IJSSR
International Journal of Social Service and Research

INTERNATIONAL JOURNAL OF SOCIAL SERVICE AND RESEARCH

THE ROLE OF INDONESIAN POLICE THROUGH "CYBER PATROL" IN PRESERVING AND MAINTAINING CYBER ROOM SECURITY

Edi Saputra Hasibuan
Faculty of Law, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia
Email: edi.hasibuan@dsn.ubharajaya

Abstract

The development of an increasingly advanced era, of course, has an impact on rapidly advancing technology and information. The era of the Industrial Revolution 4.0 has also become something that requires everyone to be more sensitive and accustomed to using technology. However, like two sides of the same coin, it seems that everything that has a positive impact also has a drawback or negative impact, any deviation either by system error or from human resources, causing new problems in the cyber world. Carding crimes, data abuse, phishing, and defacement of a website, as well as activities that cause unrest such as defamation and hoaxes are some examples of disturbing activities in the cyber world. This study aims to determine the role of the Indonesian police through "cyber patrol" in maintaining and maintaining security in cyberspace. The normative research method was used by examining each article, its rules and application, and combining it with a literature study by analyzing books, journals, papers, print media, and online news related to the Cyber Patrol. The police, as agencies that bridge this matter, are also not tired of continuing to work and provide innovation in dealing with every symptom and phenomenon in society. With the presence of the Cyber Police, it is hoped that they will be able to create comfort in using social media and other platforms

Keywords: police; cyber; patrol

Received August 03, 2022, Revised August 18, 2022, Accepted August 27, 2022

INTRODUCTION

The progress of an information system has forced a revolution in many ways, including news spread. For example, in the past, everyone could enjoy tea in the morning while waiting for the newspaper delivery with the latest news to arrive. All information is listed in newspapers that are sold from morning to evening. Now, only by opening a device through an internet connection can anyone access news through the news portals that have been provided, without the need to wait and turn pages one by one (Stevenson, 2010). this is only as far as the fingers play to turn the page and look for other news.

Not only that, another thing that is also very visible in the impact of the changes is when someone can talk and even see each other by using video calls on the available applications. In the past, meeting each other who were separated by distance took time. We are getting easier to connect with anyone as long as there is the internet, an infinite world (Cyber Space).

Cyberspace terms cannot be separated from work by Novelist science fiction named William Gibson. In one of his works entitled Neuromancer this term by William intends to describe or show a form of virtual hallucinations. He realized that a new room (space) emerged due to the electrically conducting wire media (cyber) connection, bringing together computer systems and telecommunications systems in electronic system activity. Increasingly, this term has become popular for communication from computer networks, which later became a global computer system network (William, 1984). Moreover, professionals in threat intelligence and cybersecurity concur that internet crime is growing exponentially (Cascavilla et al., 2021).

The threat of crime in the cyber world is not just a figment. Indonesia is increasingly massive, and the enactment of Electronic Identity Cards (E-KTP), mobile banking, and e-commerce provides an opportunity for criminals to misuse sensitive data. According to their needs, the realization of the E-KTP is a personal data recording program launched by the government (Latumahina, 2014).

Cases regarding crimes in cyberspace are indeed very diverse. If examined, the backgrounds of the perpetrators may vary. Some are just for fun, some intend to penetrate security to test a system, and the worst is those who commit crimes to gain and make a person suffer certain losses. In October 2021, the site of the National Cyber and Crypto Agency (BSSN) experienced a deface in which there was a change in its appearance of a site. BSSN admits that there is no important data related to disturbing public interests. The deface attack allegedly occurred in retaliation because, previously, someone from Indonesia hacked the Brazilian state website (CNN, 2021).

Furthermore, in the account burglary case in early February 2020, the victim was a senior journalist named Ilham Bintang, who had an account burglary by eight professional hackers. This case occurred by duplicating a telephone number where the last telephone number had been dead for a long time (not valid). This telephone number duplication was using the Population Identification Number listed on the victim's ID card; at that time, the victim himself was in Australia. Furthermore, with the new number they already have, the perpetrators replace the electronic mail account (email) so that from there, it allows the perpetrators to get the victim's new password. In this way, the hackers can also see the bank data owned by the victim and scoop up rupiah coffers from the victim's account (Velarosdela, 2020).

Cybercrime is indeed continuous with the increasing growth of telephone users. This makes the government get an additional burden with the emergence of this phenomenon, and the government must be busy and alert in dealing with internet network traffic. Internet installation in the form of levelling and improving facilities in each region includes effective oversight and regulation in the face of these developments (Hill, 2009).

