Legal Protection Against the Rise of Cyber Crime Cases in Indonesia

Firstnandiar Glica Aini Suniaprily, Prista Prasiwi, Adhy Nugraha
Faculty of Law, Universitas Islam Batik Surakarta
Email: firstnandiar@gmail.com

ABSTRACT

The rise of cyber crime cases in Indonesia is a significant challenge in the context of legal protection for the community in the face of the times. Rampant cyber crime cases, such as the case of hacking a company server in San Antonio, Texas, United States by a hacker with the initials BBA, highlight the lack of competence of law enforcement officials in stemming cyber crime. The normative research approach used looks at the applicable legal regulations, namely Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) which has been revised into Law No. 19 of 2016. The relevant articles, such as Article 49 Jo Article 33 and Article 45 paragraph (4) Jo Article 27 paragraph (4), explain the criminal provisions for hacking crimes. The results show that perpetrators of cyber crime can be sentenced to imprisonment and fines. However, obstacles in law enforcement include the limited ability of investigators, inadequate evidence and infrastructure, and broad jurisdiction. Therefore, efforts to eradicate cybercrime in Indonesia need to be carried out with preventive measures such as public education and blocking, as well as repressive through criminal sanctions in accordance with applicable laws. The conclusion of this research shows that law enforcement against cyber crime must be more effective by referring to the ITE Law and increasing the competence of law enforcement officials in order to stem the rise of cyber crime cases in Indonesia.

Keywords: Cyber Crime, Legal Protection, ITE Law

A. INTRODUCTION

Enforcement of cyber crime in Indonesia still does not reflect effective law enforcement even though Indonesia has Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. The law has not been able to accommodate cyber crimes that are increasingly prevalent in Indonesia, which include credit card fraud, banking fraud, defacing, cracking, sex transactions, pornography, online gambling, spreading false news via the internet and terrorism. This happens because cyber crime is not limited by the territory of a country, thus showing the alignment in the field of information, media, and informatics develops without being blocked.

One of the growing and prevalent crimes is credit number theft. According to Rommy Alkatiry, the misuse of other people's credit cards on the internet is the biggest cyber crime case related to the internet business world in Indonesia. The misuse of other people's credit cards is not too complicated and can be done physically or online. The name and credit card of another person obtained at various places (restaurants, hotels, or any place that makes credit card payment transactions) are entered in the application for purchasing goods on the Internet. This then opens up opportunities for hackers to enter, modify, or damage the homepage (hacking) so that cases of hacking or hacking are increasingly common.[1]

In his action, he sent an email link http://ddiam.com/shipping200037315.pdf.exe to one of the employees at the company. The link directs users to another link containing cryptolocker. BBA is also known to have committed other criminal acts in the form of carding with the mode

[1] Suhariyanto, B. (2014). Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan Dan Celah Hukumnya. Jakarta:Rajawali Pers, h.18.

of spending other people's credit cards and trading other people's credit card data. For his actions, BBA is subject to Article 49 Jo Article 33 and Article 48 paragraph (1) Jo Article 32 paragraph (1) and Article 45 paragraph (4) Jo Article 27 paragraph (4) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE. The perpetrator was arrested by the Directorate of Cyber Crime of the Criminal Investigation Agency of the Indonesian National Police at his residence in Sleman, Yogyakarta on Friday, October 18, 2019.

Efforts to handle cyber crime in the hacker classification require the seriousness of all parties considering that information technology has been used as a means of cultured communication. The existence of laws regulating cyber crime, especially in the classification of hackers, is necessary, but if the implementation does not have the ability and expertise in this field and the community continues to be targeted, the purpose of the formation of the law will not be achieved. According to the provisions of Article 30 and Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, every person intentionally and without rights or unlawfully accessing a computer and or electronic system belonging to another person by any means to obtain electronic information and or electronic documents is subject to criminal sanctions of imprisonment of between 6 (six) to 8 (eight) years and or a fine of around Rp 1,000,000,000,- (one billion rupiah) to Rp 2,000,000,000,- (two billion rupiah).

Although the legislators have formulated criminal provisions as in the provisions of the above regulations, in reality law enforcement on hacker cybercrime is still lacking. One of the reasons is that not all victims have the desire to report even though they have suffered material losses. In addition, the lack of competence of law enforcement officials in combating cyber crime hackers also has an influence on law enforcement. This is then the background of the author to further examine the law enforcement against cyber crime hackers. based on this background, How is law enforcement against cyber crime hackers?

B. RESEARCH METHOD

This research is a normative legal research by focusing on the collection of legal materials through literature studies, including primary legal materials, secondary legal materials and tertiary legal materials. In addition, the author also conducted interviews with Mr. Khairumam as the Judge of Bantul Court and Mr. Kurniawan as the Cyber Crime Unit of Bantul Police. The material collected will be analyzed using qualitative analysis techniques, namely by providing exposure, describing in detail and thoroughly about the data obtained from the research process so as to explain the enforcement of criminal law against cyber crime hackers.

C. RESULTS AND DISCUSSION

The development of science and technology today is not only able to provide a positive impact, but the development is apparently misused as a means of crime. It is very important to anticipate how the legal policy, so that cyber crime that occurs can be overcome by criminal law, including in this case is about the enforcement system. Indonesia itself already has a legal regulation of cyber crime contained in Law Number 19 of 2016 concerning Electronic Information and Transactions, which is an amendment to Law Number 11 of 2008.

