POLICE EFFORTS IN COMBATING CYBERCRIME AT THE RIAU ISLANDS REGIONAL POLICE

R Moch Dwi Ramadhanto[1], Idham[2], Parameshwara[3], Fadlan[4], Erniyanti[5]

[1] *Student, Master In Law, Universitas Batam, Batam, Indonesia*
[2,3,4,5]*Lecture, Faculty of Law, Universitas Batam, Batam, Indonesia*

ABSTRACT

The State of Indonesia is based on the law in the 1945 Constitution article 1 paragraph (3). All citizens have the same position before the law and government and are obliged to uphold this law and government without exception. Fake news (hoax) is news, information, counterfeit or fake news, while in KBBI, it is called a hoax, which means fake news. Hoax is a harmful excess of freedom of speech and opinion on the internet: mainly social media and blogs. Meanwhile, the journalistic dictionary interprets fake news (libel) as news that is not true. It leads to defamation cases. Another term for fake news in a journalistic context is fabricated news/fake news. Reporting that is not based on reality or truth for a specific purpose. Fake news (hoaxes) can cause anxiety, hatred, and hostility; the source of information is unclear and unverified and tends to corner certain parties. The circulation of hoax news quickly occurs among people with deficient literacy levels. Usually, they readily accept information for granted without checking. They even spread it without considering the accuracy of the information they receive, and the community ends up falling into a confusion of news, provocation, and mutual suspicion. If hoaxes are allowed to continue, they will impact human character and can even interfere with mental health. In Riau Island, Cybercrime is also rife due to the lack of public and individual awareness of what is conveyed; they do not take the origin of the news to be delivered. This is due to the lack of oversight in Cybercrime, so it needs supervision in providing information. Besides that, human resources are a point that the police must pay attention to in Countering Cybercrime.

Keyword: *Cyber Crime*, Criminal, Police Effort

1. INTRODUCTION

The State of Indonesia is based on the law in the 1945 Constitution article 1 paragraph (3). All citizens have the same position before the law and government and are obliged to uphold this law and government without exception. A state based on legal principles is characterized by several principles, among which are that all actions or actions of a person, whether individual or group, people or government, must be based on legal provisions and statutory regulations that existed before the activity or movement was carried out or based on applicable laws.

The rule of law is a country that stands above the law that guarantees justice to its citizens, justice is a requirement for achieving happiness in life for its citizens, and as the basis of justice, it is necessary to teach a sense of decency to every human being so that he becomes a good citizen, as well as regulations. Fundamental law only exists if the rule of law reflects justice for the association of life between citizens, for Aristotle, who rules in the state, is not a real human being. Still, in a just mind, while the absolute ruler is only the holder of law and balance, decency will determine whether or not a regulation of laws and making laws are part of the ability to state government, that what is important is educating people to become good citizens.Berita bohong (*hoax*) adalah kabar, informasi, berita palsu atau bohong, sedangkan dalam KBBI disebut dengan hoax yang artinya berita bohong. Hoax merupakan ekses negatif kebebasan berbicara dan berpendapat di internet. Khususnya media sosial dan blog. Sedangakan dalam kamus jurnalistik mengartikan yaitu berita bohong (*libel*) sebagai berita yang tidak benar sehingga menjurus pada kasus pencemaran nama baik. Istilah lain berita bohong dalam konteks jurnalistik adalah berita buatan atau palsu (*fabricated news/fake news*) (Janner Simarmata, 2019).

Reporting that is not based on reality or truth for a specific purpose. Fake news (hoaxes) can cause anxiety, hatred, and hostility; the source of information is unclear and unverified and tends to corner certain parties. The spread of hoax news is also carried out for various reasons, such as humor, art, entertainment, education, and others. The circulation of hoax news quickly occurs among people whose literacy level is still deficient, usually, they readily accept information for granted without checking, they even spread it without considering the accuracy of the information they receive. The public was confused about news, provocation, and mutual suspicion. If hoaxes are allowed to continue, they will impact human character and can even interfere with mental health.

