International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 03, 2020
ISSN: 1475-7192

Efforts to Overcome Cyber Crime Actions in Indonesia

[1]Muhammad Hatta

Abstract--*The presence of the internet can penetrate the boundaries between countries and accelerate the spread and exchange of information throughout the world. Although there are many positive impacts of internet use, there are also negative impacts that disturb the community. One can easily become a criminal (cyber crime) only by creating blogs, accounts, applications, programs, sites in various mass media and social media to commit fraud, data theft, illegal use of credit cards, the spread of pornographic content, online gambling, online prostitution, hate speech, radicalism, terrorism and so on. To overcome crime in the virtual space, the government has issued Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions. But not all internet users know and understand the substance of the law. Therefore, the government, employers and institutions that are engaged in information and communication technology have the responsibility to socialize the law to the public to prevent crime in the virtual space.*

Keywords--*Actions, Cyber Crime, Penetrate.*

I. INTRODUCTION

The development of information technology and especially internet communication has led to significant social, economic and cultural changes taking place so quickly. This technology relates to systems that can collect, store, process, produce and disseminate information to the public effectively and quickly. This technology is believed to be the main alternative for the implementation of social, economic and government social activities. However, information technology is currently a "double-edged sword", besides being able to contribute to improving welfare, progress, human development, as well as being an effective means of committing crime [1].

The use of information and communication technology is an electronic system that is computer-based and can only be seen virtually [2]. In the dimension of the virtual world, one's activities are difficult to limit because information technology is very cheap and easily accessible from any part of the world [3]. As a result, everyone can commit crime both among internet users and other people who have never been in contact with those who are involved [4]. For example, someone makes a transaction with another person's credit card without the owner's knowledge. In addition, through virtual media, a person is very easy to create pictures, statuses, memes and videos that contain elements of hatred, attack other people's honor, radicalism and terrorism. Even someone can become a propaganda expert just by creating blogs, accounts, sites using fake identities [5].

To prevent the use of cyber crime, the government has issued Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the ITE Law). The purpose of the issuance of this law is to make use of the internet safely and prevent its misuse. However, this

[1]*Department of Law, Faculty of Law, Universitas Malikussaleh, Aceh Utara, Indonesia, muhammad.hatta@unimal.ac.id*

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

law does not limit the freedom of democracy in Indonesia but this law limits the rights of thinking and arguing in a public space that can cause harm to the public both materially and materially.

The use of the internet must be directed towards mutual benefit, providing a sense of security, justice and legal certainty for users and providers of information technology. Therefore, the issuance of the ITE Law aims to guarantee, protect and respect one's rights and freedoms in accordance with moral considerations, religious values, security and public order. In order to achieve this goal, the government must provide an understanding to the public that the existence of the ITE Law is not considered to curb the freedom of democracy, instead the ITE Law places the freedom of democratic society to the right patron.

II. RELATED WORKS

Rapidly evolving computer technologies have become an integral part of modern life. While it simplifies social life, the changes brought by technology also bring some security issues [6]. Cyber criminals seem to keep their business without any hindrance. Home computer users are particularly vulnerable to attack by a sophisticated and globally scattered hacker group. In the era of smart phones, the situation worsened, hackers offered even more attacks of abuse [7]. Research efforts in the field of computer warfare are extensive and involve a number of issues such as legality, computer weapons and deterrence. Despite all of the cyber war research activity, a great deal has overlooked one aspect: restoring peace and security after its end [8]. Computer end-user hygiene often plays a major role in disrupting computer security. Therefore, we need a deeper understanding of the differences between users that are related to good or bad hygiene and an updated view of what users do to promote proper hygiene [9].

III. RESEARCH METHODS

This paper uses a qualitative research methodology. According to McCracken, qualitative methodology is research using descriptive data or information obtained by observation, interviews and analysis of various documents related to the research being conducted [10], [11].The purpose of the research is qualitative to describe, record, analyze, give factual and accurate description and interpret a situation, facts or phenomenon where the internet network has given opportunity to terrorism group to develop its network in Indonesia.

IV. RESULT AND DISCUSSION

Internet and Its Impact

Information technology through the internet has led to faster and more rapid exchange of information. The internet and its supporting technology devices seem to want and have made the world almost borderless [12]. The development of information and communication science and technology has led to various changes in the political, economic, social and cultural fields [13]. Even the dimension of state sovereignty extends, no longer consists of land, sea and airspace, but also virtual space or cyberspace [14]. The rapid development of information and communication technology that uses internet network facilities has caused concern in various countries in the world so that a number of countries restrict internet access to their citizens. Some countries in Asia, Africa and the Middle

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

East impose strict restrictions on the internet because it is feared that the public will be difficult to control with various kinds of information circulating from outside [15].

