Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website

Sukirno[1,*], Edy Lisdiyono[2] and Sri Mulyani[2]

[1]*Universitas Nahdlatul Ulama Purwokerto, Banyumas, and Universitas 17 Agustus 1945, Semarang City, Pawiyatan Luhur Street, Bendan Dhuwur, Semarang City, Indonesia*

[2]*Universitas 17 Agustus 1945, Semarang City, Indonesia; Pawiyatan Luhur Street, Bendan Dhuwur, Semarang City, Indonesia*

Abstract: The existence of legal positivism that prioritizes legal certainty is expected to resolve various cybercrime criminal cases. One of them happened in the case of the Mojokerto City Government site hacking. The case has troubled the community, especially the city government of Mojokerto. The research method uses normative juridical research with a legal approach, concepts and collects primary legal materials in hacking rules and information technology in cybercrime crime. The study results found that the existence of legal positivism in the crime of cybercrime positions the law as statutory regulation and law as an order containing sanctions. In-Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions contains orders and prohibited actions. The actions taken by the suspect are deemed unfair if there are no sanctions or punishments because, according to legal positivism, justice that is legality (statutory regulation) is justice that prioritizes legal certainty. The law in force in article 46 paragraph 3 of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions must be imposed on the suspect in the Mojokerto City government website hacking case.

Keywords: Legal Positivism, Law Enforcement, Cybercrime, Hacking, Mojokerto City.

INTRODUCTION

The development of science and technology, which is relatively rapid nowadays, has become a daily reality and even is a community demand that cannot be negotiated. The main goal of the development of science and technology is to change the future of human life for the better, more accessible, cheaper, faster, and safer. The development of science and technology, especially information technology such as the internet, dramatically supports everyone to achieve their life goals in a short time, both legally and illegally, by justifying any means because they want to gain profits by "cutting the compass." The harmful impact of the development of the "Maya World" is inevitable in the life of modern society today and in the future.

The advancement of all-digital information technology has brought people to the revolutionary world of business (digital revolution era) because it is easier, cheaper, more practical, and more dynamic to communicate and obtain information. On the other hand, the development of information technology also raises a dark, vulnerable side to an alarming stage with concerns over the development of criminal acts in information technology related to "cybercrime" or major crimes (Arief, Kebijakan Kriminalisasi dan Masalah Jurisdiksi Tindak Pidana Mayantara, 2001).

Cybercrime generally refers to criminal activity with computers or computer networks as the main element, and this term is also used for traditional criminal activities where computers or computer networks are used to facilitate or allow the crime to occur. One type of e-commerce crime is online fraud. Online fraud, referred to in e-commerce, is online fraud that uses the internet for business and commerce purposes to no longer rely on a natural, conventional company base (Sitompul, 2001).

Cybercrime is a means for a crime to occur, which is also known as cybercrime; for some people, this cybercrime is only in the scope of the fraud, hackers, spreading fake news, or spreading anything that contains pornographic elements, but not That alone can be said to be cybercrime, many other forms of crime are still foreign which are also included in the Cybercrime category.

Most people worldwide think that fraud or the spread of false information via the internet can only be found in email, but by technological developments that are increasingly out of control, and the virtual world is increasingly widespread. Which is getting out of control every day, and the virtual world is expanding. So that

*Address correspondence to this author at the Universitas Nahdlatul Ulama Purwokerto, Banyumas, and Universitas 17 Agustus 1945, Semarang City, Pawiyatan Luhur Street, Bendan Dhuwur, Semarang City, Indonesia;
Tel: (+62) 8999911717; E-mail: sukirno2594@yahoo.com

E-ISSN: 1929-4409/21

fraud through the internet is limited to email and on websites, blogs, and others. Internet scams on blogs usually contain advertisements and lead to low-quality or malicious sites containing fraudulent or fake news.

Formerly internet fraud under the telecommunication laws. However, telecommunications law is included in the legal framework of telematics because of telematics' development that moves so fast following the changes in the world today. These aspects continue to adjust substantially in practice, while the rules of the game are not significant. The role of government in every country has become so important that governments worldwide are struggling to deal with telematics problems, especially the so-called "unwanted information" available to citizens on the internet (cyberspace). Therefore. Formulating an accommodative framework for the problems faced is imperative (Maskun, 2013).