Law enforcement is one of the components in law enforcement. Law enforcers are those who directly or indirectly contribute to a law enforcement process. Basically, law enforcers will combine values, rules, and behavior. Law enforcers generally often take action and maintenance in achieving the goals of justice. The attitude of law enforcers in carrying out their duties, it is not uncommon to exercise discretion which is a decision-making in overcoming

the problems faced but in making decisions law enforcers must stick to the rules, although it does not rule out the possibility of discretion without adhering to the rules, because the regulations on the issue do not yet exist.[2]

In Indonesia, law enforcement officials who have the authority to handle hacker cyber crime cases are divided into 3, namely;

1. Court

Parties who file a case in court certainly have the intention of obtaining a settlement and resolution of the case fairly and in accordance with the expectations and desires of the parties seeking justice (justiciabellen). To get a fair settlement of the case and in accordance with the expectations and desires of the parties seeking justice must go through an evidentiary process. The process aims to know the sitting of the case clearly, namely true events and false events. In the evidentiary process the parties are given the opportunity to express their opinions about the events that occurred. This is very important because it is the basis for affirming rights and denying the rights of the other party. In terms of expressing opinions, it is not enough for the parties to just give their opinions orally or in writing, but they must be supported and accompanied by valid evidence according to the law so that the truth can be ascertained.

2. Prosecutor's Office

The Public Prosecutor's Office has the main task as one of the law enforcement agencies in the Indonesian criminal justice system. The task is to carry out prosecution and vice versa. Prosecution is the only authority that is only owned by the prosecutor's office and is not owned by other law enforcement agencies. In carrying out its functions, duties and authority, the prosecutor's office is independent from all influences of government power, and the influence of other powers. The state guarantees prosecutors in carrying out their profession without intimidation, interference, temptation, and inappropriate interference or disclosure of anything that has not been tested, whether against civil, criminal, or other liability.

3. Police

The police are one of the law enforcement officers. The duties of the police apparatus are to maintain security and public order, enforce the law, provide protection, protection and services to the community. All rules regarding the police function itself are regulated in Law No. 2 of 2002 concerning the Indonesian National Police. The regulation explains that one of the functions of the police is to carry out the functions of state government that provide protection, realize or maintain order, provide services and protection to the community, and enforce the law. This is clearly stated in Article 14 paragraph (1) of the Police Act.

In criminal cases in general, the police will immediately act to investigate even though there is no report or complaint first. However, this certainly requires various considerations first. The investigation action is the duty of the police as stated in Article 14 paragraph (1) letter g which states that the police are authorized to investigate criminal acts in accordance with the criminal procedure law which was previously preceded by investigative actions by investigators.

From the results of the police investigation, the hacking was carried out by BBA with the mode of attacking malicious programs (computer viruses) of the Ramsomeware type. BBA purchased Ramsomeware or malware capable of taking control containing Cryptolocker on the internet black market or dark ware. The Ramsomeware was sent widely to more than 500 overseas email addresses. If one of the victims received and opened the email, the company's software would be encrypted. This is an opportunity for BBA to ask for ransom money to victims. Because, if not given a ransom within a certain time, the company's system will be paralyzed. BBA was arrested on October 18, 2019 by the Cyber Crime Directorate of the

[2] Soekanto, S. (1990). Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum). Bandung:Mandar Maju. h. 6.

National Police at his residence in Sleman. BBA was tried in Bantul District Court with case number 41/Pid.Sus/2020/PN Btl (ITE). BBA was proven legally and convincingly guilty of committing a cyber crime that resulted in the disruption of electronic systems, so the Bantul District Court sentenced the defendant BBA to 7 months imprisonment.

Criminal liability for hacking is based on the provisions of Article 30 of the ITE Law. In article 30 of the ITE Law, a person can be convicted if the person accesses the victim's electronic system or computer and also in this article determines that the method used is by any means (including hacking) as long as it is done without his right. If a website is hacked by a hacker, then the web hosting service provider cannot be held criminally liable. The web hosting service provider is only a media provider, but the owner of the web hosting service provider cannot avoid being held criminally liable if the owner makes his service solely to facilitate criminal acts. Similarly, an apartment building provider cannot be held liable if the owner of the apartment is entered by a herd of thieves.

CLOSING

1. CONCLUSION

Based on the results of research conducted by the author, it can be concluded that criminal law enforcement against cyber crime hackers based on Law Number 19 of 2016 concerning Electronic Information and Transactions, which is an amendment to Law Number 11 of 2008 by focusing on the role of law enforcement officials consisting of the police, prosecutors, and courts. The hacking case committed by BBA refers to the provisions of Article 49 Jo Article 33 and Article 48 paragraph (1) Jo Article 32 paragraph (1) and Article 45 paragraph (4) Jo Article 27 paragraph (4) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE. This article is used as the basis for the prosecutor to formulate charges and charges against the perpetrator. Meanwhile, the judge will lead the trial process and give a decision in accordance with the evidence and examination in the trial.

2. ADVICE

The judge's consideration in deciding a case can aggravate and mitigate the defendant. So that in this case, the defendant was sentenced to seven months. The police in carrying out their functions have several obstacles, which are based on aspects of the ability of investigators, limited evidence, limited facilities and infrastructure, and the breadth of existing jurisdictions.

REFERENCES

Suhariyanto, B. (2014). Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya. Jakarta: Rajawali Pers.

Soekanto, S. (1990). Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum). Bandung: Mandar Maju.