International Journal of Law, Crime and Justice
Vol.1, No.3 September 2024
e-ISSN: 3047-1362; p-ISSN: 3047-1370, Pages 136-143
DOI: https://doi.org/10.62951/ijlcj.v1i3.137
Available online at: https://international.appihi.or.id/index.php/IJLCJ

Efforts to Implement Cybercrime Offences in Using Social Media

Ahmad Zulqarnain Hasibuan[1], Syaiful Asmi Hasibuan[2]
[1-2]Panca Budi Development University, Indonesia

Address : Jl. Gatot Subroto No.km, Simpang Tj, Kec. Medan Sunggal, Medan City, North Sumatra 20122, Indonesia

Abstract Knowing how legal remedies are in the use of social media, social media has become a phenomenal and inseparable need for the Indonesian people. Some of the features possessed by social media include uploading statuses, sharing news pages, chatting, audiovisual communication and other features. Even though all people's behavior on social media platforms has been regulated by law, criminal acts as cybercrime still occur. Cybercrime is an unusual form of crime, in fact this crime can not only harm society, but can cause losses, and the peak can even destroy a country. This information age is often referred to as the digital revolution through technological developments and the development of communication tools. The internet is an information and communication technology that is most often encountered in human activities. The internet is one for surfing in cyberspace without any restrictions, a network that is very easy to access. The Criminal Procedure Code (KUHAP) and the Law on Information and Electronic Transactions (UU ITE), namely Law Number 19 of 2016 Amendments to Law Number 11 of 2008 have been applied to cyber crime.

Keywords: Cybercrime, Social Media, Criminal

1. INTRODUCTION

Many things are happening at this time with internet access that is very easy to access anytime, anyone and anywhere, minors can access the internet via their mobile phones and then view sites that are spread on social media that tell adult problems. So that it causes unexpected consequences such as imitating the negative things they have seen, which can cause damage to the nation's successors. So that humans can also master technology, a real bad impact occurs with various forms of cybercrime (Cyber Crime) as a result and even the target of the globalisation of information, various technological products such as the very well know mobile phone or what we often know as a mobile phone, greatly facilitates humans in accessing information which can also facilitate cybercrime.

Cybercrime is a criminal activity in cyberspace using the main means of sophistication of computer technology as a tool and internet network as a medium. Cybercrime is a crime that has a cross-border nature, meaning that this crime can occur anywhere and occur in various countries and can occur at any time. Cybercrime also has two meanings, namely, in a broad sense. Cybercrime is all illegal acts committed through computer networks and the internet to gain profit by harming other parties. While in a narrow sense, Cybercrime is all illegal actions aimed at attacking computer security systems and data processed by a computer system.

Cyber crime, also referred to as virtual crime, utilises technological developments to

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 28 2024; Online Available: July 31 2024;

commit unlawful acts with various motives, ranging from self-indulgence or ignorance to criminal acts that cause financial or political harm. This type of crime also depends on the offender's ability to master technology. With this, several cybercrime cases have emerged in Indonesia such as credit card breaches, hacking of several websites, buying and selling fraud, intercepting data transmissions, distributing illegal content on social media, hate speech, hijacking social media accounts and manipulating data.

The Electronic Information and Transaction Law or ITE Law is the first Cyberlaw in Indonesia that specifically regulates information and electronic transactions. The material of the ITE Law can be grouped into two major parts, namely the regulation of information and electronic transactions and the regulation of prohibited acts (CyberCrime). CyberCrime provisions are international instruments used by many countries. The two major contents regulated in the ITE Law are the regulation of electronic transactions and Cyber Crimes. The material of the ITE Law is the implementation of several principles of international provisions, the scope of the ITE Law material, in general, among others, contains information and electronic documents, sending and receiving electronic mail, electronic signatures, electronic certificates, the implementation of electronic systems, electronic transactions, intellectual property rights and privacy, as well as criminal provisions relating to the use of information and electronic transactions.

With laws and regulations governing the problem of cybercrime in social media, it is hoped that criminal offences in electronic crimes can be resolved so that in the future this problem can be resolved so that people can be more careful in taking actions in social media. Based on the background description above, the author is interested in studying and knowing more about these problems in a scientific work with the title, Efforts to Determine Cybercrime in Using Social Media.

Problem Formulation

1. How is the determination in criminal offences against misuse of Social Media
2. How is the Criminal Policy carried out to prevent the misuse of Social Media.

Literature Review

Social media abuse is the spread of hoax news, cyberbullying, defamation, data falsification, hacking fraud and others. Criminal sanctions are given to someone when they commit an offence or crime. Criminal sanctions become the realm of public law so that its implementation requires intervention from the state. The imposition of punishment only focuses on giving pain to the perpetrators of criminal offences. The settlement of criminal cases does not always have to be resolved by the judicial system. Justice that is expected by the community can be realised through other alternatives outside the litigation channel.

The perpetrators of cyber crime are usually called hackers. Police efforts in overcoming cyber crime also refer to Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), namely the Police as Investigators and Investigators of a criminal offence, specifically regulated in Article 1 of Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), in Article 1 paragraph 1 which contains that: 'Investigators are state police officers of the Republic of Indonesia or certain civil servants who are specifically authorised by law to investigate criminal offences'.