Some of the above trigger the National Police, as a state institution tasked with protecting the public, to take a brilliant idea by conducting Cyber Patrols to provide maximum protection, which is tasked with monitoring all activities in cyberspace through various social media and platforms and ready to receive reports from those who have been or are being victims of cybercrimes.

METHOD

In this study, the normative research method was used by examining each article, its rules and application, and combining it with a literature study by analyzing books, journals, papers, print media, and online news related to the Cyber Patrol. The target data collected is related to cyber cases, prosecution, and prevention, then the existence of the Cyber Patrol, especially concerning the efforts made by the Cyber Police.

RESULTS AND DISCUSSION

A. Cyber Crime and the Importance of Data Protection

Humans are indeed intelligent and unique creatures. At the same time, humans are creatures who love to cause problems. How not, in reality, the existence of the law exists to regulate human behaviour. The existence of order, tolerance, security, and harmony cannot be separated from the presence of law in human life. Even like that, there are still many people who still commit violations and act against the law. If the law can be found in real-world criminal acts, such as robbery, fraud, humiliation, persecution, and so on, it comes through the Criminal Code and other regulations that specifically regulate it. Now, with the internet's presence and the virtual world's existence, problems seem to start moving from a real place to another place called cyberspace.

Advances in technology and information are increasingly rapidly giving birth to a variety of behaviours, both negatively and positively. From there, Law Number 11 of 2018 was born, later changed to Law Number 19 of 2016 concerning Information and Electronics. This law is not due to ordinary things, but the various phenomena in cyberspace have become the background of why this law was born.

Today, violations of the use of the internet in cyberspace have entered a growing stage, meaning that when one of the internet users harms and damages the activities of others, which often results in losses, one of which is data breaches. Data includes facts, communications or opinions relating to confidential, private, or sensitive individuals so that the data owner wants to keep and restrict other parties from collecting, using, or distributing it (Sautunnida, 2018).

Regarding data protection and privacy, Samuel Warren and Lois Brandeis wrote the legal conception of the right to privacy in Harvard Law Review Vol. IV No. 5, 15 December 1980. The article entitled "The Right To Privacy" was the first to conceptualize the right to privacy as a legal right (Warren & Brandeis, 2013). From this, it can be seen that the existence of legal rights must be protected.

Cybercrime case does not only occur in Indonesia but throughout the world. A case occurred in 2017 regarding the theft of data by a supermarket employee in the UK. The perpetrator, Andrew Skelton, stole employee salary data and used the data for personal purposes. In this case, Morrisons, the head of the supermarket, argues that the supermarket cannot be prosecuted because it happened not because of the will or orders of the company but purely a crime committed by an individual. But in the end, the British High Court ruled that the company remains responsible for criminal acts committed by its employees (Corfield, 2018). It can be seen from this case that data entry can indeed lead to other criminal cases, such as burglary, hacking, or phishing.

The parts of Cyber itself exist in several forms: Cyber Crime is a form of virtual crime that utilizes computer media connected to the internet that exploits other computers that are also connected to the internet. Cyber Threat, a threat here, is defined as a threat in the operation of information that interferes with confidentiality and availability. Cyber-attacks, you could say, are the realization of previous threats, intentionally disrupting the confidentiality, integrity, and availability of information physically and logically in the information system. Cyber Security is every effort to protect and minimize interference with the confidentiality of information; last is Cyberlaw, which is a form of legal protection related to legal subjects, namely individuals who take advantage of the technology and information they use, such as the ITE Law as an example.

B. Cyber Patrol A Breakthrough in Monitoring and Ordering Cyberspace

1. Police Flexibility

In practice, the police must be professional and always ready to deal with any symptoms in the community and must be able to become a flexible agency by following the times and adapting them. From a sociological point of view, there will always be related to a position (status) thus, understanding the role of the National Police cannot be separated from its position in the constitutional system adopted (Ismail, 2011).

In a democratic system, the function of the police can be grouped into three functions that demand character and ways of working with each other: fighting crime, protecting citizens and maintaining public order (preservation of law and order) (Ismail, 2011). From these police functions, four roles must be carried out: the role of the law enforcement agency, the role of maintaining order (law and order maintenance), the role of peacekeeping official, and the role of (public servant). These four roles lead to the output of protecting (to protect) and serving (to serve) so that the police as guardians of civil values in a climate of democratic life can be realized (Ismail, 2011).

