IJCLS 4(2) (2019), 106-116

IJC LS

INDONESIAN JOURNAL OF CRIMINAL LAW STUDIES
http://journal.unnes.ac.id/sju/index/php/ijcls

THE PREVENTION OF NEGATIVE CONTENT BY USING VPN (VIRTUAL PRIVATE NETWORK) TOWARDS WEBSITE THAT IS BLOCKED BY THE GOVERNMENT

Wahyu Nugroho, Ismunarno, Budi Setyanto [1]
[1]*Universitas Sebelas Maret, Solo, Central Java, Indonesia*

Received July 2 2018, Accepted October 20 2019, Published November 30 2019

DOI: 10.15294/ijcls.v4i2.21762

How to cite:
Nugroho, W., Ismunarno, I., & Setyanto, B. (2019). 'The Prevention Of Negative Content By Using Vpn (Virtual Private Network) Towards Website That Is Blocked By The Government', *IJCLS (Indonesian Journal of Criminal Law Studies)* 4(1): 9-14. DOI: 10.15294/ijcls.v4i2.21762

Abstract

This research aims to know how is the prevention of negative content that is accessed by using VPN towards website that is blocked by the government through Indonesian National Police and the obstacle of its prevention. The research conducted is non-doctrinal research, which is a research to know some practical situations. This research uses primary and secondary data. Primary data is direct interviews with the Indonesian National Police and Ministry of Communication and Informatics to know blocking efforts and regulations of applications missuse. Secondary data is obtained by literature studies. The government has blocked websites with negative content based on Minister of Communication and Informatics Regulations Article 19 years of 2014 about Handling of Websites with Negative Content. Government-blocked websites can be opened with VPN applications. Indonesian National Police's step in handling the missuse of VPN applications to access negative content is with the prevention efforts. There is no device missuse regulations yet makes an obstacle to prevent represively. Ministry of Communication and Informatics begins to regulate the utilization of VPN application in the terms of licensing.

Keyword: *Negative Content Prevention; Virtual Private Network*

INTRODUCTION

On the present time people are demanded to be completely modern because the age continue to develop, so if the technology left behind, then everything will be left behind, because technology progress is a benchmark for the progress of others. Advancement in technology have developed rapidly and technological development can not be separated from the progress of information technology. It cannot be denied because today's technology of the internet has become an important part in the daily life

**Email: Wahyu.hoho29@gmail.com*
Address: Kadipiro, Kec. Banjarsari, Kota Surakarta, Jawa Tengah 57136

of all walks of life. "The internet is an interesting discovery from the beginning obtained by humans for now" (Budi Agus Riswandi, 2003: 1). The internet is the beginning of the progress of a nation, because the internet provides broad access to information beyond the territory of a country.

Various discoveries in the field of information and communication technology currently use by people by using internet through personal computers (personal computers / PCs) or other electronic media anywhere. These advances that support humanity have provided facilities and benefits for humans and their efforts to improve the welfare of humanity. Information and communication technology is currently used by individuals (individuals), corporations, governments and community groups for various human activities such as education, health, business, government, communication, entertainment, and others (Sigid Suseno, 2012: 1) .

The use of the internet can provide broad benefits for internet users in communicating and accessing information in the fields of education, government, economics, lifestyle, and entertainment. In modern times the use of the internet can be used and helps everyday life. In using internet-specific information and communication technology, everyone has a personal responsibility for their actions. This is an embodiment of the internet that has positive and negative influences. However, the use of the internet does not always have a positive impact, internet users can use the internet for negative things such as using and distributing negative content. Because of that can described that negative content is an internet site that contains negative content such as pornography, SARA (ethnic, religious, racial and intergroup discrimination), can be considered illegal, illegal drugs, drugs, gambling, radicalism, war or bulliying, violence to children and violate of Intellectual Property Rights (Hiwan Christianto, 2017: 117).

The spread of negative content is very widespread on the internet because internet users need to be free to do any activity on the internet compared to in real life. Freedom of accessing negative content makes others free of the dangers of negative.