Electronic transactions are legal actions using computers, computer networks, and other electronic media. The government publishes the dissemination of hoax news through social media, including violating Article 28 paragraph (1) and paragraph (2) of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which reads:

1. Everyone who deliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions shall be subject to imprisonment for a maximum of 6 (six) years and a fine of Rp. 1,000,000,000.00 (one billion rupiahs) .
2. Everyone who deliberately and without rights disseminates information aimed at causing hatred or hostility towards specific individuals and community groups based on ethnicity, religion, race, and inter-group (SARA) will be punished with imprisonment for a maximum of 6 (six) years and a maximum fine of IDR 1,000,000,000.00 (one billion) (Janner Simarmata, 2019).

The efforts to deal with crimes committed by the Police include:

1. Pre-Emptive: The initial efforts made by the Police to prevent crime. Efforts made in pre-emptive crime prevention are instilling good values or norms so that they are instilled in a person to prevent him from committing crimes, if the values or standards have crystallized properly, then it can eliminate the intention to commit crimes even though there is an opportunity. In this pre-emptive response effort, the Police as law enforcers prevent crimes from occurring by providing an understanding of the importance of complying with applicable laws [1].
2. Preventive That is a follow-up of pre-emptive efforts which are still in the prevention stage before the crime occurs. The emphasis of this effort is to eliminate the opportunity to commit a crime. Repressive Efforts are efforts made when an offense or crime has occurred by enforcing the law (law enforcement) against the perpetrator. The police, carrying out effort, conduct legal counseling related to crime and provide lessons about legal arrangements related to crime. So that it can minimize the perpetrators of committing crimes, besides that the police conduct counseling.
3. Repressive. The effort is carried out when a crime has occurred whose action is in the form of law enforcement by imposing a sentence. The countermeasures are taking action against the perpetrators of crimes according to their actions and repairing them again so that they are aware that the activities committed are unlawful and detrimental to society. This effort can also be accompanied by reasonably firm measures from law enforcers, especially the police.

In the Riau Archipelago, Cybercrime is also rife due to the lack of public and individual awareness of what is conveyed, so they do not take the origin of the news to be delivered. This is due to the lack of oversight in Cybercrime, so it needs supervision in providing information, besides that human resources are a point that the police must consider in Countering Cyber Crime in the Police The Riau Archipelago region cannot be separated from the widespread role of the internet, so that there are no restrictions on spreading hoax news and internet usage at young and old ages [2]. The author wishes to conduct research entitled "Police Efforts in Combating Cybercrime in the Riau Islands Regional Police."

A. Research Benefits

Referring to the formulation of the problem that the author has stated above, the author wishes to research the Obstacles and Efforts to Overcome Cyber Crime in the Riau Islands Regional Police. The following are the benefits of this research:

1. Theoretically

With this research, I hope it can use as a reference or additional reading material that will put forward the theoretical discipline of law. The writing of this thesis is expected to provide an understanding of what efforts have been made by the Police in Overcoming Cyber Crime at the Riau Islands Regional Police. In addition, expected to be helpful as a reference or reference material in researching similar matters, and writing this thesis can assist

readers in developing lecture materials. It is expected to be able to contribute new knowledge in the field of public order.

2. Practically

The results of this study are expected to provide an accurate, practical solution to the problems under investigation. Besides that, it is input material for practitioners who are directly involved and can reveal new theories for developing existing approaches in carrying out a policy of laws and regulations in the field of public order.

B. Research Methods

This research method is a managed, systematic, data-based, critical, objective, and scientific investigation or investigation of a specific problem aimed at finding alternative solutions to related issues. The following are the methods in this study:

1. Research Specifications

The specification of this research is only to carry out analysis only up to the level of diathesis, namely analyzing and presenting facts systematically so that they can be more easily understood and concluded. Research specifications or the type of research is a choice of the kind of research format in researching research objects in the field of law studied by researchers. In particular, according to the type, nature, and purpose, the specifications of legal research by Soerjono Soekanto are distinguished, namely normative legal research and sociological or empirical legal research [3].

The specification and type of research for this thesis is normative legal research while at the same time combining it with sociological (empirical) legal research using secondary data obtained directly as the first source through field research through interviews and primary data as a source/information material in the form of direct legal material, secondary legal material.