Based on a letter from the President of the Republic of Indonesia. No.R./70/Pres/9/2005 dated 5 September 2005, the text of the ITE Law was officially submitted to the House of Representatives. On 21 April 2008, this law was enacted; thus the process of enacting the ITE Law has lasted about five years. Therefore, the ITE Law, which consists of 13 chapters and 54 articles, is a relatively new law both in terms of its enactment and the material it regulates. Law No. 11/2008 on Electronic Information and Transactions is necessary for Indonesia, because currently Indonesia is one of the countries that has used and utilised information technology widely and efficiently, and factually does not have many legal provisions, especially from the aspect of criminal law.

Research Methods

The data collection technique in this research is document study or library research, and the data analysis used in this research is qualitative analysis. Qualitative approach is the method that will be chosen in this writing more specifically through emphasis on literature study. This research is normative legal research, namely research conducted by collecting and analysing secondary data. This research is descriptive, namely research by means of exposure which aims to obtain a complete picture (description) of the state of the applicable

laws and regulations associated with legal theories. The research method is used as a systematic way to search, find, develop, analyse a problem, test the truth objectively and optimally and carry out the correct method in research. This research uses normative juridical research methods.

2. DISCUSSION

Article 1 of Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), in Article 1 paragraph 1 which states that: 'Investigators are state police officers of the Republic of Indonesia or certain civil servants who are specifically authorised by law. Based on the letter of the President of the Republic of Indonesia. No.R./70/Pres/9/2005 dated 5 September 2005, the text of the ITE Law was officially submitted to the House of Representatives. On 21 April 2008, this law was enacted; thus the process of enacting the ITE Law has lasted about five years. Therefore, the ITE Law consisting of 13 chapters and 54 articles is a relatively new law both in terms of its enactment and also in terms of the material it regulates.

Law Number 11/2008 on Electronic Information and Transactions is necessary for Indonesia, because currently Indonesia is one of the countries that has used and utilised information technology widely and efficiently, and factually does not have many legal provisions, especially from the aspect of criminal law .

Other criminal provisions outside the Criminal Code, in the form of insult, defamation, defamation, unpleasant behaviour, provocation, incitement and spreading false news. In the case of the alleged occurrence of the criminal offence of hate speech based on the Chief of Police Circular Letter Number SE/06/X/2015 on Hate Speech, it refers to the provisions of Article 156 of the Criminal Code, Article 157 of the Criminal Code, Article 310 of the Criminal Code, Article 311 of the Criminal Code, Article 28 paragraph (2) jis. Article 45 paragraph (2) of Law Number 11 Year 2008 on Electronic Information and Transactions. Criminal liability for persons proven to fulfil the elements of the criminal offence in Article 28 paragraph (2) of ITE based on Article 45A paragraph (2) of ITE is imprisonment for a maximum of 6 years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah).

According to Riduan Syahrani, what is meant by proof is the presentation of valid evidence according to the law to the judge examining a case in order to provide certainty

about the truth of the events presented. The existence of evidence is very important, especially to show the existence of legal events that have occurred.

Some of the changes in the new ITE Law are as follows:

a. Confirming that the criminal elements in the provision refer to the provisions of defamation and slander regulated in the Criminal Code.

b. Lowering the criminal punishment in 2 (two) provisions in Article 29 as follows: First, the criminal punishment for insult and/or defamation is reduced from a maximum imprisonment of 6 (six) years to a maximum of 4 (years) and/or a fine from a maximum of Rp 1 billion to a maximum of Rp 750 million. Second, the criminal punishment for sending electronic information containing threats of violence or fear is reduced from a maximum imprisonment of 12 (twelve) years to a maximum of 4 (four) years and/or a fine from a maximum of Rp 2 billion to a maximum of Rp 750 million. Third, implementing the decision of the Constitutional Court on 2 (two) provisions as follows:

c. Amend the provisions of Article 31 paragraph (4) which originally mandated the regulation of interception or wiretapping procedures in a Government Regulation to be in the Law.

d. Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hukum yang sah.

e. Synchronising the procedural law provisions in Article 43 paragraphs (5) and (6) with the procedural law provisions in KUHAP, namely: First, search and/or seizure, which originally had to obtain permission from the Chief of the local District Court, should be adjusted to the provisions of KUHAP. Second, arrest and detention, which originally had to request a determination from the Chairman of the local District Court within 1×24 hours, was readjusted to the provisions of the Criminal Procedure Code.

f. Strengthening the role of Civil Servant Investigators (PPNS) in the ITE Law in the provisions of Article 43 paragraph (5) related to the authority to limit or terminate access related to information technology criminal offences and the authority to

request information from Electronic System Operators related to information technology criminal offences.

Law No. 19 of 2016 on Electronic Information and Transactions on the amendment of Law No. 11 of 2008 on Electronic Information and Transactions has been relatively accommodating normatively in answering the needs of society in conducting activities in the cyber world.

