SOSHUM
Jurnal Sosial dan Humaniora
[Journal of Social Sciences and Humanities]
Volume 8, Number 2, 2018
p-ISSN. 2088-2262 e-ISSN. 2580-5622
ojs.pnb.ac.id/index.php/SOSHUM/

Law Implementation of Cybercrime in Indonesia

I Nyoman Sukayasa[1] & Wayan Suryathi[2]✉

[12] Department of Business Administration, Politeknik Negeri Bali
✉ Bukit Jimbaran, Kuta Selatan, Badung – Bali, Indonesia, PO BOX 1064 Tuban
E-mail: wsuryathi2011@yahoo.co.id

Article Info

History Articles
Received:
February 2018
Accepted:
July 2018
Published:
July 2018

Keywords:
cybercrime pattern, implementation of legal basis, law enforcement of cybercrime case

ABSTRACT

Cybercrime is a criminal act that is prohibited by every country in the world. Cybercrime cases have occurred and gave negative impacts on Indonesian computer users. This study explains that common cybercrime patterns consist of cracking, carding, twitter hijacking, cybersquatting, use of someone else's account, identity theft or data leakage, data forgery, online probing and port scanning, sabotage and extortion, against government and against property, and virus attacks. This research uses qualitative descriptive approach, with statute approach analysis technique and empirical juridical method. Data collection was done through document studies on articles and case reports in Indonesia. The patterns and forms of cybercrime in Indonesia are stated in articles 27 to 35 of Law Number 11/2008. The criminal act against cybercrime applies chapter 45 to article 52 of Law Number 11/2008. The application of the legal basis of cybercrime cases that has occurred in Indonesia is subject to articles 263, 362, 363, 378, 282 paragraph 1 of the Criminal Code, articles 29 and 56 UURI Number 44/2008, article 8 and 303 of Law Number 7/1974.

INTRODUCTION

Information technology such as the internet is very important in human life today. Many human activities are done in connection with the Internet. The development of the Internet can be analogous as coins, on the one hand, change from the inefficient world to become more fast-paced and instant, on the other side of the internet also raises a new problem of sophisticated crime called cybercrime. Information technology can bring positive and negative impacts on people's lives. The positive impact of internet information technology, among others, can be used as a communication media (chatting), can be used as a media to search information (Google and Youtube), can be used as data exchange media (email, newsgroup, world wide web), can be used to ease the activity of transacting and doing business in trading. While the negative impacts of information technology are all kinds of criminal activity on the Internet such as can be misused or contain the risks of its security, especially security when the transfer of data on the network. Data passing through a computer network can be tapped, stolen, or tampered with. The stolen and misused data are then used for personal gain, can even be used for criminal acts such as pornographic media, information media of cruelty, fraud, gambling, and theft of money. Therefore, cybercrime can be called a new phenomenon in the world of crime and criminals are always one step ahead compared to law enforcers' actions. Information from Raymond (2016) social network users are generally unaware of the nature of friendship containing crime programs through the links they receive, for example, brought to a dangerous site.

Based on http://tekno.liputan 6.com described in Akamai Report, State of The Internet Report, Symantec Internet Security Threat Report, Indonesia including the top five users of social networking in the world, ranked 6th as internet users and become the most cyber-attack country (38%) of the ten countries in the world, where attacks appear to be the largest in the country itself. According to Setya (2015) Deputy Director of Special Economic Crimes Police Criminal Investigation that in the last three years recorded 36.6 million cybercrime attacks occurred in Indonesia. According to Ramli (2004) with the issuance of Law Number 11/2008, the government has actually tried to overcome the problems of cybercrime or cybercrime, with the law is expected to minimize the number of crimes in this category. Based on this, the determination of the legal basis for the violations that occurred is governed by the Intellectual Property Rights Act Number 19 of 2002 and the ITE Law (Information and Electronic Transactions) Number 11 of 2008 discussed below.

The formulation of the issues discussed in this paper is as follows.
a) How the patterns and forms of cybercrime occur in Indonesia.
b) What are the legal grounds applied in Indonesia relating to cybercrime?

While the general purpose of this research is listed as follows.
a. Pattern and form of cases of cybercrime that occurred in Indonesia.
b. The legal basis applied in Indonesia related to cybercrime.