2. Approach Method

The approach method in this research combines the normative approach of "legal research" with the empirical approach of "juridical sociology." Decomposing research explanations carries out the research mechanism with this combined approach method from an inductive to a deductive method and vice versa. The author does this to help explain the relationship between research variables and research objects so that it can produce an understanding that is very helpful for readers, especially researchers and academics.

3. Data Collection Techniques and Data Collection Tools

This type of research is included in the combined research group between normative legal research (library research) and observational research [4]. As data and data sources used in this study are primary data and secondary data, which can be grouped as follows:

1. Primary Legal Materials, namely the primary data that the author obtained by viewing, collecting, and comparing applicable legal regulations, including laws, government regulations, and related matters in this thesis originating from Law Number 19 the year 2016 concerning information and electronic transactions on the spread of fake news (hoax).
2. Secondary Legal Materials, in secondary data can be divided into three types, namely:
   a. Primary Legal Data, the authors conducted interviews, namely direct debriefing of the respondents that the authors have specified above.
   b. Secondary legal data, such as journals, articles, and other literature related to this research.
   c. Tertiary legal data, such as dictionaries, clippings, and so on that, are similar to the tertiary legal material that can support research.

4. Data Analysis

Data analysis was carried out qualitatively by describing the research, then comparing the data and legal theories, legal experts, and legislation, where the study started with data collection, data processing, and finally, data presentation. While concluding, will use the deductive method, namely the author takes data, statements, and opinions, which are general, and then draws specific conclusions [1].

2. RESULTS AND DISCUSSION

1. Definition of Cybercrime

The development of computer, information, and communication technology has also led to the emergence of new crimes that have different characteristics from conventional crimes. Computer abuse, as one of the impacts of the three technological developments, is inseparable from its nature which has its attributes so that it brings complex problems to be solved about the issue of handling them starting from investigations, investigations to prosecutions.

Cybercrime is a form of crime that arises because of internet technology. Some opinions identify cybercrime as computer crime. This cybercrime can cause losses in several fields, namely political, economic, and socio-cultural, which is significant and pays more attention than other high-intensity crimes [2].

Cybercrime is an act that is disgraceful and violates decency in society and violates the law, even though until now, it has been difficult to find legal norms that specifically regulate cybercrime. Therefore, the role of culture in efforts to uphold the law against cybercrime is essential to determine the nature of being reprehensible and violating the social decency of an act of cybercrime [3]

2. Cyber Crime Characters

Cybercrime arises because of advances in digital information and technology, which make it easier for people to communicate, get information, and facilitate business. However, the convenience provided by technology makes technology a destination for acquiring and spreading distractions. The characteristics of cybercrime are the use of information technology to commit crimes that are supported by digital information and technology. According to Abdul Wahid and M. Labib, cybercrime has several characteristics including: [3].

a. Actions carried out illegally, without rights or ethically taking place in cyberspace or territory, so that it cannot be determined which state jurisdiction applies to them;
b. These acts are performed using any internet-related device;
c. These actions result in material or immaterial losses, which tend to be greater than conventional crimes;
d. The perpetrators are people who dominate the use of the internet and its applications;
e. These acts are often carried out transnationally.

Based on the characteristics above, to facilitate handling, cybercrimes can be classified as [1]

a. Cyberpiracy, namely the use of computer technology to reproduce data or software and then distribute information or software through computer technology.
b. Cybertrespass, namely the use of computer technology to increase access to individual or organizational computer systems.
c. Cybervandalism, namely the use of computer technology systems to create programs that interfere with electronic transmission processes and destroy data on computers.

Based on Perpol No. 8 of 2021 Article 8 paragraph (1), where special requirements for criminal acts of information and electronic transactions as meant in market seven letter a, include:

a. Perpetrators of information crimes and electronic transactions that spread illegal content.
b. The perpetrator is willing to delete the content that has been uploaded;
c. The perpetrator conveyed an apology through a video uploaded on social media and a request to delete content that had spread.
d. The perpetrator was willing to cooperate with Police Republick Indonesia investigators to conduct a follow-up investigation.