The forms of CyberCrime that often occur in the North Sumatra Regional Police are defamation, online gambling and immoral content. Up to May 2022, defamation is the most common form of cybercrime from year to year. Followed by cases of indecent content/pornography which experienced a decrease in the number of cases each year and also cases of online gambling which are CyberCrime criminal offences that have experienced the most drastic decrease in the number of cases until 2022.

The role of the police, especially in the North Sumatra Regional Police in law enforcement of cybercrime until 2022, can be seen from the results of research where the police initially receive reports or complaints related to cyber crime problems and then conduct investigations in determining the status of the reported suspect as a suspect in law enforcement of cybercrime which is carried out after clear evidence and can be linked directly to the reported or direct action. The process of proving the reported party as a suspect (perpetrator) is carried out by examining physical evidence, witness and victim testimony, expert witness testimony, and reported party testimony.

Defamation committed by using 'writings and drawings'. Writing is the result of writing either by hand or by any instrument in the form of a series of words/sentences in any language whose content contains a certain meaning, attacking the honour and good name of the person done on a paper or other object that can be written. The writing may be made in any language, provided that it is in a language understood by the people in the place where it is broadcast, displayed or pasted. Law as a tool to change society or social engineering is nothing but the ideas that the law wants to realise.To ensure the achievement of the function of law as community engineering towards a better direction, it is not only required the availability of law in the sense of rules or regulations, but also a guarantee of the realisation of these legal rules into legal practice, or in other words, a guarantee of good law enforcement.

The working of the law is not only the function of the legislation, but also the activities of the implementing bureaucracy. The types of cyber crime in the form of

grouping, namely: decency content, gambling, causing hatred, sending information on threats of violence, illegal access crime, falsification of information or electronic documents, and other criminal offences.

The policy of overcoming cyber crime with criminal law is included in the field of penal policy which is part of criminal policy. From the criminal policy point of view, crime prevention efforts (including cybercrime prevention) cannot be done only partially with criminal law (penal means), but must also be taken with an integral/systemic approach. Cybercrime takes a huge toll on victims, especially financially. Most of the victims can only regret what happened. They hope to have learnt a lot from their experiences by now, and what needs to be done now is to prevent the possibilities that can harm us as IT actors. The prevention can be in the form of:

1) Educate users (provide new knowledge about cyber crime and the internet world)
2) Use hacker's perspective (use hacker's thinking to protect your system)
3) Patch the system (close the holes of weaknesses in the system)
4) Policy (setting policies and rules to protect your system from unauthorised people)
5) IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System)
6) AntiVirus.

3. CONCLUSIONS

Cyber crime has become a new problem as a result of technological developments, where proving criminal offences is increasingly difficult and the perpetrators are also increasingly difficult to identify. Cyber crime can also cover a wide area to the international world, so that the investigation of the case is increasingly difficult to do and requires special expertise for the police in the field of information technology. The perpetrators of cyber crime are usually called hackers. Police efforts in tackling cyber crime also refer to Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), namely the Police as Investigators and Investigators of a criminal offence, specifically regulated in Article 1 of Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), in Article 1 paragraph 1 which contains that: ‘Investigators are state police officers of the Republic of Indonesia or certain civil servants who are specifically authorised by law to investigate criminal offences’. The policy of tackling cybercrime with criminal law is included in the

field of penal policy which is part of criminal policy (crime prevention policy). From the perspective of criminal policy, crime prevention efforts (including cybercrime prevention) cannot be done partially with criminal law (penal means), but must also be taken with an integral/systemic approach.

REFERENCE

Republik Indonesia. (2016). Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik tentang perubahan atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jakarta: Lembaran Negara.

Republik Indonesia. (1981). Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Jakarta: Lembaran Negara.

Kepolisian Republik Indonesia. (2015). Surat Edaran Kapolri Nomor SE/06/X/2015 tentang Ujaran Kebencian (Hate Speech). Jakarta: Kepolisian Republik Indonesia.

Ruth, et al. (2023). Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara. Volume 2, 2 Maret, 300.

Lubis, M. R., et al. (2022). Peran Polri Dalam Menanggulangi Tindak Pidana Penghinaan Dan/Atau Pencemaran Nama Baik Melalui Media Elektronik (Studi di Polda Sumatera Utara). Vol 5, No. 2, November.

Hery, et al. (2021). Penerapan Kebijakan Digital dalam Rangka Pencegahan Cyber Crime Ditinjau dari Undang-Undang ITE. Jakarta, 2 Desember.

Kusnadi, F. (2020, September 15). Hasil wawancara dengan AKP Fery Kusnadi selaku Tim Penyidik dari Subdit V Cyber Crime Ditreskrimsus Polda Sumut.

Dwi. (2022). Implementasi Upaya Penanggulangan Tindak Pidana Cyber di Era Teknologi. Lampung.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. Jurnal Bisnis dan Ekonomi (JBE), 18(2), 189.

Presiden Republik Indonesia. (2005). Surat Presiden RI. No.R/70/Pres/9/2005 tanggal 5 September 2005.

Wahid, A., & Labib, M. (2005). Kejahatan Mayantara (Cyber Crime). Jakarta: PT. Refika Aditama.