The influence of negative content has often been reported in various media in the form of loading pornographic images, gambling, fraud, harassment, defamation and hoaxes. In addition, the use of social networking also has a negative impact, one of which is cyberbullying which usually affects children and fellow teenagers. Even the cyber crime known as cybercrime has reached hacking of important sites in the country ((https://kominfo.go.id/index.php/content/detail/3303/ Internet-Sehat-dan-Aman--INSAN-/0/internet_sehat, accessed on Sunday, July 7, 2019 at 17:30 WIB).

Community activities in using information technology and electronic transactions are regulated in Act Number 11 of 2008 concerning information and Electronic Transactions which have been amended and refined by Act Number 19 of 2016 concerning Information and Electronic Transactions. This law contains all activities regarding the official approval of the criminal. In tackling negative content, the government diverts sites that contain negative content based on Minister of Communication and Information Regulation No. 19 of 2014 concerning Handling of Negative Loaded Internet Sites. Blocking is done in two ways, namely waiting for reports and using a system such as DNS Newsletters. DNS Nawala is a free service consisting of DNS filtering which is free of charge and can be used by all internet users. This service filters or filters negative content that contains pornographic content, violence or internet freedom (https://nasional.tempo.co/read/ 701319 / this-how-is-the-ministry-communication-blocking-sites-prohibited / accessed on 29 November 2018 at 20:20 WIB).

The blocking made by the Ministry of Communication and Information is quite significant in reducing access and distribution of negative content on the internet.

Many parties find it difficult to access negative sites due to blocking by the government, but sites that are blocked by the government can still be accessed by passing the government blocking system by using a VPN (Virtual Private Network) application. VPN is a safe alternative as a tool to open government-blocked sites. VPN networks offer security and are not detected because the IP used is the Public IP of the VPN server.

The existence of a VPN as a tool that can be used as an alternative to opening government-blocked sites makes blocking done by the government useless. This method is very easy to do both from getting applications and using VPN. VPN service application is available free on ¬google play store and app store. Everyone can provide and download VPN applications because there is no licensing system for VPN application circulation. Until now there are no regulations for VPN applications or their use. Even VPNs are legal even though they are used as a facility to access negative content.

The accessibility of sites blocked by the government will make government control over surfing the internet even more ineffective. In addition, access to sites that are blocked by the government will make negative content accessible and inspire or lead to cyber or conventional crime such as rape, terrorism, narcotics abuse transactions and others. "Being aware of the psychological concepts that exist in every human being, no matter how recent the development of information technology is, it will also be the newest form and mode of the individual committing crime" (Maskun, 2013: 44).

The government and law enforcement such as the National Police of the Republic of Indonesia must pay more attention to the misuse of applications so that the government's goal of protecting the public interest from all types of disturbances as a result of misuse of Electronic Information and Electronic Transactions that disturb public order can be achieved. The police and government must make preventive efforts to prevent the spread of negative content and misuse of applications, especially VPNs, although there are no explicit statutory regulations.

Based on the background of the problem above, the author is interested in examining how the actions of the Indonesian National Police and the Government in tackling the distribution of negative content using VPN (Virtual Private Network) against sites that are blocked by the government.

Corruption in Indonesia occurs almost on all lines of government. In Indonesia, bureaucratic corruption or according to Mahmood (2005) corruption in the civil administration does not only occur in the headquarters, but has spread to the regions. Because of the widespread of corruption cases in Indonesia, many people argue that corruption in Indonesia is still considered as endemic, systemic and widespread (Lubis, 2005). Corruption like this happens in all levels of government, not only in the headquarters but also in the regions. In fact, since the enactment of regional autonomy, there has been a sharp increase in the tendency of corruption in Regional Governments (Rinaldi, Purnomo, and Damayanti, 2007).