In cases raised regarding hacking (break-ins) are legal events that need to be in the spotlight. That in this case, the perpetrators committed a legal act by breaking into the Mojokerto city government website and spreading fake news by presenting the ugliness of the Mojokerto city government. This hacking has been carried out since March 2017. At that time, the suspect Zulham, who was hurt by the fact that his furniture was not fully paid for by the Mojokerto City Government, asked Candra to hack a website belonging to the Mojokerto City Government. Then replace the appearance of the website page with writing allegations of corruption by many officials. This action is very detrimental to the community, especially the City Government of Mojokerto.

As for the same research that has been done before, including:

First, Antoni's research with the title cybercrime in online viewing explains that as a reasonable effort to overcome crimes in society, including cybercrime, the penal tool appears to be a method that can be used by applying crimes to perpetrators of criminal acts categorized as cybercrime. With the integration of penal and non-penal facilities and minimizing the possibility of various weaknesses in overcoming cybercrime problems, especially in SIMAK online, what is expected can be realized (Antoni, 2017).

Second, Bonanda Japatani Siregar's research with the title of cybercrime problems and regulation through internet activities in the 2018 simultaneous regional election saradi case explains that several factors influence cybercrime law enforcement, namely: the legal factor itself, law enforcement factors, cultural factors, community factors. And political factors. As for the obstacles found in the enforcement process of the cybercrime law, namely in the attempt of cybercrime errors against SARA's criminal act in the 2018 simultaneous regional elections of law enforcers who carried out analogies or parables and equations (Siregar, 2018).

Third, Kyung-shick Choi and Claire Seungeun Lee's research with the title the present and future of cybercrime, cyberterrorism, and cybersecurity explains that cyber criminology combines knowledge from criminology, psychology, sociology, computer science, and cybersecurity to provide an in-depth understanding of cybercrime. Cybercrime and cybersecurity are interconnected across multiple places, platforms, and actors. The problem of cybercrime is constantly and rapidly changing and developing, especially with the emergence of new technologies (Choi & Lee, 2018).

Fourth, Mir Mohammad Azad's research, Kazi Nafiul Mazid, and Syeda Shajia Sharmin with the title Cyber Crime Problem Areas, Legal Areas, and the Cyber Crime Law explains that cybercrime is increasing day by day, but our government is trying to protect. Every citizen should also be very careful about it. As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals will attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. There are 1.5 million cyber-attacks annually, which means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is protected while online (Azad, Mazid, & Sharmin, 2017).

Based on this case, it is interesting to be discussed in this paper in order to provide meaningful information for the development of science and law in the field of cybercrime in Indonesia, especially for law enforcement in the future; therefore, it is necessary to discuss further these issues, including how the existence of legal positivism in criminal acts cybercrime? Moreover, what are the implications of the flow of legal positivism on law enforcement in the case of the hacking of the Mojokerto city government website?

METHODS

This study using normative juridical research. The definition of normative juridical is a type of research that emphasizes more on library research, where the materials used will be obtained from laws, literature, mass media, which are related to writing materials. Besides the data obtained from the literature, the author will also describe the results of this study. After obtaining data using juridical normative, the authors describe in words in the study entitled the implications of legal positivism for law enforcement of cybercrime crime in Indonesia in the case of hacking of the Mojokerto City sites government (Simaremare & Noho, 2021).

The analytical method used refers to laws, existing regulations, looks at existing legal principles and concepts, regulations related to hacking, and information technology, and further explores the implications of legal positivism for hacking cases. Normative juridical research is needed because it is necessary to make an inventory of positive law, discover the principles and basic philosophy (dogma or doctrine) of positive law, and in-concreto legal findings feasible be applied to resolve specific legal cases (Noho, 2019).

How to collect data used in a study depends on the scope and objectives of the study. According to Ronny Hanitijo Soemitro (1990), data collection techniques consist of literature study, observation, interviews, and use of questionnaires. Based on the scope, objectives, and approach in this study, the data collection technique used is a literature study of the secondary data analyzed. The secondary data obtained will be used to support the analysis in this study

RESULTS AND DISCUSSION

The Existence Of Legal Positivism In Cybercrime

Positivism is a philosophical school that, since the early 19th century, has greatly influenced many thoughts in various fields of science regarding human life. It was influenced by the paradigm thinking of Galileo - Galilei, Isaac Newton, and Auguste Comte. The concept of positivism is a concept of truth that rejects finality in life.