Internet in terms of writing can be reviewed from two aspects, namely: a. internet (with an initial lowercase "i") is a computer network where the computer can connect and communicate. Internet network (with initial uppercase "I") is a collection of networks consisting of millions of computers that can communicate with each other with the same communication rules. While the

term telematics is originated from the French term "Telematique" to show the meeting of the communication network system with information technology, while the information technology is limited to the development of information processing devices technology. The definition of cybercrime according to Fernando (2016) is a crime using computer technology as a major crime tool. It can also be said to be unlawful acts that utilize computer technology based on the sophistication of the development of Internet technology. Li (2017) explains the concept of his research in China that cybercrime is a computer crime which targeting computer information system.

According to Clough (2015), in general, there are three classes of cybercrime, namely: a. Crime in which a computer or computer network. Infringement act where the computer as a target, such as the use of malware (malicious software), conduct denial of service attacks, and so forth, b. Crime in which the use of a computer is the incidental aspect of the crime commission. According to Fawn Ngo (2017), there are 4 types of cybercrime: a. Cyberstalking (this type of crime is committed to disturb or harass a person resembling terror). b. Carding (a crime committed to stealing credit card numbers belonging to others and used in trade transactions on the internet). c. Hacking and Cracker (referring to someone who has a great interest in learning the computer system in detail and performing acts of destruction on the internet, d) Cybersquatting and or typo squatting (a crime by registering another company's domain name and then attempting to sell it to that company with a more expensive price or a crime by creating a lookalike domain).

According to Fernando (2016), cybercrime can be distinguished into three categories: cyberpiracy, cybertrespass, and cyber vandalism. Cyberpiracy deals with the use of computer technology to reprint software or information, and distribute information or software through a computer network Cybertrespass deals with the use of computer technology to improve access to an organization's or an individual's computer system, as well as a password-protected website cyber vandalism deals with the use of computer technology to create programs that interfere with the process of electronic information transmission, which can escalate into destructing data in computer and computer network, so as to be called cybercrime. According to Lizamainardianty (2012) differentiates cybercrime through two approaches, namely based on the motive and by type of activity. Based on the motives, cybercrime is classified as pure crime, grey crime, individual crime, criminal acts of property/copyright and acts of attacking the government. Based on the type of activity, cybercrime is classified as Unauthorized Access to Computer System and Service, Illegal Contents, Data Forgery, cyber espionage, cyber sabotage and extortion, an offense against intellectual property, infringements of privacy, cracking, carding.

METHODS

The object of this research is the application of legal basis of cybercrime case. The source of this research data comes from secondary data. According to Pabundu (2006: 57), data can be obtained from books, reports, decree. This type of research is reviewed from data collection including secondary research which according to Erwan (2011: 36) is research by reviewing and conducting library study based on data compiled by another party. According to Hamid (2011: 3) legal research including the type of research without samples, data analysis used with the approach of normative law and statute approach and empirical juridical methods. The empirical

juridical method according to Abdulkadir (2004) is a field study that examines the implementation and implementation of laws and regulations in the field.

RESULTS AND DISCUSSION

Cybercrime phenomena force cyber and digital technology users to form rules and legislation that protect the interests of every individual who uses the network. Patterns and forms of cybercrime in Indonesia are outlined in accordance with Law Number 11 the Year 2008 in Chapter VII of Article 27 to Article 37. The implementation of the rules is as follows.

Article 27: (1) Any person who intentionally and without the right to distribute and/or transmit and/or make accessible electronic information and/or electronic documents that have content that violates morality.
(2) Every person intentionally and without the right to distribute and/or transmit and/or make accessible electronic information and/or electronic documents that have a gambling charge.
(3) Any person intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents with defamatory and/or defamatory content.
(4) Every person intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that have a blackmail and/or threatening charge.

Article 28: (1) Every person intentionally and without the right to disseminate false and misleading news resulting in consumer losses in Electronic Transactions.
(2) Every person intentionally and without the right to disseminate information aimed at generating a sense of hatred or hostility towards certain individuals and/or community groups based on ethnicity, religion, race, and intergroup (*Suku, Ras, Agama dan antar Golongan, or SARA*).

Article 29: Every person intentionally and without the right to send Electronic Information and/or Electronic Documents containing threats of violence or intimidating personally addressed.

Article 30: (1) Any person who knowingly and without rights or illegally access the Computer and/or the Electronic System of another Person in any way.
(2) Any person who knowingly and without right or unlawfully access the Computer and/or Electronic System in any way for the purpose of obtaining Electronic Information and/or Electronic Documents.
(3) Any person who knowingly and without right or unlawfully access the Computer and/or Electronic System in any way by violating, breaching, surpassing, or breaking the security system.

Article 31: (1) Any person who intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a particular computer and/or electronic system of others.

