Legal Protection for Cyber Crime Victims on Victimological Perspective

Angkasa[1*]
[1]Faculty of Law, Jenderal Soedirman University, Purwokerto 53122, Indonesia

Abstract. All this time, a second victimization in a criminal justice system is considered to be an identical problem for the victims of crime. Thus, it is fair if the whole assessment is more oriented to the legal protection for the victims, especially the child victims in the crime of fornication and coition. However, when viewed from different sides, the source of error is not always absolute to the perpetrator but also because of the victim precipitation. This study examines the victim precipitation and its prevention with the aim to understand the degree of victim precipitation and the proportional prevention, that is not only from the aspect of the perpetrators but also from the aspect of the child victim and the community who have the potential to become victims. This research was conducted in the jurisdiction of Purwokerto City and Banyumas Regency, using sociological juridical research and qualitative research approach. The results show that there are several forms of victim precipitation in the crime of sexual fornication and coition to the child. Meanwhile, the prevention must be conducted comprehensively, either from the internal of the victim, or externally from various related parties.

1 Introduction and Literature Review

Based on the data supported by The Ministry of Communication and Information the Republic of Indonesia, in 2018 Indonesia is the sixth country on internet usage by its population after China, US, India, Brazil and Japan. In Indonesia's population, 130 million people are recorded as the internet users on 2018. It shows a significant surge in a number compared to 2014. According to the e-Marketer research institute, the nation's net population reached 83.7 million people in 2014 [1]. The data shows more than half or about 51.5 percent of the total population in Indonesia actively use internet technology. Based on data from the Indonesian Internet Service Providers Association (APJII) 51.5 percent of Indonesian citizen

* Corresponding author: drangkasa_64@yahoo.com

that use the internet, 65 percent are in Java, and the lowest is used by Maluku and Papua at around 2.5 percent [2].

Regarding the huge number of internet users, the opportunities for being a cybercrime and becoming a victim of cybercrime are also increasing. Moreover, based on data showing the behavior of Indonesian internet users' 70 percent of internet users access the internet from mobile devices or mobile gadgets while the rest use the internet statist or home network [2]. The internet can also be activated for 24 hours in one day, it means that the range to conduct a cybercrime as well as being a victim becomes limitless. Since the internet has a very wide network, the perpetrators and their victims can be located geographically according to the reachable internet network. The distance between the perpetrator and victim is not a problem anymore, meaning that the victim and the perpetrator can be separated thousands of kilometers away, crossing the pond, even land to the ocean.

On the victim's perspective, cybercrime can be mentioned as a type of victimization which victim's scope is not only national but also global through unlimited place and time, there is no national boundary, no jurisdiction, and leads to create more victims anywhere and anytime

According to the results of Verisign's research, a company that provides intelligence services of cyberspace based in California, USA states that Indonesia is a country which gain the first ranks in terms of cybercrime and finally displaced the State of Ukraine [2]. There was another data about the source of cybercrime, based on data in 2013 the Indonesian Ministry of Communication and Informatics got the second rank after China [2].

2 Objective of the Study

This research seeks to have a study about three things including the analysis of the loss and / or suffering of cybercrime victims, acknowledging the causes of cybercrime victimization from victimology perspective and observing the legal protection of cybercrime victims on victimology perspective. This is conforming the **Zvonimir-Paul Separovic** perspective about the following three purposes.

> "1. to analyze the manifold aspects of the victim's problem; 2. to explain the causes for victimization; 3. to develop a system of measures for reducing human suffering [3]".

3 Methodology

The research method used in this study is Victimological Juridical. It is intended to implement the legal studies that is conducted to the objects within the victimology scope. The data obtained is secondary data in the form of legal norms and research results. The analysis is carried out based on the victimology theory.

