INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 5, Issue - 11, Nov– 2019
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.497
Received Date: 19/11/2019 Acceptance Date: 30/11/2019 Publication Date: 30/11/2019

Eradication of Cybercrime in Indonesia based on Cyber Laws

[1] Masdin Saragih, [2] Elpina
[1, 2] Faculty of Law, Universitas Simalungun, Indonesia

Abstract: *Cybercrime is a crime that is very detrimental to others. This crime is hidden. The intermediary media for this crime is the computer network. Without a computer network, there is no cybercrime. Cybercrime works through data theft and data misuse. Data that has been stolen will be used as a tool to blackmail someone or steal money. Cyber laws are needed to anticipate these crimes. In law, crime is regulated by several supporting articles. Eradication of cybercrime can be reduced by applying the law to cybercriminals. The result is that every time there is a cybercrime, the cyberlaw will act for decision making in resolving the criminal case. Many attempts were made to eradicate cybercrime, but what happened was that the perpetrators often escaped observation. Eradication not only applies punishment to the perpetrators of the crime, but technology is needed to trace the perpetrators in cyberspace. A tracking system is required to find the location of the perpetrators of these crimes so they can be arrested and processed legally. By applying techniques like this, cybercrime will be reduced.*

Keywords: *cybercrime, cyberlaw, cyberspace, eradication.*

1. INTRODUCTION:

The increasingly connected world makes many vulnerable parties victims of cybercrime. The development of technology is directly proportional to the emerging cyber threat. Criminal groups use new technology to identify targets and launch attacks on various industrial scales. Cybercrime does not only break into banks. Crimes committed with the help of technology intermediaries (computer networks) can be said to be a cybercrime [1]. Defamation and hate speech are forms of cybercrime cases. It can be seen that the police mostly handle cases like this. It can be judged that on the scale of cybercrimes that occur, there are other forms of cybercrime in addition to defamation and have more impact on society [2].

Cybercrime needs to be taken firmly. Perpetrators of cybercrime need to be given severe sanctions. It is done so that the deterrent commits the crime. Many parties are harmed by cybercrime. One of the cybercrime acts is spreading false information [3]. False information can trigger clashes between people and even between groups and countries. The message that is spread in cyberspace can not be proven its authenticity because the technology of the digital world can mimic digital data perfectly. It is different from ancient times where the recorded copy is very different from the original. Today, the copy is the same as the original [4].

The eradication of cybercrime needs to be done. Crimes like this must be watched out so as not to harm many people. Some efforts must be made, such as site blocking, digital forensics, and network security improvement. Eradication can be done if all relevant parties can work together to look for perpetrators of cybercrime jointly. Cybercrime perpetrators do not have to show themselves in acting. It is very different from someone who wants to rob a bank, must come to the bank, and make physical contact with bank officers. This crime is, of course, easy to be paralyzed, and this is very different from the activities carried out by cybercrime perpetrators [5]. Cybercrime perpetrators work secretly. Only mistakes can reveal this crime. Eradication based on law and technology is expected to cripple cyber crime activities.

2. THEORIES:

2.1 Cybercrime

Cybercrime is a term that refers to criminal activity with a computer or computer network being a tool, target, or place of crime. These include online crime, online auction fraud, check fraud, credit card, confidence fraud, identity fraud, child pornography, violence, and others. Although cybercrime generally refers to criminal activity with a computer or computer network as its main element, this term is also used for traditional crime activities where a computer or computer network is used to facilitate or allow the crime to occur.

Examples of cybercrime where computers are tools are spamming and crimes against copyright and intellectual property. Cases of cybercrime in which computers are targeted are illegal access (deceptive access control), malware, and DoS attacks. Examples of cybercrime where the network as a place is identity fraud. Traditional crime with computers is child pornography and online gambling. Some of the fraudulent sites under the guise of online gambling are included in a website which is a crime site in cyberspace which is being monitored by the police with violations of article 303 of the Criminal Code concerning gambling and article 378 of the Criminal Code concerning fraud under the guise of online games by forcing the website owner to close the website through the DDOS method of the website in question. Likewise, identity fraud in online games. By simply filling in a fake identity address, the online game is confused with a fake identity address. If this continues to happen, then the online game will be a loss or bankruptcy and even the possibility of bankruptcy or bankruptcy.