In the field of law, this flow has quite influenced the development of law. Yusriadi (2018) provides an understanding of legal positivism is a school of thought that requires the release of metayuridical thoughts on the law as embraced by exponents of natural law; every legal norm must exist in its objective nature as positive norms confirmed as a concrete contractual agreement between citizens. The community (or its representatives).

Several figures influence legal positivism, including H.L.A Hart, John Austin, and Hans Kelsen. These three thinkers view legal positivism in different terms.

First, HLA Hart proposed various meanings of positivism; namely, the law is an order, analysis of legal concepts is a worthwhile effort to make, decisions can be deduced logically from existing regulations without the need to point to social goals, moral punishment cannot be enforced and defended by rational reasoning, and law as enacted, stipulated, positum, must always be separated from the law that should be created, which is desired (Imaniyati, 2003).

Second, John Austin, a significant positivist, maintained that the only law source was the supreme power in a country. Other sources are called subordinate sources. In this statement, Austin defines the source of the law as the direct maker. Because, whether it is near or far, the sovereign party or the highest legislative body is the maker of the law; and all laws flow from that same source. In Austin's view, the law is an order of sovereign political power in a country (Rahardjo, 2014).

According to Teguh Teguh Prasetyo and Abdul Halim Barkatullah (2016), the three core teachings of Hans Kelsen are three concepts:

1. Pure theory of law, in a nutshell, it can be said that Hans Kelsen wants to clean law science from non-legal elements, such as history, morals, sociology, politics, and so on. Kelsen wants to accept the law as it is, namely in the form of regulations made and recognized by the state;

2. Teachings about groundnorm. Groundnorm is a parent that gives birth to legal regulations in a specific legal system. Groundnorm is like the fuel that powers the entirely legal system and;

3. The teaching of stufenbautheory, the general rule of law, is derived from the basic norms at the top of the pyramid, and the more diverse and spread it is. The basic norm above is abstract, and the lower it gets, the more concrete it is.

This legal positivism into cybercrime crime has an impact or implication, in which cybercrime or often referred to as cybercrime, is a new form or dimension of current crime that has received wide attention in the international community. Volodymyr Golubev calls it the new form of antisocial behavior. Several other nicknames or names for cybercrime in various writings include, among others, cybercrime "cyber space In virtual space offence," a new dimension of high tech crime, a new dimension of transnational crime, and a new dimension of white-collar crime (Arief, 2007).

This cybercrime crime can be classified into two as stated in the flow of legal positivism, namely law as a rule and law as an order containing sanctions. Law as a rule, in this case, is Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions consisting of 13 chapters is a new legal regime to regulate cyberspace in Indonesia. The law puts forward at least three aspects in it, namely (Tobing, 2010):

1. In juridical aspects, the principle approach of expanding jurisdiction is used (Extra Territorial Jurisdiction) because electronic transactions have cross-territorial characteristics and cannot use conventional legal approaches;

2. In the aspect of electronic transactions, electronic transaction activities can be carried out in both public, and private spheres, and electronic transactions that are stated in electronic contracts are binding on the parties, and the parties have the authority to choose the law that applies to international electronic transactions they make;

3. In the aspect of protecting the public interest, the Government has the authority to protect the public interest from all kinds of disturbances as a result of the misuse of information and electronic transactions that disrupt public order and the national interest, and the Government determines that certain agencies must have back-up e-data and on-line data.

Law as an order that contains sanctions, namely in the aspects of prohibited actions:

1. Spread electronic information containing pornography, gambling, violence, fraud;

2. Using and or accessing computers and or electronic systems in any way without the right to obtain, change, destroying, or removing information in computers or electronic systems;

3. Using or accessing computers and or electronic systems in any way without any rights to obtain, modify, damaging, or removing information in computers or electronic systems belonging to the Government which because of their status must be kept confidential or protected;

4. Using and or accessing computers and or electronic systems in any way without rights to obtain, modify, damaging, or eliminating information in computers or electronic systems regarding national defense or international relations that may cause interference or harm to the State or relations with international legal subjects;

5. To take action that without rights, the transmission of programs, information, codes or orders, computers and or electronic systems protected by the State becomes damaged; and

6. Using and accessing computers and or electronic systems without rights or beyond their authority, both from within and outside the country, obtain information from computers and or electronic systems protected by the State.

