the local police station. Then the case will be examined further. If the District Police feels that the case is too difficult, the victim will be directed to make a complaint to the Regional Police.

Repressive legal protection for victims of hacking criminal offenses when related to article 5 paragraph (1) of the Protection Of Witness And Victim Law, the victim does not get all the protections listed in the article. Protection that will be given to victims of hacking include:

1. Protection in the form of giving information without pressure
2. Free from the tricky questions
3. Get information about the development of the case
4. Obtain information regarding court decisions
5. Getting information in case the convict is acquitted
6. Confidential identity.

In providing repressive protection, DITRESKRIMSUS SUBDIT V SIBER East Java Regional Police emphasizes protecting the privacy of victims. Many victims expect the recovery of a hacked account to be returned to them. But unfortunately this is not included in the rights of victims of criminal acts of hacking. Recovery of a hacked account whether returned to the victim or not depends on the judge's decision. However, it is very unlikely that the account that was hacked was returned to the victim, because the account was used as evidence in the trial. Even though the trial has been decided by the Panel of Judges, the majority of the accounts that have been hacked cannot be returned to the victims.

IV. Conclusion

1. That the crime of hacking is caused by many factors both internally and externally. But complaints of hacking (hacking) in the DITRESKRIMSUS SUBDIT V SIBER, East Java are mostly caused by internal factors. Namely, the perpetrators of the crime of hacking (hacking) hacking because of the motive to seek material gain.
2. If hacking has occurred, the victim will receive repressive protection, including privacy, freedom to file complaints, and receive information on the progress of the investigation / investigation. The return of a recovered account is not included in the legal protection by Siberian Subdit V, because the restored account will be evidence in the trial and after the trial.

Suggestion

1. It is better for BSSN to conduct more in-depth socialization to the public so that they understand that their every action in cyberspace is supervised by BSSN. In addition, it would be nice for the Directorate General of Sub-V Siber to form a special team of information technology scholars to investigate cybercrime, because even though members of the Siberian V Subdit have been equipped with technology, however, it is still different from information technology scholars who study information technology more deeply .
2. So far, Siberian Sub Directorate V has been focusing on young people. Preferably, the socialization of the crime of hacking focuses more on the target of the elderly, because they were born before there was advanced technology like now, so they are difficult to understand technology. So they assume enough to use social media without regard to security. They are also more easily fooled by the links that spread because they do not know the mode of the perpetrators of the crime of hacking.
3. For victims of a crime of hacking, if they expect that their social media is restored it is better to ask for help from ID-CERT than to make a complaint to the Sub-V Siber. However, it would be nice if in the future ID-CERT and Subdit V Siber would cooperate in cracking down on hacking.

Acknowledgments

1. Mr. Dr. H. Sutrisno, S.H., M.Hum., As Dean of the East Java "Veteran" UPN Faculty of Law.
2. Mrs. Mas Anienda Tien F, S.H., M.H as Deputy Dean I of the Law Faculty of UPN "Veteran" of East Java.

3. Mrs. Dra. Ec. Nurjanti Takarini, as Deputy Dean II of the Faculty of Law at UPN "Veteran" of East Java.
4. Mr. Fauzul Aliwarman, S.HI., M.Hum Deputy Dean III and at the same time Lecturer Guardian at the Faculty of Law, UPN "Veteran" East Java.
5. Mr. Eko Wahyudi, S.H., M.H., as the Coordinator of the Study Program at the Faculty of Law, UPN "Veteran" East Java.
6. Mrs. Sri Maharani MTVM., S.H., M.H., As a Supervising Lecturer both during the course and during this thesis research.
7. Lecturer in the Faculty of Law of the Surabaya "Veteran" National Development University who has helped a lot during this education.
8. Thesis examination team that has provided evaluations, criticisms and suggestions that are important for future writers.
9. Mr. and Mrs. Administrative Section of the Faculty of Law of the National Development University "Veteran" of East Java which has provided convenience in administrative administration.
10. Parents Writers who have supported and prayed for fluency in writing this research.

References

https://www.course-net.com/kenapa-indonesia-miliki-tingkat-kesadaran-cyber-security-rendah-setingkat-kamboja-ini-jawabannya/ diakses pada 19 Oktober 2019 20:06 WIB

Marina Raisa Theodora Napitupulu, Skripsi : "*Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking) Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik(Putusan Nomor 253/Pid.B/2013/Pn.Jr)*", Medan : Universitas Sumatra Utara, 2018

Muladi dan Barda Nawawi Arif, 1992, *Bunga Rampai Hukum Pidana*, Alumni, Bandung.

Wawancara dengan Briptu Arif W. S.H, Tanggal 21 Oktober 2019 di Kantor DITRESKRIMSUS SUBDIT V SIBER Polda Jatim

Widodo, 2007, *Analisis Kriminologis Tentang Penyebab Pelaku Kejahatan Yang Berhubungan Dengan Komputer (Studi Di Unit V Infotek/ , Direktorat Ii Markas Besar Kepolisian Negara Republik Indonesia)*, Hukum dan Dinamika Masyarakat Vol.4 No.2