One of the Cyber Police establishments began by issuing a circular letter from the National Police Chief, namely (SE) No. SE/2/11/2021 concerning Ethical Cultural Awareness to Create a Clean, Healthy, and Productive Digital Space for Indonesia. The SE is a decision to follow up on the President's request for the police to be more selective in handling cases of alleged violations of Law No. 11 of 2008 as amended by Law No. 19 of 2016.

Some of the points outlined by the National Police Chief, which are expected to be realized by the ranks below him, are: (Circular Letter of the Chief of Police No. Se/2/11/2021) First, following the development of the use of digital space which continues to develop. Second, understand the ethical culture that occurs in the digital space by taking an inventory of various problems and impacts that occur in society. Third, prioritizing preemptive and preventive efforts through virtual police and virtual alerts aimed at monitoring, educating, giving, warning, and preventing the public from potential cybercrimes. Fourth, in receiving public reports, investigators must distinguish between criticism, input, hoaxes, and defamation that can be punished. Fifth, after receiving the report, the investigator must communicate with the parties, especially the victim (not represented) and facilitate by giving the widest possible space to the disputing parties to mediate. Sixth, investigators conduct comprehensive studies and case titles on cases handled involving elements of the Criminal Investigation Agency, or the Directorate of Cyber Crime can go through zoom meetings and make collegial collective decisions based on existing facts and data. Seventh, investigators have the principle of criminal law to be the last resort in law enforcement and prioritize restorative justice in handling cases. Eighth, parties and victims who take peaceful steps become part of the priority of investigators to carry out restorative justice. Ninth, no detention is carried out for the victim whose case still wants to go to court, but the suspect has apologized and is aware of his actions. Before the file is submitted to the Public Prosecutor (JPU) to be given space for mediation again. Tenth, investigators should coordinate with the public prosecutor in its implementation, including providing advice on the implementation of mediation at the prosecution level. Eleventh, to carry out supervision in stages on every investigation step. Then give rewards and punishments for continuous assessment.

Furthermore, the National Police Chief provides a classification of ITE Law cases that can be resolved through restorative justice efforts, namely defamation, slander and humiliation, by issuing the National Police Chief's Telegram Letter No. ST/339/II/RES 1.1.1/2021 regarding guidelines for Handling Cyber Crime Cases using the ITE Law. This telegram was issued on 22 February 2021. Various parties strongly support this effort, one of which is the National Police Supervision Commission; its spokesman Poengky Indarti said that the circular needs to be understood and used as a guideline for the implementation of Police investigators to always prioritize a preventive attitude in ITE Law cases, especially cases that are mild and can forgive each other. Despite other cases that have the potential to divide the nation, such as the SARA issue, hoaxes need to be followed up by legal processes to achieve legal certainty (Halim, 2021).

2. The Existence of Cyber Police in Conducting Cyber Patrols in Providing Security and Convenience in the Virtual World

Cyber Police conduct Cyber Patrol activities by monitoring every activity in the virtual world, especially through social media and various other platforms. In the domestic scope, the efforts made by the National Police in tackling the occurrence of cybercrime have made several efforts, namely (Utomo & Putranti, 2016):

a) Respond to and receive every report from the public on cybercrime allegations and record every case handled against the report.
b) Conduct online investigations (via the internet/virtually) against crimes using social networks, email and e-commerce.
c) Coordinating with the Ministry of Communication and Information
d) Cooperating in the banking sector, especially with Bank Indonesia, to avoid fake accounts used by criminals.
e) We urge the public always to use the internet safely.
f) It is improving the understanding and training of Indonesian Police expertise in cybercrime by sending its members to training and courses in several developed countries.

The efforts and activities carried out by the police in improving Cyber security so far have had many significant impacts through arrests and the disclosure of causes related to cybercrimes. In December 2019, the Cyber Police arrested Ransomware perpetrators at companies in the USA. The perpetrators spread or blast emails to potential victims containing a link that has been installed crypto locker, which can cause the mail server system at a company to be encrypted at a company, and the perpetrator directs the victims to open the link. If a company eats the bait, the perpetrator asks for a ransom in cryptocurrency so that the webmail server can be reused (Cyber Police, 2022).

Another example can also be seen through fraud cases under the guise of online loans, and the perpetrator pretends to be the party who will provide online loans. Still, if someone is interested, then the person is asked for some money as administrative funds. After the money is given, the perpetrator disappears and immediately decides to communicate with the victim by blocking the victim's contact number. It did not take long. After receiving the report, the Regional Police Force Cyber Sub-Directorate team conducted further searches and found the perpetrator's location in a village in South Sulawesi Province. It is conceivable how communication technology allows someone to make money by fraudulent means without having to meet and regardless of distance. From the search, one of the interesting things was finding evidence, namely a box of starters (Cyber Police, 2022). This indicates that the perpetrators use many numbers to eliminate traces and make tracking difficult. Unfortunately, it is not easy; law enforcers always try to be 1 step ahead of the criminals.