Meanwhile, the implementation mechanism refers to the Memorandum of Understanding number 131/KMA/SKB/X/2021 concerning the Implementation of Adjustments to the Limits for Misdemeanor Crimes and the Number of Fines, Quick Examination Procedures, and the Implementation of Restorative Justice.

3. Forms and Types of Cyber Crime

Cybercrime is a relatively new form of crime compared to other conventional forms (street crime). In simple terms, crime in cyberspace (cybercrime) can be interpreted as a type of crime committed by influencing the internet media as a means of its form. With the development of technology, various kinds of crimes will be carried out because they are caused by multiple factors, as previously explained. As for the different types of technological crimes, the victims' reports and the results of the identification of legal experts are adjusted and classified based on the applicable law. Crimes whose actions are closely related to the use of computer technology and telecommunications networks in several publications and practices are grouped into the following forms:[1]

a. *Unauthorized access to computer system and service*

It is a crime in a computer network system that is carried out illegally without permission, or the knowledge of the owner of the computer network system is entered. Usually, the perpetrators (hackers) do this to take or steal essential and confidential information. However, some do it simply because they feel challenged to prove their experience penetrating a system with a high level of protection. This crime is increasingly widespread with the development of internet technology.

b. *Illegal content*
Committing a crime by entering data or information into the internet about something unethical, incorrect, and considered to disturb public order or violate the law. The following are examples of illegal content:
1) Loading of false and defamatory news that will damage the dignity or self-esteem of other parties.
2) Loading of things related to pornography.
3) Loading of information constituting state secrets, agitation and propaganda against the legitimate government, and so on.

c. *Forgery* Data
It is a crime in which important documents and data stored on a computer as scriptless documents via the internet are falsified. This crime is usually aimed at e-commerce documents by making it appear that a typo has occurred, which aims to benefit the perpetrator.

d. *Cyber espionage*
It is a crime that carries out espionage activities against other parties by utilizing the internet network, by entering the target party's computer network system. This crime is usually committed against business rivals whose essential data or documents are stored on the computer.

e. *Cyber sabotage and extortion*
It is a crime committed by disrupting, damaging, or destroying data, computer programs, or computer network systems connected to the internet. Usually, this crime is committed by inserting a logical bomb, a computer virus is included in a computer network so that computer programs, data, or computer network systems cannot be used as they should.

f. *Offence against intellectual property*
It is the property that is directed against intellectual property rights owned by someone on the internet, for example, illegally reducing the appearance of the webpage of a site owned by another person, broadcasting information on the internet, which is another person's trade secret, and so on.

g. *Infringements of privacy*
It is a crime directed against someone's information that is very personal and confidential. This crime is usually directed against someone's personal information stored on a computerized personal data form, which, if known by another person, can harm people materially or immaterially, such as credit card numbers, ATM PIN numbers, information about hidden defects or diseases, and so on. etc.

In general, the types of cybercrimes developed in today's society can be divided in several ways, the problem of cybercrimes based on their motives can be divided in several ways, including: [1]

a. Hacker. Hackers mean to destroy, in a broad sense, those who infiltrate or harm through computers. Hackers can also be defined as people who like to learn the ins and outs of computer systems and experiment with them.
b. Cracker. A cracker is someone who can and can penetrate the network and steal or damage the network.
c. Precker. A precker is very skilled at penetrating networks and will tell the network that others can penetrate the network's security.
d. Hacking
Hacking (hacking) is an activity carried out to find information about other people through existing programs using computers. Hacking is a form that receives a lot of attention and is often called the first crime because, from a technical perspective, piracy has advantages over other cybercrimes.
e. *Cyber fraud*
Cyber frand It is a fraud that will be carried out through its main ingredient, the internet.
f. Cyberporn

Cyberporn or cyber pornography is a cybercrime in which the perpetrator presents pornographic images on websites through internet media. In addition, cyberporn is also used as a business arena for sex, for example, selling and buying porn VCDs, pornographic pictures, etc.

