International Journal of Social Science and Human Research

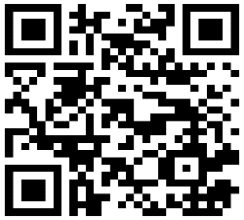
ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 07 Issue 04 April 2024

DOI: 10.47191/ijsshr/v7-i04-56, Impact factor- 7.876

Page No: 2440-2443

Criminal Law Policy as An Attempt to Overcome Cyberstalking Crimes in Indonesia



Sylvia Christie Permatasari[1], Pujiyono[2]

[1]Student Master of Law Diponegoro University, Indonesia

[2]Lecturer Master of Law Diponegoro University, Indonesia

ABSTRACT: Cybercrime is defined as a crime committed using information and communication technology, such as computers or the internet. Cyberstalking is one type of cybercrime, and there is no legislation in place to protect people from stalking in Indonesia. The existing regulations are ineffective in addressing this issue since they continue to employ inadequate articles. As a result, it is proposed that legislation be created immediately that particularly controls protection against stalker actions in cyberspace, to provide security and a sense of security to the community.

KEYWORDS: Policy; Criminal Law; Crime; Cyberstallking

I. INTRODUCTION

These days, we have entered the modern period, commonly referred to as the digitization era. This is evidenced by the existence of evolution, development, and advancement in science and technology. Furthermore, technological developments cannot be separated from the existence of the Internet, which has had a significant impact on society, both positively and negatively. One of the beneficial effects of technological developments on people's lives is the presence of social media, which aims to support activities that meet people's needs. Meanwhile, the negative impact of technical innovations on people's lives includes the misuse of technology, resulting in a type of online-based crime.

Online-based crimes certainly cause losses for their victims. These victims are mostly women, and one of these internet crimes is cyberstalking. It is now inextricably linked to social media. Obviously, before accessing social media, users have to fill out their personal information for registration purposes in order to utilize the social media later. Thus, users will undoubtedly believe that their personal information is safe, but this is not the case when irresponsible people abuse social media and commit crimes such as stalking.

Cyberstalking can include false accusations, threats, identity theft, or equipment destruction, sexual solicitation of minors, and other forms of recurrent abusive behavior. Moreover, cyberstalking refers to surreptitious behaviors in which someone obtains personal information about another person using the internet, typically a social networking site.[1]

While using social media, the perpetrator, who is obsessed with the victim, typically creates multiple fake accounts, each with a deliberately disguised identity, and each account is purposefully set up to follow someone in order to monitor the victim's daily life and routine, causing the victim to feel disturbed. They may feel nervous and uncomfortable about the stalking they are experiencing, even if the stalker does not share anything containing harassment, insults or defamation, blackmail and/or threats, or even terror. As a result, stalkers cannot face legal consequences because it is unclear whether such conduct is a legal violation.

Based on the explanation above, this study analyzes legal issues in the form of Criminal Law Policy as an Attempt to Overcome Cyberstalking Crimes, as well as obstacles to overcoming cyberstalking crimes.

II. RESEARCH METHODS

This type of research is legal research. Legal research is defined as "research that examines and analyzes legal norms and the operation of law in society, using specific methods, systematics, and thinking, in-depth examination, problem-solving, and objectives".[2] This study took two approaches: statutory and case-based. The data used in this research is secondary data, which includes both primary and secondary materials. Moreover, the primary sources include legislative rules and Court Decision No. 12/PID/2017/PT.DPS. Secondary materials on cyberstalking include literature, books, and scientific publications. The datagathering approach for this study employs qualitative analysis to investigate and respond to the legal challenges addressed, which are criminal law policies addressing cyberstalking crimes in Indonesia.

III. DISCUSSION

A. Criminal Law Policy in Attempts to Overcome Cyberstalking Crimes in Indonesia

Cyberstalking is a type of cybercrime that involves repeatedly using information technology connected to the internet and includes features such as threats of hate speech, coercion, or intimidation that can induce fear and anxiety. In addition, victims will be followed and pursued online. Their privacy is violated, and their every move is monitored; this is a sort of harassment that can disrupt the victim's life and leave them feeling fearful and threatened. Therefore, the act of cyberstalking as an act that is contrary to the law requires that some form of law enforcement be carried out against it.