Regional autonomy gives great authority to the regions to manage their own households. To be able to carry out optimal regional autonomy, sufficient funds are needed. Local governments must begin to look for sources in their area to be relied upon as the backbone of Regional Original Revenue (PAD). This then becomes a problem of its own when the rampant cases of corruption have an impact on regional income. The rise of corruption of course brings a detrimental impact to the state and society. The impact of corruption is very broad economic, social and poverty, the collapse of government authority, politics and democracy, the impact of law enforcement, defense and security, and even environmental issues. In addition to

inhibiting economic growth, corruption also impedes the development of a democratic governance system. Corruption fosters the tradition of carrying out acts that benefit themselves clandestinely, while closing the possibility for the weakest citizens to enjoy development and a better quality of life (Pope, 2008).

One of the most potential and vulnerable regional income to corruption is retribution. Regional retributions are regional levies as payments for services or special allowances that are specifically provided and/or given by the regional government for the benefit of private or business entity. One of the regional retribution is market retribution. This market retribution is included in the general service retribution which provides a potential contribution to the improvement of community development and welfare. For this reason, the Regional Government must properly use the results of the Market Retribution.

Surakarta City has 44 markets so the potential for market retribution is very large. Management of market retribution is carried out by the Office of Trade and Market Management. Withdrawal of market retribution, initially carried out manually. Retribution officers go to traders for payment of retribution every day. retribution withdrawal using this system raises various problems, as revealed by the Head of Trade Office (DISDAG), Solo, Subagiyo, they are the collection process takes a long time and the number of officers that must be deployed, the number of traders who delay the retribution payment up to months, transparency and lack of control which causes a high potential for leaks of retribution.

Overcoming these problems, the Surakarta local government imposed e-retribution. E-retribution is expected to increase the effectiveness of retribution withdrawals, so that the costs can be reduced and can increase transparency so as to prevent corruption. Based on this background, the problem is how the implementation of e-retribution in breaking the chain of corruption. This study aims to describe the implementation of e-levies in the traditional markets of Surakarta city as an effort to break the chain of corruption.

RESEARCH METHODS

The type of research in this study is socio-legal or empirical legal research. The research approach used by the writer is a qualitative approach. The data obtained by observation, interviews and documentation. The informants are the police officer, the tchnician and the legal department. Data analysis in this study uses data analysis from Directorate of Cyber Crime Criminal Investigation Agency of the Republic of Indonesia State Police.

FINDINGS AND DISCUSSIONS

The duties of the Directorate of Cyber Crimes are the same as the other directorates in the Criminal Investigation Body of the Republic of Indonesia State Police, namely the investigation and investigation of criminal acts. Preventive efforts were carried out by Binmas and the Patrol team. In dealing with negative content, the police know that the Ministry of Communication and Information Technology can block negative sites based on the Minister of Communications and Information Technology Regulation No. 19 of 2014 concerning Handling of Negative Loaded Sites.

Countering negative content is prevented by the Police. The task of preventing criminal acts is carried out by Babinkamtibmas and also patrols in uniform by Sabhara. In cyber patrols, it is often carried out by the directorate of cyber crime because of

limited human resources and tools. The police in tackling negative content preventively is to conduct a press realease of the results of investigations and investigations to the public in order to prevent the occurrence of criminal acts and the existence of victims of cyber crime.

Crime in the field of cyberspace grows in line with advances in information technology. The use of Communication and Electronic Transaction media is regulated in Act Number 19 of 2016 concerning Amendments to Act Number 11 of 2008 concerning Information and Electronic Transactions containing uses, prohibitions and criminal sanctions. In preventing the spread of negative content, the government can block negative loading sites based on the Regulation of the Minister of Communication and Information No. 19 of 2014 concerning Handling of Negative Sites Content.

