MUST: ***Journal of Mathematics Education, Science and Technology***
Vol. 7, No. 1, Juli 2022 Hal 84-96
DOI: http://doi.org/10.30651/must.v7i1.15972

UNDERSTANDING CYBERCRIME AND CASES THAT OCCUR IN INDONESIA

Made Dwi Bayu Laksana, I Made Hery Suryawan
ITB Stikom Bali
bayugaming2158@gmail.com , herysuryawan10@gmail.com

Received 1 November 2022; revised 23 November 2022; accepted 1 Desember 2022.

ABSTRAK

Penyebaran informasi saat ini sangat mudah beredar karena adanya teknologi dan internet. Namun berbagai permasalahan muncul akibat penyalahgunaan teknologi tersebut, seperti cybercrime serta penyebaran berita hoax. Kontrol informasi sangat penting untuk mengevaluasi kredibilitas informasi serta sumbernya. Penelitian ini menyebutkan bagaimana mengatasi cybercrime serta hoax melalui seleksi informasi yang tepat. Namun hasil penelitian menunjukkan bahwa cybercrime dan penyebaran informasi hoax masih terjadi bahkan hingga saat ini. ada 3 ancaman UU ITE di Indonesia yang berpotensi menimpa pelaku cybercrimedengan memanfaatkan mediasosial yaitu ancaman pelanggaran kesusilaan pasal 27 ayat (1), penghinaan atau pencemaran nama baik pasal 27 ayat (3), dan penyebaran kebencian berdasarkan suku, agama, ras serta antar golongan (SARA) pasal 28 ayat (2). Upaya buat mencegah cybercime bisa dilakukan menggunakan cara melindungi komputer dari virus, menjaga privasi, mengamankan e-mail, melindungi Id/Account, menghasilkan backup data, serta selalu up to date terhadap berita. ada beberapa faktor yang harus diperhatikan dalam menyeleksi asal berita dari internet supaya terhindar dari bahaya cybercrime, yaitu, relevansi, akurasi, otoritas reputasi, objektivitas, kekinian, cakupan dan bukti yang kuat.

Kata kunci: cybercrime, kasus cybercrime, UU ITE

ABSTRACT

The dissemination of information today is very easy to circulate due to the existence of technology and the internet. Variousproblems arise due to the misuse of these technologies, such as cybercrime and the spread of hoax news. Information control is essential to evaluate the credibility of information as well as its umber. This research mentions how to overcome cybercrime and hoaxes through the selection of appropriate information. However, research shows that cybercrime and the spread of hoax information still occur even today. there are 3 threats of the ITE Law in Indonesia that have the potential to hit cybercrime perpetrators by utilizing social media namely the threat of violation of decency article 27 paragraph (1), humiliation or defamation of article 27 paragraph (3), and the spread of hatred based on ethnicity, religion, race and inter-group (SARA) article 28 paragraph (2). Efforts to prevent cybercime can be done using how to protect the computer from

viruses, maintain privacy, secure e-mail, protect Id / Account, generate data backups, and always be up to date with news. There are several factors that must be considered in selecting the origin of news from the internet in order to avoid the dangers of cybercrime, namely, relevance, accuracy, reputation authority, objectivity, currentness, coverage and strong evidence.

Keywords: cybercrime, cybercrime case, ITE Law

INTRODUCTION

The internet is a network of computers that are interconnected and communicate with each other. With the internet, everyone around the world can communicate using just a smartphone. Users can search for a variety of any information needed on the internet, sothat's how many individuals use it.

This development has made world relations less borderless, which has also had an impact on the social changes of society significantly. The result of this development in addition to providing benefits for the welfare and progress of society is also followed by the development of crime with various modes that use computers and computer networks as tools such as auction fraud, online gambling, identity fraud, child pornography, and terrorists. Crimes that occur in cyberspace are born due to the negative impact of technological developments, crimes that occur from various forms and types have consequences for the legal protection of their users, this is important considering that every human being must be protected in accordance with his dignity and dignity as a human being.

Indonesia is a country of law as stated in the constitution, as a country of law, of course, the state is obliged to protect every citizen from every act that can be harmful, especially if these actions can damage the order of life of the nation and state. Just like Kejahatan that occurs in cyberspace or commonly referred to as cybercrime. Cybercrime or digital crime is any form of crime that occurs in cyberspace or occurs digitally. Digital crimes are committed by involving computers and devices connected to a network. This cybercrime is part of international crime, because this crime occurs in cyberspace so it is difficult to determine which country's legal jurisdiction should be applied to the perpetratora.