Implications For The Hacking Case Of The Mojokerto City Government Website

This hacking has been carried out since March 2017. At that time, the suspect Zulham, who was hurt by the fact that his furniture was not fully paid for by the Mojokerto City Government, asked Candra for help to hack the Mojokerto City website Government. Then replace the appearance of the website page with writing allegations of corruption by many officials.

Hacking the second government website, www.mojokertokota.go.id, this arrest incident originated from the mayor of Mojokerto Mas'ud Yunus. He felt that the hackers recorded his name by displaying his name on the Mojokerto City Government website's index page. According to one code search, a few months ago, to be precise, on March 23, 2016, the Mojokerto City Government website page experienced a hacking incident. The hackers only displayed many words which insulted the City Government of Mojokerto. As a result of the two suspects' actions, access to the Mojokerto City Government website, which officials and the public usually access, was inaccessible for almost

three months. The city government was also disadvantaged and threatened that the employees involved would be fired.

Previously the official website of the city government was attacked by hackers. In addition to changing the appearance, hackers also displayed many data that discredited one of the Mojokerto City Regional Secretariat sections. The hacker-style appearance was discovered on March 23, 2016, at around 1:46 p.m. However, fifteen minutes later, this writing disappeared. The www.mojokertokota.go.id page cannot be accessed. It was only a day later that the Information and Communication Transportation Agency did the site repair and, at the same time, reported the case to the East Java Police.

The actions of the suspect (zulham) are prohibited by Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions; therefore, the actions of the suspect are prohibited, so the suspect must be held accountable.

Regarding the criminal responsibility of the perpetrators of hacking above, there are views on related matters. Barda Nawawi (2011) states that there are general guidelines that need to be seen before a person is sentenced to a crime:

1. Guidelines in imposing penalties (Article 55 (1);
2. Guidelines for forgiveness (not imposing a crime or action) - Article 55 (2)
3. Guidelines to be able to impose a sentence even though there is a reason to eradicate the crime (related to the principle of culpa in causa) - article 56

If using the legal positivism approach, according to Hans Kelsen, the proper punishment for the suspect (Zulham) is to impose a sentence still even though there is a reason to eradicate the crime. In Hans Kelsen's view, the law must be purified from social, economic, and political, especially moral.

This legal positivism implies a guarantee of legal certainty, and the public will quickly know what is allowed and what cannot be done. The state or government will act decisively by what has been stipulated in the law so that the task of law enforcers will be easier because they do not need to consider the values of justice and truth but merely apply statutory provisions to concrete cases.

The conception of justice in imposing a crime on the suspect of hacking the website above must be based on positive legal provisions in the form of an objectively determined law. This rule of law is positive law, and it is the object of science, not law metaphysically. This theory is called the pure of law which presents the law without defending it by calling it fair or rejecting it by calling it unfair. This theory seeks actual and possible laws, not valid laws.

This view of justice by Hans Kelsen is interpreted as legal justice. It is fair if a rule is applied in all cases where according to the content, the rule must be applied. Justice in the sense of legality is a quality that is not related to the content of positive rules but with their implementation. According to legality, the statement that an individual's action is fair or unfair means legal or illegal; that is, the action is by or not with valid legal norms to assess as part of a positive legal order. Only in the meaning of legality can justice enter into law science (Asshidiqie & Safa'at, 2012).

From Hans Kelsen's explanation above, hacking suspects must be held accountable for their actions. The Criminal liability imposed on persons, namely zulham suspects who are deemed to have committed a prohibited act as described in Article 30 paragraph 1 and paragraph 3 of Law No. 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions, states that:

> "Everyone knowingly and without right or unlawfully accesses another person's Computer or Electronic System in any way (Article 30 paragraph 1)" and "Everyone who knowingly and without right or unlawfully accesses a Computer or Electronic System in any way even by violating, breaking through, exceeding, or breaking into the security system (Article 30 paragraph 3)".

Therefore, as a result of the suspect's actions, he was charged with criminal sanctions under Article 46 paragraph 3 of Law No. 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions, states that "Every person who meets the elements referred to in Article 30 paragraph (3) shall be sentenced to imprisonment of up to 8 (eight) years or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah) " (Syamsudin, 2011).