Blocking by the government can still be opened using a VPN application. Indonesia is the largest VPN user in the world due to the number of websites blocked by the government. VPN creates a new identity that can be used to create a new identity and can be used to break the internet block in a country. In a survey made by the Global Web Index, 41 percent of internet users in Indonesia use VPNs to access sites on the internet. Content accessed using VPNs such as iTunes, Netflix, Youtube, Vimeo and negative content sites such as pornography. The big reason for using VPN is to access sites blocked by the Ministry of Communication and Information of the Republic of Indonesia with TRUST Positive. The use of VPN to break through government block is mostly done in countries like China, Indonesia and Thailand. (https://tekno.kompas.com/read/2016/03/29/08370097/Situs.Banyak.Diblokir.Indonesia.Jadi.Pengguna.VPN.Tertinggi accessed on Tuesday, June 18, 2019 at 15.50).

The National Police of the Republic of Indonesia as a state instrument that maintains the security and order of the people in charge of maintaining, protecting, and maintaining the integrity and sovereignty of the state. Based on Act Number 2 of 2002 Concerning the Indonesian National Police The function of the police is one of the functions of the state government in the field of maintaining public order and security, law enforcement, protection, protection, and service to the community and the aim is to realize domestic security which includes maintenance of public security and order, order and enforcement of the law, implementation of protection, protection and service to the community, and the maintenance of public peace by upholding human rights.

Misuse of technology and information by accessing and distributing negative content is still a difficult problem to be fully overcome. The Indonesian National Police must be more observant and effective in acting. Law enforcement must be in accordance with statutory regulations. Law enforcement of Information Technology and Electronic Transactions is carried out by the Directorate of Cyber Crime, Indonesian Criminal Investigation Agency of the Republic of Indonesia, which is the same as other directorates in handling cases, namely in the context of repressive law enforcement. The performance of the Directorate of Cyber Crimes is more focused on investigating criminal acts.

Based on interviews by the author with the Cyber Crime Directorate, VPN (Virtual Private Network) applications are not prohibited from circulating in Indonesia. The use of VPN applications is still legal to use in Indonesia. VPN is free to use even to be used as a tool to facilitate acts prohibited by law. There is no such prohibition because VPN is a neutral tool, meaning that it can be used for positive or negative actions.

The use of VPN as a tool to make accessible sites blocked by the government is not a violation of Article 27 of Act Number 19 of 2016 Regarding Information and Electronic Transactions. Where Article 27 of Act of the Information and Electronic

Transaction stipulates that any person intentionally and without the right to distribute and / or transmit and / or make access to Electronic Information and / or Electronic Documents that have contents that violate decency, gambling, insults and / or defamation, extortion and / or threats. The use of VPN to access government-blocked sites is not included in the activities of distributing and / or transmitting and / or making accessible of Electronic Information and / or Electronic Documents.

The Electronic Information and Transaction Act regulates devices that are prohibited under this Act, namely Article 34 of Act Number 19 of 2016 Regarding Electronic Information and Transactions. Article 34 (a) regulates "Every person intentionally and without rights or unlawfully produces, sells, procures for use, imports, distributes, provides, or owns Computer hardware or software designed or specifically developed to facilitate acts as referred to in Article 27 to Article 33. Article 34 (b) regulates "Any person intentionally and without right or unlawfully produces, sells, procures for use, imports, distributes, provides, or has a password through a Computer, Access Code, or similar thing intended to make the Electronic System accessible for the purpose of facilitating acts referred to in Article 27 to Article 33."

VPN is a tool that can be used to open sites that are blocked by the government and can then be carried out for acts prohibited by the Law, but are not included in Article 34 of the Electronic Information and Transaction Act because VPNs are not specifically created to facilitate regulated actions. in Article 27 to Article 33 of the Information and Electronic Transaction Act. VPNs are made with good intentions although it is true that VPNs are often misused to open sites that are blocked by the government and then become a mode of violation of law and regulations.

The absence of rules does not mean that the Indonesian National Police cannot act in a manner that is disturbing to the public. "The activity of harmonizing the relations of values that are set out in the rules or views that are settled and manifest and act as a series of translation of the final stage of value to create (as social enginering) maintain and maintain (as social control) peace of life." (Soerjono Soekanto, 1983: 2). There must be a harmonization in law enforcement with norms that develop within the community, given that the law always lags behind the development of society so that events which are actually acts against the law cannot be overcome simply because the law does not yet exist. The absence of regulations regarding misuse of applications such as VPNs is a major obstacle to repressive law enforcement.