4. Faktor Penyebab Terjadinya Cyber Crime

The causes of cybercrime include:

a. Unlimited internet access.
b. Negligence of computer users. This is one of the leading causes of computer crime.
c. Easy to do with little security reasons and no need for super modern equipment. Although computer crimes are easy to commit, it can be difficult to track them down, thus encouraging criminals to continue doing this.
d. The perpetrators are generally intelligent people who are curious and passionate about computer technology. The knowledge of computer criminals about how a computer works are far above is of computer operators.
e. Weak network security system.
f. Lack of public attention. Society and law enforcers are still paying great attention to conventional crimes. Computer criminals continue to commit crimes [1].

5. Factors Driving the Growth of Cyber Crime

Several factors are driving the growth rate of cybercrime or cyber crime, including the following:

1. Kesadaran hukum masyarakat
2. Faktor keamanan
3. Faktor penegakan hukum
4. Faktor ketiadaan Undang-Undang

Crime in cyberspace can happen anywhere and by anyone. This crime will not occur if there is high public awareness of being responsible for accessing various types of internet networks. Thus, this can minimize the growth of crime in cyberspace.

6. Pencegahan Tindakan Cyber Crime

1. *Educate user*
2. *Use hacker's perspective*
3. *Patch system*
4. *Policy*
5. IDS *(Intrusion Detection System) bundled with IPS (Intrusion Prevention System)*.
6. *Antivirus Firewalls*.

7. Penanggulangan Tindakan Kejahatan *Cyber Crime*

1. Cybercrime can be carried out without recognizing territorial boundaries and does not require direct interaction between the perpetrator and the victim of the crime. Here's how to deal with it:
2. 1. Modernizing the national criminal law and its procedural law.
3. 2. Improving the national computer network security system according to international standards.
4. 3. Increasing the understanding and expertise of law enforcement officials regarding efforts to prevent, investigate and prosecute cases related to cybercrime.
5. 4. Increasing citizen awareness regarding the problem of cybercrime and the importance of preventing this crime from happening.
6. 5. Increasing cooperation between bilateral, regional, and multilateral countries in efforts to deal with cybercrime.

8. Definition of Crime

The definition of a criminal act in question is that a criminal act or criminal act is always an act that is inconsistent with or violates a rule of law or an act prohibited by the rule of law accompanied by criminal sanctions in which the rules are aimed at acts. In contrast, threats or criminal sanctions are aimed at the person who did or the person who caused the incident.

According to legal experts E.Y. Kanter and S.R. Siantur, crime has 5 (five) elements which include

a. Subject;
b. Error;
c. Is against the law of an action;
d. An action prohibited or required by law and punishable by a criminal offense; and
e. Time, place, and circumstances (other objective elements).

9. Tujuan Hukum Pidana

Criminal law aims to protect all of a person's interests or human rights and the interests of the whole society and the State. Protect from evil or despicable actions on the one hand and all activities of arbitrary authorities on the other. Therefore what is protected by criminal law is not only individuals but the State must also be protected, and society is the property of individuals. According to Wirjono Prodjodikoro, the purposes of sentencing include:

a. a. The purpose of such punishment is to frighten someone from committing a crime and prevent someone from committing a crime, both in terms of frightening people (preventive generals) and scaring someone who commits a crime so that someone will not commit another crime in the future. (preventive specialty);
b. b. The purpose of the punishment is to educate or improve someone who commits a crime so that they become good people who benefit the surrounding community.

10. Police Efforts to Overcome Cyber Crime Crime

In tackling cybercrime, the police have made various efforts, such as giving appeals to the public through electronic media and social media by distributing broadcasts in the form of requests related to cybercrime to be forwarded to the broader community. Apart from that, information was also provided to the public through the media, newspapers, and radio, and during talk shows, the police did not stop advising the public.

In carrying out this effort, the police have taken action by processing every cybercrime case handled by applicable regulations. The police work together with existing stakeholders, namely how to catch perpetrators who are caught in the act of committing a crime or through public reports, then go to the crime scene (TKP) to arrest and detain suspects in cybercrime cases, after the arrest is made then it is processed at the police and before being handed over case file with the attorney general. The role of the police in efforts to tackle cyber crime includes three (3) things, pre-emptive action, preventive action (prevention), and repressive action (law enforcement) [2].