4 Discussion

4.1 The Kinds of Cyber Crime and The Losses and / or The Victims suffering

Based on cybercrime limitations, the type of cybercrime can be multiform. Regarding the target/object, it can be occurred to individuals and society, as well as the government. A Cybercrime with the individual victims, can be a fraud through online purchasing, including carding actions for victimization carried out by a person or group of people by using another person's credit card that is carried out by violating of the law with the support of digital documents, computers and internet

Cybercrime with corporate as the victim occurs toward corporations in the banking sector or various fields of public services. In the online-based transportation business there are corporations that have become victims of their business partners in this case several online motorcycle taxi drivers who commit fraud by carrying out fictitious orders or transactions which are popularly known as "tuyul".

Cybercrime with community as the victim, for instance like in the form of hoaxes and provocative reporting aimed to create anxiety and hostility in society. this group, can be formed by terrorist groups or any kind of groups formed for political purposes. In the era of governor elections, presidential election, this type of cybercrime would significantly increase.

Cybercrime with government as the victims, can be done by attacking the web or government sites. Based on the statistical data from the domain.go.id response incident owned by the Indonesian government in this case APTIKA's General Director in 2016, there was an increase of attacks on web defacement from 42 percent to 95 percent. This shows that almost the entire web is attacked [2].

Every single criminal act, or crime or in victimology perspective, I call it victimization, causing the loss and / or misery. As well as cybercrime. The cost of losses due to cybercrime (cybercrime) in the entire world was reported to have reached US $ 600 billion last year or around 0.8% of global GDP [4]. The results of the Norton Cyber security Insight Report study toward 17 countries, the average user of the cyber world loses closely US $ 358 per person or around a total of US $ 150 billion due to cybercrime per year [5].

The data owned by The City of London Police shows that there is a report on the occurrence of cybercrime, with a total of loss up to £ 28 million between October 2017 and March 2018. This report also states that there are 4,796 reports, social media and e-mail accounts hacking that cause losses with the total reached £ 11 million [6].

Psychological detriment for cybercrime can be experienced by a victim such as harassment, flaming, denigration, impersonation, outing, cyber stalking. Harassment is done by sending the disturbing messages by using e-mail, SMS, or text messages on social media continuously. Flaming can be expressed by sending a text messages which the content is full of anger and frontal. Denigration is an act against a person by spreading his ugliness on

internet, especially social media, which intends to damage the reputation of someone's dignity.

Impersonation is a form of imitation of others and do any kind of bad activities through media supported by the internet, which is aimed to bring down the credibility or good name of the person that is being imitated. For instance, hacking the other people's accounts and doing bad activities through hacked accounts. Cyber stalking is manifested by interfering and also intensely defaming someone's credibility which causes victim's intimidation [7].

4.2 The Factors of Cyber Crime Victimization in Victimology Perspective

The cause of crime or victimization in the victimology perspective is a theory known as Victim Precipitation (VP). This VP theory was originally born from Criminology. **Victim precipitation** is a criminology theory that how victim's interaction with an offender may contribute to the crime being committed. The theory is most commonly associated with crimes like homicide, rape, assault, and robbery [8]. Like all criminology theories, victim precipitation relates to how and why crime happens. While most theories focus on the acts and intentions of the offender, victim precipitation seeks to understand the interaction between the victim and the offender.

In victimization of cybercrime Victim Precipitation can be applied, it can be seen in a visible case from the reporting data read through **Indonesian Police Cyber Crime** Facebook Page. In the case mentioned above, the Victim Precipitation theory is appropriate. Victims seem to have had quite intense interactions with the perpetrators so that they arrive at the stage of fully trusting and expecting something in return from the perpetrator, who somehow is the same person as the photo sent.

Another theory that can explain the case of victimization above is that lifestyle or lifestyle-exposure theory, is a victimization theory which recognizes that not everyone has the same lifestyle and that some people try to expose their life and this kind of people tend to have more risks. Victims in this case are people who use social media Facebook.

As a comparison of research that was conducted by suggesting the results indicate that neither individual nor situational characteristics consistently impacted the likelihood of being victimized in cyberspace. Self-control was significantly related to only two of the seven types of cybercrime victimizations and although five of the coefficients in the routine activity models were significant, all but one of these significant effects were in the opposite direction to that expected from the theory [9].