In addition, to promote preventive action, the National Police also uses a method of activity called public relations on the internet by delivering information virtually. Implementing cyber public relations is considered a key component in supporting and succeeding the Indonesian National Police program, especially regarding countering negative opinions on social media related to Tohate speech. The National Police prioritizes a persuasive approach with a gentle approach rather than being carried out utilizing violence which usually will only be carried out if conditions are out of control.

CONCLUSION

Globalization era progress and the advancement of technology in the dissemination of information has become a fact that the flow of the industrial revolution cannot be dammed and continues to progress. The best choice is to respond well to these flows. Cybercrime needs serious attention for anyone; the existence of deviant behaviour from a group of people or individuals who use technology and cyberspace to commit crimes for personal gain tends to cause losses to other parties**.**

Understanding and knowledge of the importance of data protection is one thing that must continue to be improved, the government with all efforts, both through legislation and direct guidance through outreach to the public. It is an effort that needs to be appreciated and must continue to be maximized. Still, on the other hand, it has people should be aware and control of their behaviour on the internet because nowadays, our fingers can do anything, and can be anything in cyberspace, whether it be a positive thing or it has a negative impact on themselves and others. Elaboration between the community and government organs must go hand in hand to create security and comfort on the internet.

The police, as agencies that bridge this matter, are also not tired of continuing to work and provide innovation in dealing with every symptom and phenomenon in society. With the presence of the Cyber Police, it is hoped that they will be able to create comfort in using social media and other platforms. At the same time, the National Police continues to monitor and train its members to provide a preventive attitude in dealing with cases that occur in cyberspace. Thus, it can be said that the Cyber Police is not only tasked with handling public complaints or reports but also for prevention through socialization and cyber public relations to ensure that the public gets good information and prevent the circulation of hoaxes. Hopefully, this will continue to grow and provide more benefits to the general public.

REFERENCES

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. Scopus

CNN, I. (2021). *BSSN Akui Situs Diretas, Kena*

Serangan Deface. https://www.cnnindonesia.com/teknologi/20211025175708-185-712153/bssn-akui-situs-diretas-kena-serangan-deface

Corfield, G. (2018). *Morrisons supermarket: We're taking payroll leak liability fight to UK Supreme Court*. https://www.theregister.com/2018/10/23/morrisons_loses_court_appeal_data_theft/

Cyber Police. (2022). *Siber Polri Tangkap Pelaku Ransomware Pada Sebuah Perusahaan di Sebuah Perusahaan USA*. https://patrolisiber.id/

Halim, D. (2021). *Kompolnas Minta Penyidik Polri Laksanakan SE Kapolri soal UU ITE*. Kompas.Com. https://nasional.kompas.com/read/2021/02/24/08335521/kompolnas-minta-penyidik-polri-laksanakan-se-kapolri-soal-uu-ite.

Hill, D. G. (2009). *Data Protection Governance, Risk Management, and Compliance*. CRC Press. Google Scholar

Ismail, C. (2011). *Polisi Sipil dan Paradigma Baru Polri*. Merlyn Press, Jakarta. Google Scholar

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Google Scholar

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384. Google Scholar

Stevenson, A. (2010). *Oxford dictionary of English*. Oxford University Press, USA. Google Scholar

Utomo, T. C., & Putranti, I. R. (2016). Kerjasama Kepolisian Negara Republik Indonesia (Polri)-Australian Federal Police (Afp) Sektor Capacity Building Dalam Penanggulangan Tindak Pidana Cyber Crime Di Indonesia Periode 2012-2014. *Journal of International Relations*, *2*(1), 38–46. Google Scholar

Velarosdela, R. N. (2020). *Kronologi dan Peran 8 Pelaku Pembobolan Rekening Ilham Bintang*. Kompas.Com. https://megapolitan.kompas.com/read/2020/02/05/13355011/kronologi-dan-peran-8-pelaku-pembobolan-rekening-ilham-bintang?page=all

Warren, S., & Brandeis, L. (2013). The right to privacy. *Civilistica. Com*, *2*(3), 1–22. Google Scholar

William, G. (1984). *Neuromancer, ACE Science Fiction Books*. The Berkley Publishing Group, New York. Google Scholar