2.2 Cyber Law

Cyber Law is a legal aspect whose scope encompasses all issues relating to individuals or legal subjects who use and utilize internet technology that begins when online starts and enters the cyber or cyber world. Cyber Law itself is a term derived from Cyberspace Law [6]. The development of Cyber Law in Indonesia alone cannot be said to be advanced. Unequal internet users throughout Indonesia cause it. In contrast to the United States, which uses the internet to facilitate all aspects of their lives. Therefore, the development of cyberspace law in the United States has also been tremendously advanced [7].

The fundamental foundation in the juridical aspect that regulates internet traffic as a particular law, where there are main components that cover the problems that exist in the virtual world, such as:

- Legal jurisdiction and related aspects. This component analyzes and determines the validity of applicable laws and practices in the virtual world.
- The basis of the use of the internet as a means of freedom of opinion is related to the responsibilities of the parties delivering, aspects of accountability, responsibility in providing online services and internet service providers (internet providers), as well as legal responsibilities for educational service providers through the internet network.
- Aspects of intellectual property rights where there are aspects of patents, secret trademarks applied, and apply in the world.
- The aspect of confidentiality guaranteed by the provisions of the law in force in each jurisdiction of the country of origin of the party who uses or utilizes cyberspace as part of the system or service mechanism that they do.
- Legal aspects that guarantee the security of every user of the internet.
- Legal provisions which formulate ownership aspects on the internet as part of the investment value that can be calculated in accordance with financial or accounting principles.
- Legal aspects that provide legalization of the internet as part of trade or business ventures.

Based on the factors above, then we will be able to assess to justify the extent of the development of the laws governing the internet systems and mechanisms in Indonesia. Although it cannot be said to be evenly distributed, the development of the internet in Indonesia has experienced a very high acceleration, and has the number of customers or parties who use the internet network has continued to increase since the mid-90s.

One indicator to see how internet law applications are needed in Indonesia is with many companies becoming providers for internet service users in Indonesia. Companies that provide service providers in Indonesia are aware or not are parties who play a significant role in advancing the development of Cyber Law in Indonesia where the functions they perform, such as:

- Internet customer account application agreement;
- Agreement on making commercial home page designs;
- Reseller agreement for data placement on the internet server;
- Offers to sell retail products via the internet;
- Provision of information that is updated daily by commercial home pages;
- Providing opinions or polling online via the internet.

The functions above are factors and actions that can be classified as actions related to the application of law about cyber in Indonesia. Therefore it is useful in the next development; every service provider or internet user can be guaranteed. So the law about the internet needs to be developed and reviewed as a law that has its own discipline in Indonesia.

3. RESULT AND DISCUSSION:

3.1 Cybercrime Prevention

Crime activities with computers or computer networks or commonly referred to as cybercrime. Many patterns and ways that can be done by the perpetrators of cybercrime and many ways also prevent cybercrime from happening to us. To protect yourself and also to prevent unwanted losses on the business.

The following are some things for preventing cybercrime:

- Always use Up to Date security software. One of the easiest ways to prevent hackers and cybercrime from hacking and stealing information is to maintain the security of each PC and also software on the PC to keep it up-to-date. Usually in a PC or gadget device often releases periodic device updates. It is intended to close the security holes that exist on the device. To prevent cybercrime from stealing sensitive information, then follow the recommendations for updates provided by the device vendor.
- Create a strong password. Do the account passwords use strong passwords? If not quickly change accounts to prevent cybercrime. If possible enter a mixture of lowercase, uppercase and numeric numbers on each account to strengthen the password.
- Install antivirus software. Antivirus software is used to prevent, detect and eliminate various malware such as: viruses, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dielers, and spyware. For someone who has a business, it is definitely very important to invest in an antivirus software for use on various company computers. Antivirus software must be available especially for computers that store sensitive information belonging to customers.
- Make a data backup. Computer users should have a backup of their personal documents, whether it is in the form of photos, music, or others. It is intended that the data can still be saved if at any time there is data theft or there is an error in the computer system.
- Security consultant to determine how safe the business is. Another way you can do to prevent cybercrime for business is to have an IT security consultant to evaluate how safe the business is. These security specialists can carry out security checks for. These security specialists can carry out security checks to tell where the security weaknesses are. Because hackers are always constantly looking for ways to get access to personal data and steal sensitive information from various businesses.
- Use security features for the Website. Another thing that can be used is to use SSL / HTTPs for website security from information exchange. (Also Read: SSL/HTTPS FREE)