4.3. Legal Protection For Cyber Crime Victim As a System To Reduce Victim's Suffering

The third goal of victimology is to create a system to reduce victim's suffering. The system that has been built through national positive law to reduce the suffering of victims of cybercrime is upon several legal norms. A Legal norm which regulates the rights for victims

can be mentioned as a form of legal protection. Because the substance of a legal protection is about to grant the rights of every legal subject based on the prevailing laws and regulations.

The Laws that contain legal protection aspect for victims of cybercrime are found in the Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) which have been amended by the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 1 Year 2008 concerning Information and Electronic Transactions. In the victimology perspective, the form of legal protection is concretely manifested by restitution [10] or compensation [11].

There are several formulations of UUITE and cybercrime that can be classified as material law. The observation result about a legal protection, especially in the existing of victimology perspective toward punishment for victimization of cybercrime are not visible at all. The provisions of criminal sanctions are still embracing to the sanction model contained in general criminal law in the term of Criminal Code.

This should have been regretted because in one of the articles about prohibited actions it was mentioned in the provisions of the ITE Law Article 36. On this article, there are words that cause the loss of another person, and the form of loss can include material or financial losses and / or moral or psychological loss. By only giving a criminal sanction in the form of imprisonment and / or fines seems that the victims do not feel any adequate and fair legal protection.

Regarding a number of other laws and regulations, there are some which have mentioned restitution and / or compensation. Those laws are Law Number 21 of 2007 concerning the Eradication of Crimes in the Trafficking of Persons there is a restitution arrangement for victims (Article 48).

Some regulations in Indonesian positive law that have demonstrated the existence of real legal protection for victims in victimization include: Law No. 31 of 2014 concerning Amendments to Law No. 13 of 2006 concerning Protection of Witnesses and Victims, Law No. 23 of 2004 concerning the Elimination of Domestic Violence, Law Number 21 of 2007 concerning the Eradication of Crimes against Human Trafficking, Law No. 11 of 2012 concerning Child Criminal Justice System, Government Regulation (PP) Number 2 of 2002 concerning Procedures for Giving Protection to Witnesses and Victims of Serious Human Rights Violations and Government Regulation Number 44 of 2008 concerning Provision of Compensation, Restitution and Assistance to Witnesses and Victims.

5 Conclusion

Based on the discussion above, can be concluded that the legal protection in the victimology perspective for victims of cybercrime has not yet sufficient. According to the fact that the rights have not been included in concrete and real rights for victims due to minimize the suffering of victims such as restitution or compensation. Besides, the opportunity to do restorative justice seems impossible.

References

1. https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media, accessed on 9 August 2018.
2. https://www.researchgate.net/publication/322537415_TREND_CYBER_CRIME_DAN_TEKNOLOGI_INFORMASI_DI_INDONESIA , accessed on 9 August 2018.
3. Z. Separovic, *Victimology Studies of Victims* ("Zagreb" Samobor-Novaki by Pravni Fakultet, Zagreb, 1985)
4. http://kabar24.bisnis.com/read/20180223/19/742348/kejahatan-siber-di-seluruh-dunia-sebabkan-kerugian-global-us600-miliar, accessed on 9 August 2018
5. http://mastel.id/ke rugian-akibat-cyber-crime/ accessed on 8 August 2018
6. https://www.actionfraud.police.uk/news/28-million-lost-by-cyber-crime-victims-jul18
7. http://www.psikoma.com/dampak-perkembangan-psikologis-dari-korban-cyberbullying/ accessed on 9 August 2018
8. https://study.com/academy/lesson/victim-precipitation-definition-theory.html, accessed on 9 August 2018
9. F.T. Ngo, R. Paternoster, International Journal of Cyber Criminology **5(1)**, 773 (2011)
10. J. Harding, *Victims and Offenders Needs and Responsibilities* (Bedford Square Pres/N.C.V.O., London, 1982)
11. R. Ellias, *Community Control, Criminal Justice and Victim Services*, in From Crime Policy to Victim Policy Reorienting the Justice System. Ezzat Abel. Fattah (ed.) (Macmillan Press Ltd., London, 1996)