RESEARCH METHOD

The methodology used in this writing is Text Studies and Documentation of news and articles on the rise of cybercrime. Through the study of texts and documentation of news and articles that have been collected and read by the author, the author makes an analysis and description. All articles, news that have been read are studied over and over again, so that a conclusion can be condensed back into an article that is a combination and core explanations of the collection of articles.

The data collection method is carried out through the collection of documents, both written documents and electronic documents yang derived from articles. The collected data is then compared and selected to be displayed in this writing. Tovalidate research data, triangulation techniques are carried out , namely qualitative research techniques as a reference to test whether the findings or research results reflect the existing situation and are supported by existing evidence. Triangulation is in principle a technique of checking the validity of data that utilizes something else outside of that data for the purposes of checking or being a comparison to the data.

RESEARCH RESULTS AND DISCUSSIONS

1. Definition of Cybercrime

   Cybercrime is the activity of a person, a group of people, a legal entity that uses k omputer as a means of committing a crime, and k omputer as a target.

2. Characteristics of Cybercrime

   So far in conventional crimes, there are known 2 types of crimes as follows:

   1. Blue collar crime

   This crime is a type of crime or criminal act that is carried out conventionally such as robbery, theft, murder and others.

   2. White collar crime

   This type of crime is divided into four groups of crimes, namely corporate crimes, bureaucrat crimes, malpractice, and individual crimes.

Cybercrime itself is a crime that arises as a result of the existence of a cyber community on the internet, has its own characteristics that are not in harmony with the two examples above. The unique characteristics of cybercrime include the following 5 things:

1. Scope of crime

2. The nature of the crime
3. Evildoers
4. Crime Mode
5. Types of losses incurred

3. Types of Cybercrime

Based on the type of activity it performs, cybercrime can be classified into several types as follows:

1. Unauthorized Access

   Fraudthat occurs when a person enters or infiltrates a computer network system unlawfully, without permission, or without the knowledge of the owner of the computer network system he enters. Probing and ports are examples of this evil.

2. Illegal Contents

   Crimesthat are carried out by entering data or information into the internet about something that is untrue, unethical, and can be considered as violating rules or disturbing public order, for example, the spread of pornography.

3. Intentional spread of the virus

   The spread of the virus is usually done using email. Often people whose email systems are exposed to viruses are unaware of this. The virus was then sent elsewhere via his email.

4. Data Forgery

   This type of crime is carried out with the aim of falsifying data on important documents contained on the internet. These documents are generally owned by institutions or institutions that have a web-based database.

5. Cyber Espionage, Sabotage, and Extortion

   Cyber Espionage means a crime that utilizes the internet network to carry out spying activities against other parties, by entering the target party's computer network system. Sabotage and Extortion means a type of crime committed by disturbing,

destroying or destroying data, computer programs or computer network systems connected to the internet.

6. Cyberstalking

   This type of crime is committed to damage or harass someone by using a computer, for example using e-mail and is carried out repeatedly. The crime resembles terror directed at someone by utilizing internet media. This can happen because of the ease of creating emails with a certain address without having to include actual self-characteristics.

7. Carding

   Carding is a crime committed to steal credit card numbers belonging to others and used in trading transactions on the internet.

8. Hacking and Crackers

   Kata hacker generally refers to someone who has a great interest in studying computer systems in detail and how to improve their capabilities. Those who often commit acts of destruction on the internet are usually called crackers. It can be said that this cracker is actually a hacker who uses his ability to make negative things. Cracking activities on the internet have a very wide scope, ranging from hijacking other people's accounts, website hijacking, probing, spreading viruses, to disabling target targets. The latter action is referred to as DoS (Denial of Service). A dos attack is an attack aimed at paralyzing a target (hang, crash) as a result of which it is unable to provide services.

9. Cybersquatting and Typosquatting

   Cybersquatting is a crime committed by registering someone else's company name domain and then attempting to sell it to that company for a higher price. Typosquatting is a crime by forming a pun domain, which is a domain that is similar to someone else's domain name. The name was the domain name of the company's rival.