The policy governing the direction of punishment for stalking criminals cannot be isolated from the function of law enforcement, which includes police, prosecutors, judges, and advocates. Furthermore, every law enforcement officer plays an important part in Indonesia's criminal justice system. In essence, the judicial system consists of authority, inquiry, prosecutorial authority, adjudicatory authority, decision-making authority, and the ability to carry out a judgment or execution.[12]

The criminal law policy regarding cyberstalking crimes is now found in the Criminal Code and Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions. There are also several articles dealing with forms of cyberstalking that can be utilized to avoid stalking, including Article 351 paragraph 1 of the Criminal Code, which is used by the Public Prosecutor to indict the perpetrator Article 29 jo is another legislation that law enforcement officers may employ to prosecute criminals. Article 45 Paragraph (3) of Law No. 19 of 2016 regulating ITE allows law enforcement to apply this article if stalkers' activities produce electronic information documents as a result of their stalking. Article 29 Jo. Article 45 Paragraph (3) of Law No. 19 of 2016 on ITE states that: "Every person intentionally and without authorization sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at personally."

In addition, another provision that can be used is Article 27 paragraph (3) of the ITE Law, which states that "Every person intentionally and without right distributes, transmits, or makes accessible electronic information and/or electronic documents containing insulting and/or defamatory content good name." This article can be used if the results of the stalker's actions are made into content that is disseminated and contains offensive content that can cause the victim to feel insulted or tarnish their good name, or if it contains other elements such as decency, insults, threats, and blackmail, then the perpetrator of stalking can be held accountable under Indonesian positive law.

At this point, if the stalker carries out the case by photographing or documenting the victim being stalked, this act may be subject to personal data protection laws. However, if the content of the portrait, taking pictures, or documenting the results of stalking is used to gain economic advantage, it can be charged under Article 115 jo. Article 12 Law no. 28 of 2014 concerning Copyright, with the condition that the resulting content is used for commercial advertising purposes without the consent of the person whose photo is used.

Legislative policy is the process of creating legislative regulations or implementing formulations by lawmakers, specifically the government and the DPR. Moreover, the legislative policy stage is strategic because it produces a legal regulation that serves as a guide for the other phases of the criminal law policy process. This legislative product, known as a law, is at the formulation level of legal policy and has an abstract position, including in the form of regulations/laws, implying that this legislation will have significance if it is applied in reality. As a result, in order for this law to be fulfilled in society, bodies capable of carrying it out are required, which in law/political science are known as executive departments and judicial departments.[3]

On the other hand, the formation of laws specifically related to the criminal act of stalking or the formulation of articles relating to the criminal act of stalking is one of the penal policies. Comprehensive and explicit formulation of articles specifically related to criminal acts of stalking or cyberstalking is considered necessary to avoid incidents or situations such as the emergence of double interpretations by law enforcement and to ensure legal certainty and the enforcement of justice for the rights of cyberstalking victims can be fulfilled.

Aside from that, the formulation or formation, which is regarded as particularly important, is one of the consequences of a country that adheres to the principle of the rule of law, as emphasized in Article 1 paragraph (3) of the Republic of Indonesia's 1945 Constitution, which requires all actions taken by the government as the holder of power to be based on applicable laws or regulations. This is in line with Frederich Julius Stahl's conception of the rule of law (rechtsstaat), which consists of four essential elements, which are:[4]

1. Human rights protection
2. Separation of powers to guarantee these rights

---

[1] Barda Nawawi Arief, "*Masalah Penegakan Hukum dan Penanggulangan Kejahatan*", (Bandung: Citra Aditya Bhakti, 2001), p. [2] .

[3] Mochamad Sahid, "*Kebijakan Formulasi Sanksi Pidana Dalam Penanggulangan Tindak Pidana Siber Berdasarkan UndangUndang Informasi Dan Transaksi Elektronik*", Jurnal Aktualita 1.1 (2018), p. 210.