Performing functions to maintain order and protect the public, the Indonesian National Police must be more observant in seeing the reality that exists in society. Misuse of VPN applications as a crime facility for spreading negative content is part of the Misuse of device or abuse of the device, so the act of breaking into government-blocked sites should already be seen as a cybercrime (Sigid Suseno, 2012: 99).

The government needs to support the development of Information Technology through legal infrastructure and its arrangements so that the utilization of Information Technology is carried out safely to prevent its misuse by paying attention to the religious and socio-cultural values of the Indonesian people. With the renewal of regulations governing the prohibition of a tool or its misuse, a preventive and repressive law enforcement will be created for the Indonesian National Police as the legal basis for handling the misuse of the tool. This is in accordance with the definition of law enforcement according to Liliana Tedjosaputro cited by Tasman argues that "a process to bring legal desires into reality. The desires of the law here are the thoughts of the legislature formulated in the laws and regulations, and this will also determine how law enforcement is carried out "(Kasman Tasaripa, Legal Journal of Legal Opinion, 2013: 4).

Currently the Government, namely the Ministry of Communication and

Information, is starting to pay attention to VPNs as a tool that can be used to open government-blocked sites. There is no specific policy regarding application or VPN misuse caused by several things. Based on interviews with a team of technicians at the Ministry of Communication and Information of the Republic of Indonesia, the technical difficulties are:

a. Technical difficulties
   VPN is a network with a private server that creates a new IP (Internet Protocol Address). The new IP makes the actual IP hidden, so it takes several steps in finding it.
b. Requires a lot of energy resources
   Resource energy or human resources and tools that have not been evenly distributed become a separate obstacle if there is a blocking policy on VPN.
c. Substantial costs
   VPN blocking requires a very large cost, this will be a special consideration seeing that there is no urgency and priority regarding VPN blocking policies.

VPN countermeasures can be carried out preventively with appropriate regulations. There are currently no regulations governing application or abuse of VPN applications. VPN regulation as a prohibited tool is considered excessive because there has been no study of the intensity of the dangers of using VPN, but it is very possible because VPN can be a tool that facilitates criminal acts. This is in accordance with the decision of the Depok District Court No. 284 / PID.B / 2012 / PN.DPK which in legal considerations states that VPN is used as a facility for criminal acts. The existence of these reasons shows the urgency of starting discussions between the House of Representatives and the Government in making further regulations regarding the application and misuse of VPN applications.

Currently being considered by the Director General of Informatics Applications regarding appropriate policies. It is possible to block a VPN, but it will be very difficult, requiring large resources and funds. Closer will be made a licensing system for VPN application providers so that the government can control surfing activities using VPN. VPN application providers will be registered so that credibility is guaranteed given that many VPN service providers aim to steal VPN users' data that is not paid for.

There has been no official collaboration between the Republic of Indonesia National Police and the Ministry of Communication and Information in tackling the distribution of negative content on the internet. The collaboration between the Republic of Indonesia National Police and the Ministry of Communication and Information is only in the form of coordination, not law enforcement. The handling by the Ministry of Communication and Information is currently only blocking sites with negative contents. Of the blocking of 547,506 negative sites throughout 2018 by the Ministry of Communication and Information, only 16 cases were resolved to stage P21 by the Civil Servant Investigator (PPNS) of the Ministry of Communication and Information. However, there was no further action from the police to follow up on the results of blocking the negative content.

In addition to technical difficulties, regulation and law enforcement regarding cyber crime is indeed difficult to implement. Not only in Indonesia, even recognition of the difficulty of law enforcement relating to regulations and jurisdiction of a country is considered difficult for many countries.