11. Criminal Liability Against Hoax News Spreaders

Criminal responsibility can be accounted for by a perpetrator of a crime but must fulfill the 4 (four) elements of the following requirements [3]

1. There is an action (commission or omission) by the perpetrator;
2. Those who fulfill the formulations of offenses in the law;
3. The action is against the law;
4. The culprit must be accountable.

12. Proving the Crime of Spreading Fake News (Hoax)

Based on Article 184 of the Criminal Procedure Code (KUHAP) confirms that there are five valid pieces of evidence, namely:

1. Witness testimony;
2. Expert testimony;
3. Letters;
4. Instructions;
5. Statement of the accused.

In connection with cybercrime cases, the ITE Law regulates evidence other than those contained in Article 184 of the Criminal Procedure Code. The evidence referred to is emphasized in Article 5, paragraph (1) of the ITE Law, namely:

1. Electronic information and electronic documents;
2. Printouts of electronic information and electronic documents.

Conclusion

Based on the results of the discussion in this study, the researchers drew several conclusions, including:

1. With the existence of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, it becomes a legal protection for people or legal entities and the government affected by the spread of news or distribution of fake news or information. False information, or what we often hear with the term hoax, is an attempt to deceive or outsmart the reader or listener to believe something, even though the creator of the fake news knows that the information is fake.
2. The rule of law in Indonesia is a logical outcome that requires an institution that can oversee law enforcement, one of which is the police. So that the implementation of these rules requires the role of the police in efforts to tackle cybercrime, including three (3) things, namely pre-emptive action, preventive action (prevention), and repressive action (law enforcement).
3. Inhibiting factors in efforts to overcome cybercrime include internal and external factors. Internal obstacles start with a weak government and police oversight, evidence in cybercrime is easily changed, deleted, or hidden by criminals, there are rarely witnesses in cybercrime cases, and the determination of jurisdiction is unclear. In addition, external constraints include law enforcement, facilities or facilities, community, environmental factors, and cultural factors (culture).

REFERENCE

[1] Irwan, Peran Kepolisian dalam Upaya Pencegahan Tindak Pidana, Jurnal, Makassar, Unhas. 2018, hal. 55.

[2] Ahmad Qurtubi, Administrasi Pendidikan (Tinjauan Teori dan Implementasi), (Surabaya: Jakad Media Publishing, 2019), hal. 116.

[3] Noeng Muhajir, Metodologi Penelitian Kualitatif, Roke Sarasin, Jakarta: 1990, hlm. 92

[4] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D (Bandung: IKAPI, 2011) Cet. Ke-13. Hal 244.

[5] Edmon Makarim, 2005, Pengantar Hukum Telematika (Suatu Kajian Kompilasi), Jakarta PT. Raja Grafindo Persada, Hal 426.

[6] Abdul Wahid dan Mohammad Labib, Kejahatan Mayantra (Cyber Crime), Bandung: PT Refika Aditama, 2005), Hal 65.

[7] Dikdik M. Arief Mansur, dan Elisatris Gultom, Cyber Law Aspek Hukum Teknologi Informasi, (Bandung: PT. Grafika Aditama 2005), Hal 89.

[8] Abdul Wahid Dan M. Labib, Kejahatan Mayantara (Cybercrime), Penerbit Refika Aditama, Jakarta, 2009, Hal 76.

[9] Eliasta Ketaren, Cybercrime, Cyber Space, Dan Cyber Law, (2016), V Jurnal Hukum Stmik Time, Hal 36.

[10] Maskun, 2013, Kejahatan Siber (Cyber Crime) Suatu Pengantar, Kharisma Putra Utama, Jakarta, 2013, Hal 51-54.

[11] Jurnalis J. Hius, Jummaid Saputra, Anhar Nasution, Mengenal Dan Mengantisipas Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku (2014), Jurnal Hukum-Fhuui, Hal 3-4.

[12] Kanter E.Y & S.R. Sianturi, Azas-Azas Hukum Pidana Di Indonesia Dan Penerapannya, Penerbit Storia Grafika, Jakarta,2002, Hlm. 211.

[13] Sucipto.komputer.forensik..http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dantujuan.

[14] Romli Atmasasmita, 2000, Perbandingan Hukum Pidana, Penerbit Mandar Maju, Bandung, Hal 67.