10. Hijacking

    Hijacking is the crime of piracy of other people's work. the most common is Piracy software .

11. Cyber Terrorism

    An act of cybercrime includes Cyber Terrorism, jika threatening the government or citizens, including cracking into government or military sites. Some examples of Cyber Terrorism problems are as follows:

    - Ramzi Yousef, the mastermind behind the first attack on the WTC building, was known to store details of the attack in an encrypted file on his laptop.
    - Osama Bin Laden is known to use steganography for his network communications.
    - A website called the Muslim Hacker Club is known to write a list of tips for hacking the Pentagon.
    - A hacker who refers to himself as DoktorNuker is known to have defaced or altered the contents of web pages for about five years with anti-American, anti-Israel and pro-Bin Laden propaganda.

4. Statistics on the Increase in Cybercrime Cases in 2019-2020



Figure 1. Cyber attack rates for 2019-2020.

Based on the picture above, the number of cybercrimes in Indonesia increased very significantly in 2020 compared to 2019. This is due to the effects of the pandemic which makes most activities carried out online. Making

cybercrime crimes also experienced a very high increase. Modes of crime that often occur such as HOAX news, Pornography / Immorality, or The spread of hatred that often occurs on social media.

5. Cybercrime Cases

1. Pornography/Immoral Cases via Facebook.

As reported by Tempo magazine (April 16, 2014) the Directorate of Special Economic Crimes of the Criminal Investigation Agency of the Police Headquarters revealed a case of child pornographing through Facebook and Kaskus media in Surabaya, East Java. What happened happened to the victims was six minors. The police managed to identify the perpetrators and determine the manager of PT. KSM, whose initials are TAG, is a suspect. The case carried out by the suspect belongs to the realm of cybercrime. Violations committed by cybercrime perpetrators in accordance with pornography/immorality via Facebook above in accordance with the provisions of Article 27 paragraph (1) of the ITE Law and criminal threats for violators of the article are as described in Article 45 paragraph (1) of the ITE Law, namely imprisonment for a maximum of six years and/or a maximum fine of one billion rupiah. If understood in more depth, the provisions of article 27 paragraph (1) of the ITE Law have a very broad scope. This coverage may be any facebook user/member who provides profanity images or provides hyperlinks to a site that has pornographic content or commercial sex sales services and uses facebook as a place of transaction can also be charged in this article. Although the notion of porn itself is still very vague and cannot be interpreted clearly, for example, the image categorizes it as an element of photographic art. In this case, of course, procedures and a deeper understanding of investigators and judges are needed.

2. Cases of spreading hatred based on ethnicity, religion, race and intergroup (SARA).

Accordingto a merdeka.com report in Mangadil (2016: 124) stated that the wrong facebook status of a student with the initials IRF on March

16, 2010 sparked the anger of the Balinese people, who are predominantly Hindu. because when the majority of Balinese people held the Nyepi ritual, he instead wrote a status that triggered the conflict. The status immediately drew angry comments from a number of his friends on the account, until finally the person concerned wrote the latest status expressing an apology to all Balinese, especially those who are Hindus. however, a number of groups have sprung up expressing opposition, and one of the groups is rallying support for expelling the IRF from Bali. The case regarding SARA has actually become a big dilemma for the people in the world, and problems like this are very frequent in Indonesia considering that the Indonesian people are diverse, consisting of many tribes, races, groups and even religions so as to allow tensions between these groups. words in the form of insults or defamation and can cause hatred for a person or group (SARA), and can be subject to Article 28 paragraph (2) of the ITE Law with criminal threats as explained in Article 45A paragraph (2) of the ITE Law, namely imprisonment for a maximum of six years and/or a maximum fine of one billion rupiah. Ababila generalized, this criminal threat can also ensnare a person who gives a hyperlink to a site that has content that smells of SARA or facebook statutes that are considered to contain SARA and it can also be comments on facebook that cause other groups, tribes or religions to disturb their calm. In this case, not too many parties are harmed financially/materially or economically, but the problem is the impact. Insults to beliefs or religions can cause discomfort or even unrest between religious people.