[4] Muhammad Fadli, "*Pembentukan Undang-Undang Yang Mengikuti Perkembangan Masyarakat*", Jurnal Legislasi Indonesia 15.1 (2018), p. 51.

3. Statutory regulation-based government
4. Administrative justice in disputes

Criminal law policy against cybercrime is crucial since updating criminal law policy in the context of law enforcement against cybercrime or cyberstalking can incorporate international conventions and cybercrime law enforcement arrangements in other countries, resulting in the synchronization of law enforcement applications[56]. Thus, in the era of the information technology revolution, criminal law policy in resolving cyberstalking offenses remains based on the Criminal Code and Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, as well as cross-border crimes. Conventions can be applied in International conventions.

B. Obstacles in Attempt to Overcoming Cyberstalking Crimes in Indonesia

Criminal law is a part of public law that governs a person's behaviors, identifies prohibited actions, and imposes sanctions for those violations. Criminals who commit cybercrime use one or more accounts to carry out their activities. Ideally, an account should be a container or means of providing accurate electronic information about the personal identification of the account's user or owner. For example, someone sets up an email account that may be used to send and receive messages. Then, when they want to create a social media account, they are requested to register their e-mail address and carry out several data verification steps until they can finally use the social media account.

Several illegal activities may occur behind an anonymous social network account. In Indonesia, numerous social media accounts are created irresponsibly and used to attack other people's personalities, whether they are public figures or ordinary citizens. These accounts can also be used to criticize other people's good names, becoming an expression of hate speech. As a result, cases involving anonymous accounts are becoming more widespread, such as the emergence of social media accounts known to the public as "gossip accounts" and "haters accounts.".

The account owner/manager actively seeks news by stalking others, even secretly following them, taking photos or videos, and distributing them to the public. These accounts are classified as anonymous since the identity of the owner and the person responsible for the account are unknown. Article 35 of the ITE Law contains the regulation regarding anonymous accounts, which states: "Every person intentionally and without right or against the law manipulates, creates, changes, deletes, or destroys Electronic Information and/or Electronic Documents with the intent that the Electronic Information and/or Electronic Documents are considered as if they were authentic data." With sanctions as regulated in Article 51 of the ITE Law:
"Every person who meets the elements as intended in Article 35 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine IDR 12,000,000,000.00 (twelve billion rupiah)."

Therefore, regulations prohibiting the creation of anonymous accounts exist in the Indonesian legal system; nevertheless, imposing legal responsibility on anonymous account creators is still difficult to enforce. This is due to the lack of a credible internet user data collection system, which allows anyone to create a social media account using a fake identity, and the electronic system of social media applications does not currently implement a reliable data verification system to ensure the authenticity of user identities.

In addition, criminal law requires the fulfillment of the element "everyone" or "whoever" in the formulation of the offense. Thus, the use of anonymous accounts will make it challenging to prove the "everyone" element because the person in question is difficult to detect and it is difficult to carry out further legal proceedings.

For example, an Indonesian artist, Tamara Bleszinky, experienced cyberstalking and harassment by a criminal claiming to be a fan of hers. According to Decision Number 12/PID/2017/PT.DPS, the perpetrator was indicted under Article 351 paragraph (1) of the Criminal Code, which specifies that "mistreatment is punishable by a maximum imprisonment of (2) two years and eight months or a maximum fine of three hundred rupiahs." Moreover, it is important to highlight that in this decision, the perpetrator is only punished for the criminal act of abuse; cyberstalking conduct is not a crime. This is possible since Indonesia has no specific rules in place to address explicit cyberstalking crimes.

If people understand the explanation of the cyberstalking prevention policy above, it is obvious that the regulation of crimes related to this criminal act is still widespread; however, the regulation of the crime of cyberstalking is not explicitly or comprehensively regulated, implying that some form of legal interpretation is required to understand it. This can also lead to multiple interpretations (Multitafsir) of the article relating to the illegal crime of cyberstalking; hence it is important to understand the Article when it is intended to be employed.[7]

The author believes that if cyberstalking without any illegal content (violation of decency, insult/defamation, blackmail and/or threats, and threats of violence or intimidation) is criminalized, it should be considered:

---

[5] Azizurrahman, "*Pembaharuan Kebijakan Penegakan Hukum Pidana di Era Cyber*", Journal Masalah Hukum 41.1 (2012),p.
[6] .