So the implication of positivism in the above case is very influential, as H.L.A Hart stated, namely the law that is punitive, which is maintained and enforced through a process of proof and examination. These two processes have been passed by law enforcers (East Java Regional Police) by conducting investigations and investigations to be more transparent and guarantee legal certainty for the entire community.

CONCLUSIONS

Law, as a rule, namely the emergence of Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions and the law as an order containing prohibitions, namely actions that are prohibited in the law, one of which is prohibited from Using and or accessing computers and or electronic systems in any way without rights. The implication of positivism in the hacking of the site of the Mojokerto City government has contributed quite well to provide legal certainty to the community. Legal certainty that is put forward in this flow is a certainty that is legality, so fairness in this flow is justice that is legality (laws and regulations). Therefore the suspect must be given sanctions to enforce legality (statutory regulations) so that the criminal responsibility imposed on the suspect is by article 46 paragraph 3 of Law No. 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions.

REFERENCES

Antoni. (2017). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani*, *17* (2), 127-140. https://doi.org/10.19109/nurani.v17i2.1192

Arief, B. N. (2001). *Kebijakan Kriminalisasi dan Masalah Jurisdiksi Tindak Pidana Mayantara.* Semarang: Kerjasama Dirjen Postel DEPHUB dengan UNDIP.

Arief, B. N. (2007). *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia.* Jakarta: Raja Grafindo Persada.

Arief, B. N. (2011). *Tujuan dan Pedoman Pemidaan (Perspektif Pembaharuan dan Perbandingan Hukum Pidana.* Semarang: Pustaka Magister.

Asshidiqie, J., & Safa'at, M. A. (2012). *Teori Hans Kelsen Tentang Hukum.* Jakarta: Konstitusi Press.

Azad, M. M., Mazid, K. N., & Sharmin, S. S. (2017). Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law. *International Journal of New Technology and Research*, *3* (5), 1-6.

Choi, K. S., & Lee, C. S. (2018). The Present And Future Of Cybercrime, Cyberterrorism, And Cybersecurity. *International Journal of Cybersecurity Intelligence and Cybercrime*, *1* (1), 1-4.

Imaniyati, N. S. (2003). Pengaruh Paradigma Positivisme Terhadap Teori Hukum Dan Perkembangannya. *Mimbar: Jurnal Sosia da Pembangunan, XIX* (3), 268.

Maskun. (2013). *Kejahatan Siber;Cybercrime Suatu Pengantar.* Makasar: Kencana.

Noho, M. D. (2019). Politik Hukum Pengaturan Build Operate Transfer (BOT) Di Indonesia: Di Masa Lalu, Saat Ini, Dan Akan Datang. *Jurnal Hukum Media Bhakti*, *3* (1), 90. https://doi.org/10.32501/jhmb.v3i1.51

Prasetyo, T., & Barkatullah, A. H. (2016). *Filsafat, Teori, & Ilmu Hukum Pemikiran Menuju Masyarakat yang Berkeadilan dan Bermartabat*. Jakarta: RajaGrafindo Persada.

Rahardjo, S. (2014). *Ilmu Hukum.* Bandung : Citra Aditya Bakti.

Simaremare, S. P., & Noho, M. D. (2021). Disharmonized the Regulation of Biological Resources and its Ecosystem in Indonesia. *International Journal of Criminology and Sociology*, *10*, 336.

Siregar, B. J. (2018). Problem Dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Saradi Pilkada Serentak 2018. *Jurnal Penelitian Pendidikan Sosial Humaniora*, *3* (1), 330-336. https://doi.org/10.32696/jp2sh.v3i1.96

Sitompul, A. (2001). *Hukum Internet: Pengenalan Mengenai Masalah Hukum di Cyberspace.* Bandung: Citra Aditya Bakti.

Soemitro, R. H. (1990). *Metodologi Penelitian Hukum dan Jurimetri.* Jakarta: Ghalia Indonesia.

Syamsudin, A. (2011). *Tindak Pidana Khusus.* Jakarta: PT Sinar Grafika.

Tobing, R. L. (2010). *Jurnal Akhir Penelitian Hukum Tentang Efektifitas Undang – Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Jakarta: BPHN.

Yusriadi. (2018). *Positivisme Hukum.* Semarang: Fakultas Hukum Universitas Diponegoro.

Received on 03-02-2021 Accepted on 14-04-2021 Published on 26-04-2021

https://doi.org/10.6000/1929-4409.2021.10.105