3. The Case of Spreading False Information (Hoax).

Included in the realm of cybercrime the most familiar today is the spread of fake news (hoaxes). If the spread of this hoax issue contains elements of violations as explained in the ITE Law, it can also be subject to criminal penalties. The latest case happened to one of the lecturers of Civil Servants (PNS) of the University of North Sumatra (USU). Directorate of Crimesus Subdit cybercrime North Sumatra Regional Police arrested the

suspect because one of the facebook account posts said that the 3 church bombings in Surabaya were just a diversion of the issue until it went viral and invited netizens' debate because it was suspected of containing elements of hate speech (SARA) (TribrataNews, 2018). The cyber media community has become accustomed to using all texts that tend to be hoaxes, as a result it is difficult to distinguish which information is true and which is false (Triartanto, 2015: 33). Although not seen directly, the consequences caused by the spread of this hoax information, many parties are harmed in various sectors, ranging from political, economic, and social issues. At least until now the spread of hoax news in Indonesia is increasingly thriving and rampant as if there is no control. Therefore, every Facebook user is expected to understand deeply about the laws in the ITE Law related to the criminal realm of cybercrime and the spread of hoax news.

6. Cybercrime Countermeasures

The main activities of cybercrime are attacks on content, computer systems and communication systems belonging to other people or common in cyberspace. The phenomenon of cybercrime must be watched out for because this crime is relatively different from other crimes in general. Cybercrime can be carried out without knowing territorial boundaries and does not require a personal relationship between the perpetrator and the victim of the crime. Here's how to deal with it:

1. Securing the system

   The real purpose of a security system means preventing the destruction of parts in the system because they are entered by unwanted users. Integrated system security is needed to minimize the possibility of such destruction. Creating a security system should be integrated measures across its subsystems, using the goal of narrowing or even closing the existence of adverse unauthorized action loopholes. Personal security can be done starting from the system installation stage until finally going to the stage of physical security and data security. Securing system attacks through the network can also be done by securing FTP, SMTP, Telnet and Web Server security.

2. Global countermeasures

The Organization for Economic Cooperation and Development (OECD) has produced guidelines for policymakers working with computer-related crime, which in 1986 the OECD published its report entitled Computer-Related Crime: Analysis of legal Policy. Based on the OECD, some important steps that every country must take in countering cybercrime are:

- Modernizing the national criminal law and its procedural law.
- Improve the national computer network security system according to international standards.
- Increase the understanding and expertise of law enforcement officials on efforts to prevent, investigate and prosecute cybercrime-related cases.
- Increase the awareness of the people of the country regarding the issue of cybercrime and the importance of preventing such crimes from occurring.
- Increase cooperation between countries, both bilateral, regional and multilateral, in efforts to deal with cybercrime.

CONCLUSIONS

The increasing number of internet users has caused various cybercrime crimes in many countries, including Indonesia. Broadly speaking, cybercrime perpetrators , whether intentional or not, will be entangled with Law number 11 of 2008 concerning information and electronic transactions. There are at least 3 threats brought by the ITE Law in Indonesia that have the potential to attack cybercrime perpetrators by utilizing social media, namely the threat of violating the decency of Article 27 paragraph (1), insults and /or defamation of Article 27 paragraph (3), and the spread of hatred based on ethnicity, religion, race and intergroup (SARA) Article 28 paragraph (two). Criminal threats for violators of the article as described in Article 45 paragraph (1), Article 45 paragraph (3) and Article 45 Aayat (2) of the ITE Law are imprisonment for a maximum of six years and /or a maximum fine of one billion rupiah.

Every internet and social media user is obliged to make efforts that can be done to prevent cybercrime , including by protecting the computer from viruses, maintaining privacy, securing e-mail, protecting Id / Account, making data backups, and always up to date with news. Take into account the ethics of good communication as well as the selection of information. There are several factors that must be considered in selecting news sources from the internet, namely relevance, accuracy, reputation authority, objectivity, currency, coverage, and strong evidence.