(2) Any person who intentionally and without right or unlawfully intercepts the transmission of Electronic Information and / or Electronic Documents that are not public to, from, and within a particular Computer and / or Electronic System belonging to another person, whether or not causing any change or cause of any change, disappearance, and / or termination of any Electronic Information and / or Electronic Document being transmitted.

(3) Except for interception as referred to in paragraph (1) and paragraph (2), interception is done in the framework of law enforcement on request of police, prosecutor, and/or other law enforcement institution stipulated by law.

(4) Further provisions on interception procedures as referred to in paragraph (3) shall be regulated by a Government Regulation.

Article 32: (1) Any person who knowingly and unlawfully or unlawfully in any way alters, adds, subtracts, transmits, damages, removes, transfers, conceals any Electronic Information and/or Electronic Document belonging to any other person or public property.

(2) Any person who knowingly or unlawfully or unlawfully in any way transfer or transfer Electronic Information and/or Electronic Documents to an unauthorized Electronic System another person.

(3) In respect of the acts referred to in paragraph (1) which result in the release of Electronic Information and/or Electronic Documents with confidential nature becomes accessible to the public with the integrity of data that is not as it should be.

Article 33: Every person who intentionally and without right or unlawfully take any action which resulted in disruption of Electronic System and/or causes Electronic System to be not working properly.

Article 34: (1) Every person intentionally and unlawfully or unlawfully produces, sells, commits to using, imports, distributes, provides, or possesses:

a. Computer hardware or software designed or specifically developed to facilitate acts as referred to in Articles 27 to 33;
b. Password via Computer, Access Code, or similar matters intended for the Electronic System to become accessible for the purpose of facilitating the acts referred to in Articles 27 to 33.

(2) The action referred to in paragraph (1) is not a criminal offense if intended to conduct research activities, testing Electronic System, for the protection of Electronic System itself legally and not against the law.

Article 35: Every person intentionally and unlawfully or unlawfully manipulates, creates, alters, omissions, destruction of Electronic Information and/or Electronic Documents in order to make Electronic Information and/or Electronic Documents considered as authentic data.

Article 36: Every person who intentionally and without rights or against the law commits an act as referred to in Article 27 to Article 34 which causes harm to others.

Article 37: Every person intentionally engages in prohibited acts as referred to in Article 27 to Article 36 outside the Indonesian territory of the Electronic System in the juridical territory of Indonesia.

Based on the pattern and form of violation of the illicit action in Chapter VII, also set the rules of criminal action in Chapter XI Act Number 11/2008. The implementation is as follows.

Article 45: (1) Any person who meets the elements as referred to in Article 27 paragraph (1), paragraph (2), paragraph (3), or paragraph (4) shall be punished with imprisonment for a maximum of 6 (six) years and / a fine of at most Rp1,000,000,000.00 (one billion rupiahs).
(2) Any person fulfilling the element as referred to in Article 28 paragraph (1) or paragraph (2) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiahs).
(3) Anyone who meets the elements as referred to in Article 29 shall be liable to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp2,000,000,000.00 (two billion rupiahs).

Article 46: (1) Any person who meets the elements referred to in Article 30 paragraph (1) shall be liable to a maximum imprisonment of 6 (six) years and/or a fine of not more than Rp600,000,000.00 (six hundred million rupiahs).
(2) Any person fulfilling the element as referred to in Article 30 paragraph (2) shall be punished with imprisonment of not more than 7 (seven) years and/or a fine of not more than Rp700,000,000.00 (seven hundred million rupiahs).
(3) Any person who fulfills the element as referred to in Article 30 paragraph (3) shall be punished with imprisonment for a maximum of 8 (eight) years and/or a maximum fine of Rp800,000,000.00 (eight hundred million rupiahs).

Article 47: Any person who fulfills the elements referred to in Article 31 paragraph (1) or paragraph (2) shall be subject to imprisonment of not more than 10 (ten) years and/or a maximum fine of Rp800,000,000.00 (eight hundred million rupiahs).

Article 48: (1) Any person who fulfills the element as referred to in Article 32 paragraph (1) shall be punished with imprisonment for a maximum of 8 (eight) years and/or a fine of not more than Rp2,000,000,000.00 (two billion rupiahs).
(2) Any person fulfilling the element as referred to in Article 32 paragraph (2) shall be punished with imprisonment of not more than 9 (nine) years and/or a maximum fine of Rp3,000,000,000.00 (three billion rupiahs).
(3) Any person who fulfills the element as referred to in Article 32 paragraph (3) shall be punished with imprisonment for a maximum of 10 (ten) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiahs).