Many nations and regional bodies such as the Council of Europe have addressed the problem of cyber-crime and laws exist that criminalise unauthorised access and unlawful use of computers, but such laws are neither universal nor uniform. Concerns remain focused on the 'weakest links' in the supposedly seamless security

chain necessary to prevent cyber-crime by predatory criminal groups. Comity thus can only be assured if wealthy states and affected industries are prepared to extend aid to those states or agencies less capable. Consensus is the best strategy, for the suppression of computer-related crime entails a mixture of law enforcement, technological and market-based solutions. It can be argued, however, that a strict enforcement agenda is usually not feasible because of the limited capacity of the state. It is also feared that over-regulation could stifle commercial and technological development. Those sceptical of a heavily interventionist approach also argue that the marketplace may at times be able to provide more efficient solutions to the problems of computer-related crime than the state. Even if they were increased, police resources could never be enough. Deficits characterise the technical and computing capacities of public police, and it is often difficult to retain trained agents (Broadhurst, R.G. 2006:24-25).

Difficulties so far have also been felt because VPN server application and service providers originate from abroad, so enforcement is often limited by the jurisdiction of a country.

CONCLUSION

The Republic of Indonesia National Police carries out their duties in accordance with statutory regulations. Efforts to tackle negative content are carried out preventively with Babimkamtibmas and the Sabhara patrol team by using cyber patrol. Efforts to tackle the repressive misuse of the VPN application are difficult because there are no statutory rules that govern. The misuse of VPN applications to open sites that are blocked by the government has been reviewed by the Ministry of Communication and Information and there will be a permit for the provision of VPN applications because VPN blocking requires high energy resources. There has been no specific collaboration between the Republic of Indonesia National Police and the Ministry of Communication and Information in law enforcement against sites that are blocked by the government.

The National Police of the Republic of Indonesia must keep trying to maintain order and security in society, especially in the rapidly developing world of technology while the law will always lag behind the development of society. The absence of rules is not an obstacle to preventive measures by utilizing the media to conduct a campaign to prevent cyber crime. Lawmakers must be more responsive to technological issues so that there are no more perpetrators of crime or victims. The Ministry of Communication and Information must start regulation on the provision of VPN with a license. Cooperation between the Indonesian National Police and the Ministry of Communication and Information should have begun to penetrate law enforcement.

BIBLIOGRAPHY

BOOKS

Budi Bagus Riswandi. 2003. *Hukum dan Internet di Indonesia*. UII Press: Yogyakarta

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

Sigid Suseno. 2012. *Yurisdiksi Tindak Pidana Siber*. Bandung: PT Refika Aditama

Soerjono Soekanto. 1983. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Fakultas Hukum Universitas Indonesia

JOURNALS

Broadhurst, R.G. 2006, 'Developments in the global law enforcement of cyber-crime', *Policing: an International Journal of Police Strategies and Management*, Vol. 29(3): 408-433

Hwian Christianto. 2017. "Mekanisme Penegakan Hukum Perkara Pidana Pornografi Melalui Internet", *Jurnal Veritas Et Justitia* (Vol. 3, No.1)

Kasma Tasaripa. 2013. "Tugas dan Fungsi Kepolisian Dalam Peranya Sebagai Penegak Hukum Menurut Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian." *Jurnal Ilmu Hukum Legal Opinion, Edisi 2, Vol (1) Tahun 2013*

INTERNET

https://kominfo.go.id/index.php/content/detail/3303/Internet-Sehat-dan-Aman--INSAN-/0/internet_sehat

https://nasional.tempo.co/read/701319/begini-cara-kementerian-kominfo-blokir-situs-terlarang/

https://tekno.kompas.com/read/2016/03/29/08370097/Situs.Banyak.Diblokir.Indonesia.Jadi.Pengguna.VPN.Tertinggi

QUOTE

You may have heard of Black Friday and Cyber Monday. There's another day you might want to know about: Giving Tuesday. The idea is pretty straightforward. On the Tuesday after Thanksgiving, shoppers take a break from their gift-buying and donate what they can to charity.

Bill Gates