REFFERENCES

Abidin, D. Z. (2015). Crime in Information and Communication Technology. Scientific Journal of Media Processor, 10(2), 1–8. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

Aldawood, H., & Skinner, G. (2019). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018, October 2019, 62–68. https://doi.org/10.1109/TALE.2018.8615162

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2). https://doi.org/10.3390/bdcc5020023

Arwana, Y. C. (2022). Victims of Cyber Crimes in Indonesia : A Criminology and Victimology Perspective. December 2021, 181–200. https://doi.org/10.15294/lsr.v2i2.53754

Banjarnahor, A. C., & Priyana, P. (2022). Cybercrime Juridical Analysis of Kredivo's Handling of Phishing Cases. HERMENEUTICS : Journal of Legal Sciences, 6(1). https://doi.org/10.33603/hermeneutika.v6i1.6754

Flowers, D. (2019). The politics of criminal law against countermeasures. Journal of Indonesian Legislation, Vol.16(No. 1), 1–15. https://e-jurnal.peraturan.go.id/index.php/jli/article/view/456

Chang, L. Y. C. (2017). Comparative Criminology in Asia. Comparative Criminology in Asia, July 2017. https://doi.org/10.1007/978-3-319-54942-2

Fitriani, Y., & Pakpahan, R. (2020). Analysis of Social Media Abuse for the Spread of Cybercrime in Cyberspace. Horizons : Journal of the Humanities, 20(1), 2579–3314. http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala

Garba, A., Maheyzah Binti Sirat, Siti Hajar, & Ibrahim Bukar Dauda. (2020). Cyber Security Awareness Among University Students: A Case Study. Science Proceedings Series, 2(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320

Garba, A., Musa, M. A., & Othman, S. H. (2020). A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative. Int. J. Emerg. Technol, 11(July), 41–49.

Gunawan, H. (2020). Cyber Crime In Jinayah Jurisprudence Perspective. El-Qanuniiy Journal: Journal of the Sciences of Social And Social Institutions, 6(1), 96–110. https://doi.org/10.24952/el-qanuniy.v6i1.2473

Hartati, S., Karyono, H., & Karno Sabowo, H. (2022). Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia. International Journal of Educational Research & Social Sciences, 3(1), 425–436. https://doi.org/10.51601/ijersc.v3i1.290

Faith, N., Susanto, A., & Inggi, R. (2020). Analysis of Digital Forensic Development in Cybercrime Investigation in Indonesia (Systematic Review). Journal of Telecommunications and Computers, 9(3), 186. https://doi.org/10.22441/incomtech.v9i3.7210

Karina Cornelia, Jubaedah, N. P. E. W. (2021). The Process and performance of Combating Cyber Crimes In Indonesia. The Process and Performance of Combating Cyber Crimes In Indonesia, 8(1), 1–20. https://doi.org/10.15408/sjsbs.v8i4.21795

Koto, I. (2021). IJRS: International Journal Reglement & Society Cyber Crime According to… Cyber Crime According to the ITE Law. August, 103–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. IEEE Access, 8, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Mahardika Jhon ; Jhon, R. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. Indonesian Journal of Criminal Law Studies, 3(1), 25–34. https://doi.org/10.15294/ijcls.v3i1.16945

Mahdi, I., & Dalle, J. (2021). Examining the Adequacy of Constitutional Laws Related to Cybercrimes in Indonesia. International Journal of Cyber Criminology, 15(1), 122–132. https://doi.org/10.5281/zenodo.4766537

Miranda, M. J. A. (2018). Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. International Management Review, 14(2), 5–10. https://help.salesforce.com/articleView?id=admin_loginrestrict.htm&type=5,

Peker, Y. K., Ray, L., Silva, S. Da, & Gibson, N. (2016). Raising cybersecurity awareness among college students. Journal of The Colloquium for Information System Security Education (CISSE), September, 1–17.

Rifauddin, M., & Halida, A. N. (2018). Beware of Cybercrime and Hoax Information on Facebook Social Media. Khizanah Al-Hikmah : Journal of Library, Information, and Archival Science, 6(2), 98. https://doi.org/10.24252/kah.v6i2a2

Septanto, H. (2018). The Influence of Hoaxes and Hate Speech a Cyber Crime with Simple Technology in People's Social Life. Journal of Science and Technology, 5(2), 157–162.

Siahaan, A. P. U. (2018). Cybercrime Violations and Jurisdictional Forces in Indonesia. Journal of Engineering and Informatics, 5(1), 6–9.

Sulisrudatin, N. (2014). Analysis of Cybercrime Cases in the Banking Sector in the Form of Credit Card Data Theft Mode. Scientific Journal of Aerospace Law, 9(1), 26–39. https://doi.org/10.35968/jh.v9i1.296