3.2 Personal Efforts to Eradicate Cybercrime

Cybercrime actions that do not take a few victims will ultimately encourage many parties to try to overcome them both in terms of regulators such as the government, and other stakeholders such as the private sector, as well as the community itself. Some things that can encourage the prevention of cybercrime are as follows:

- Educate User. Educating the public IT practitioners to be more vigilant against cybercrime.
- Use Hacker Perspective. The importance of using a hacker perspective so that we know the actions that need to be taken to secure the system.
- Strengthen system security and obey applicable rules. You can use third party security to strengthen the system and follow the laws of the government so that system security can also be more secure.

3.2 Government Efforts to Eradicate Cybercrime

Complex cybercrime problems must be dealt with in a systematic and structured manner that involves the role of the government in administering the country as well as regulators who are entitled to state security. Indonesia, which ranks the top in cybercrime in the world, has made various efforts to prevent cybercrime, including:

- ITE Law. As a legal approach to cybersecurity, Indonesia already has an Information and Electronic Transaction Law to prevent cybercrime from occurring. However, this law must still be re-evaluated because many articles are less relevant.
- Blocking. This effort was made by the government to protect Indonesian children or adolescents from being exposed to harmful content such as porn sites and hoax news. The government can use screening systems such as Positive Trust, DNS Nawala, and the Nusantara Whitelist System, which provide recommendations for positive sites.
- Cyberspace and State Code. In 2017, the government formed a body to prevent the occurrence of cybercrime that has eight functions. Among them are related to identification, detection, protection, and prevention of e-commerce, coding, cyber diplomacy, cybercrime management centers, recovery of vulnerability, incident, and cyber attacks.
- HR Focus. The government organizes various programs that focus on improving the trained human resources such as information change agent training and organizing technology-based competitions.

4. CONCLUSION:

Cyber crime cannot be denied because there is a rapid technological development, and it is followed by the lifestyle of the people who have now shifted to a dependency in using technology in their daily lives. Therefore, taking preventive action against cyber crime as early as possible can minimize the problem of cyber crime attacks, so that security in technology can be reached by all circles and levels of society. The eradication of cybercrime can be done in collaboration with the community with the government to minimize the possibility of cybercrime. By coordinating between parties, cybercrime crime rates can be reduced.

REFERENCES:

1. A. P. U. Siahaan, "Pelanggaran Cybercrime dan Kekuatan Yuridiksi di Indonesia," *J. Tek. dan Inform.*, vol. 5, no. 1, pp. 6–9, 2018.
2. M. Saragih, H. Aspan, and A. P. U. Siahaan, "Violations of Cybercrime and the Strength of Jurisdiction in Indonesia," *Int. J. Humanit. Soc. Stud.*, vol. 5, no. 12, pp. 209–214, 2017.
3. V. C. E. Tarigan *et al.*, "CYBERCRIME CASE ON SOCIAL MEDIA IN INDONESIA," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 7, pp. 783–788, 2018.
4. M. D. T. P. Nasution, Y. Rossanty, A. P. U. Siahaan, and S. Aryza, "The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 6, pp. 1583–1592, 2018.
5. S. Ullah, M. Amir, M. Khan, H. Asmat, and K. Habib, "Pakistan and cyber crimes: Problems and preventions," in *2015 First International Conference on Anti-Cybercrime (ICACC)*, 2015, pp. 1–6.
6. A. M. Zain, N. E. Saberi, F. Jaafar, F. H. A. Fauzi, W. N. R. W. Ramli, and F. A. Lugiman, "Social Media and Cyber Crime in Malaysia," in *International Colloquium of Art and Design Education Research (i-CADER 2014)*, Singapore: Springer Singapore, 2015, pp. 515–524.
7. P. Brown, K. Christensen, and D. Schuster, "An Investigation of Trust in a Cyber Security Tool," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 60, no. 1, pp. 1454–1458, Sep. 2016.