Article 49: Any person who meets the elements as referred to in Article 33 shall be liable to a maximum of 10 (ten) years imprisonment and/or a maximum fine of Rp10,000,000,000.00 (ten billion rupiahs).

Article 50: Every person who fulfills the element as referred to in Article 34 paragraph (1) shall be liable to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp10,000,000,000.00 (ten billion rupiahs).

Article 51: (1) Any person who meets the elements as referred to in Article 35 shall be liable to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiahs).

(2) Any person fulfilling the element as referred to in Article 36 shall be liable to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiahs).

Article 52: (1) In the case of criminal acts as referred to in Article 27 paragraph (1) concerning decency or sexual exploitation of a child shall be subject to a one-third reduction of the principal penalty.

(2) In the event that the acts as referred to in Article 30 through Article 37 are directed to Electronic Computers and/or Electronic System and/or Electronic Document owned by the Government and/or used for public services are criminally charged with one or more third.

(3) In the case of acts as referred to in Article 30 to Article 37 is directed to Electronic Computers and / or Electronic System and/or Electronic Documents owned by the Government and/or strategic bodies including but not limited to defense institutions, central banks, banks, finance, international agencies, aviation authorities are threatened with maximum criminal penalty of each Article plus two thirds.

(4) In the case of criminal acts as referred to in Articles 27 to 37, the corporation shall be punished with a principal penalty plus two thirds.

Based on the results of data collection from HTTP: // deluthus.blogspot.com there are also some legal bases that have been implemented as the settlement of real cases happening in Indonesia, as described below.

a. Cases of embezzlement of Rp372.100.000,00 in private banks by the computer by two students based on news of *Suara Pembaruan* Newspaper edition of January 10, 1991. The settlement is based on the law of article 362 of the Criminal Code or Article 378 of the Criminal Code.
b. The video case of two artists *Luna Maya* and *Cut Tari* whose personal attack mode by RJ, subject to the rules of article 29 UURI Number 44 of 2008 on pornography, article 56 on the length of punishment and article 282 article 1 KUHP about a fine of at least Rp250 million to 6 billion.
c. The case of hackers, carding, and cracker in Bandung. The settlement under the law of article 406 of the Criminal Code, article 378 of the Criminal Code on fraud, article 363 on theft and article 263 on falsification of identity.
d. Online gambling case in Semarang, December of 2006 in risking European football battle. The settlement is based on the legal basis of article 303 on gambling and Law 7/1974 article 8 on the threat of a sentence of more than 5 years.

CONCLUSION

Based on the results of research and discussion above it can be described in the conclusion in this study. Cybercrime is a criminal act that is prohibited by each country, because it gives negative impact such as the occurrence of cracking, carding, piracy of twitter, cybersquatting, the use of other accounts, identity theft or leakage data, forgery of data, online gambling probing and port scanning, sabotage and extortion, against government and against property, and virus spread. The application of the cybercrime legal basis includes articles 263, 362, 363, 378, 282 verses 1 of the Criminal Code, articles 29 and 56 of UURI Number .44 of 2008, articles 8 and 303 of Law Number 7/1974, articles 27 to 35, 45 of Law Number 11 of 2008.

Seeing the existence of many cybercrime cases in Indonesia, it is necessary to overcome with several policies such as modernizing the material criminal law and criminal procedure law and developing computer preventive and security measures, urging the authorities to improve supervision of non-penal policies such as training for officials and law enforcement officers on cybercrime.

REFERENCES

Abdulkadir. (2004). *Hukum dan penelitian hukum*. Bandung: PT Citra Aditya Bakti

Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press

Erwan Agus Purwanto. (2011). *Metode penelitian kuantitatif*. Yogyakarta: Gava Media

Fawn Ngo, K.J Aishankar and Jose R. Agustina. (2017). Cyber criminologi. *International Volume* 11 (2), Juli-Desember 2017

Fernando, Dian. (2016). Contoh kasus cybercrime dan penyelesaiannya. Retrieved from https://eduonemedia.wordpress.com, February 16.

Lizamardianty. (2012), Contoh kasus cybercrime yang pernah terjadi, modus dan penyelesainnya. Retrieved from http://Lizamardianty Wordpress.com, March 08)

Ramli, Ahmad M. (2004). *Cyberlaw dan haki dalam sistem hukum indonesia*. Bandung: Refika Aditama

Raymond, Goh. Jumlah pengguna internet indonesia capai 881 juta. http://tekno.liputan6.com. Retrieved on 26 April 2016

Undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, Jakarta.