[7] Barda Nawawi Arief, "*Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*", (Semarang: Universitas Diponegoro, 2000), p. 34.

1. If such actions are to be criminalized, then the type of offense that is appropriate is a complaint offense. The complaint offense permits prosecution based on the aggrieved party's allegations. This occurs because the disturbance generated by this action is more directed towards disturbing someone's personality and does not directly affect the public interest. Thus, it is necessary to limit the extent to which the state can intervene in the prosecution of this offense.
2. The law enforcement process will function if it is supported by an effective system, which includes adequate law enforcement structures and institutions. The state must provide a mechanism for tracing abusers who utilize anonymous accounts so that they can be arrested and criminal law can be filed against them.
3. The principle of minimum evidence must still be followed. To declare someone guilty, at least two pieces of evidence plus a judge's conviction are required. In circumstances like these, the evidence that can be produced will be dominated by digital evidence such as screenshots of messages exchanged and social media activity history, therefore evidence regulations are required for this criminal offense. Criminalization cannot be implemented haphazardly. Furthermore the principle that must remain a guide is the principle of legality (nullum delictum, nulla poena sie praevia lege poenali) put forward by von Feurbach. This expression contains the meaning that "no act can be punished except according to criminal legislation that existed before the act was committed". The principle of legality is the most crucial in criminal law, particularly when determining criminality.

IV. CONCLUSION

Regarding the description provided in the previous section, it is possible to conclude that the criminal law policy governing cyberstalking crimes is currently contained in the Criminal Code, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Law Number 28 of 2014 concerning Copyright. However, the majority of these rules and regulations remain considered ineffective due to the lack of precise restrictions governing the criminal act of cyberstalking. The formation of laws specifically related to the criminal act of stalking or the formulation of articles relating to the criminal act of stalking is one of the penal policies. Furthermore, comprehensive and explicit formulation of articles specifically related to criminal acts of stalking or cyberstalking is deemed necessary in order to avoid incidents or situations such as the emergence of double interpretations by law enforcement and to ensure legal certainty and the enforcement of justice for the rights of cyberstalking victims can be fulfilled.

In attempts to overcome cyberstalking crimes in Indonesia, there is an obstacle in that the regulation of cyberstalking crimes is still widespread, but the regulations for cyberstalking crimes are not regulated explicitly or comprehensively, which means that some form of legal interpretation is required to understand it (p.). This can also give rise to multiple interpretations (Multitafsir) in articles relating to the crime of cyberstalking, hence it is critical to be careful to comprehend these articles before using them in policies to overcome cyberstalking crimes.

REFERENCES

1) Rahel Octora, 2019, “Problematika Pengaturan Cyberstalking (Penguntitan Di Dunia Maya) Dengan Menggunakan Annonymous Account Pada Sosial Media”, Jurnal DIalogia Iuridica, p. 77-96.
2) Barda Nawawi Arief, 2000, “Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara”, Semarang: Diponegoro University.
3) _____, 2001, “Masalah Penegakan Hukum dan Penanggulangan Kejahatan”, (Bandung: Citra Aditya Bhakti). P. 1264.
4) Salim and Erlies, 2013, “Penerapan Teori Hukum Pada Penelitian Tesis dan Disertasi”, Jakarta: Raja Grafindo Persada, p. 1-356.
5) Azizurrahman, 2012, “Pembaharuan Kebijakan Penegakan Hukum Pidana Di Era Cyber”, Jurnal Masalah Hukum 41.1, p. 298-305.
6) Muhammad Fadli, 2018, “Pembentukan Undang-Undang Yang Mengikuti Perkembangan Masyarakat”, Jurnal Legislasi Indonesia 15.1, p. 49-58.
7) Mochamad Sahid, 2018, “Kebijakan Formulasi Sanksi Pidana Dalam Penanggulangan Tindak Pidana Siber Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik”, Jurnal Aktualita 1.1. p. 205-221