In Indonesia, the use of the internet has also experienced very rapid development. Internet cafes (cyber cafes) thrive like mushrooms in the rain. In fact, the internet can be used cheaply to remote villages so that Indonesia has become one of the countries with the largest number of internet users in Southeast Asia. According to the Indonesian Internet Service Providers Association (APJII), the number of internet users in 2017 reached 143.26 million people. Most internet users in Indonesia are from the age group 25-29 years and 35-39 years. However, teen age groups that consume the internet are increasing. APJII mentions the age group of teenagers who actively use the internet from the age group of 15-19 years as many as 12.5 million users and the age group 10-15 years as much as 768 thousand users [16].

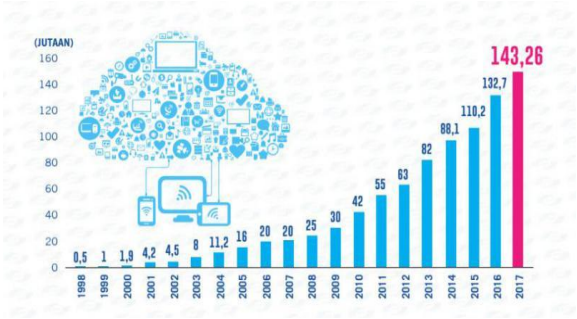

Figure 1. The Growth of Internet Users in 2017

The number of very large internet users in Indonesia from relatively young age backgrounds has the potential to become perpetrators and victims of mayantara crime. A feeling of wanting to know, fad, try and like challenges has given birth to hackers who are still relatively young in the world class. Indonesia is the first largest number of hackers in the world with 38% achievement [15].Following with China, the United States, Taiwan, Turkey, India and Russia. The number of hackers in Indonesia, allegedly because of the many hacking learning media available in cyberspace such as YouTube, blogs, Facebook, Instagram and others. In the case of the breach of the www.tiket.com site, Sultan Haikal, a hacker who graduated from junior high school who was only 19 years old, had hacked the www.tiket.com site and caused a 4.1 billion loss [17].

Likewise, the hacking of Malaysian websites due to the Indonesian flag incident was reversed at the SEA Games in Kuala Lumpur 2017. They hacked Malaysian websites and made images of Malaysian flags also overturned. In fact, Indonesian hackers have conducted a "war" in cyberspace with Australian hackers in 2013. This war began with the theft of Garuda Indonesia customer credit card data by hackers Australia. Indonesian hackers respond to Australian hackers by destroying Australian government sites and 178 other Australian websites. In addition, Hecker Indonesia has been in the spotlight of the world because it is able to hack satellite and control the world internet network [18].

The high number of internet users in Indonesia is one of the factors that increase mayantara crime or cyber crime. Based on data from the Directorate of Crime of Cyber Crimes (DitTipidsiber) Criminal Investigation of the

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

Republic of Indonesia Police stated that the number of cyber crimes in 2017 totaled 1,763 cases [19]. According to data from the Identity Theft Resource Center (ITRC), in July 2018 the number of cyber crimes in July 2018 totaled 668 cases with a total lost data reaching 22,408,258 data. [20]. From these data, the highest number of cyber crimes cases are fraud cases with 767 cases. The second rank is handling 528 cases of insult and defamation [21]. However, cyber crime is not only done by Indonesian citizens but foreign citizens also carry out their actions in Indonesia with various modes.

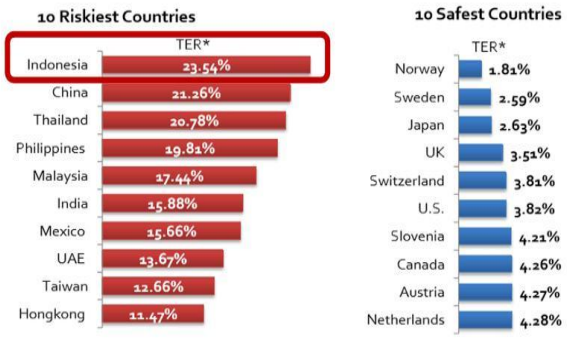

Figure 2. The Most Risky and Safe Countries Against IT Security Attacks [22]

Based on the data in Figure 2, shows how weak the security system of the use of information technology and electronic transactions in Indonesia so that Indonesia is ranked first as the country most at risk of experiencing cyber crime attacks from hackers from various countries in the world. There have been several cases of cyberattacks carried out by foreign nationals in Indonesia, for example, hundreds of organized Chinese citizens from several groups committed acts of fraud and theft through the internet network in Indonesia. In just two weeks, this syndicate group can make a profit of 2 billion rupiah. Therefore the government and society must realize that the development of crime using information technology is increasing. Cyber crime syndicates not only can attack individual and corporate security systems, they can even break down the government's defense system.

Efforts to Overcome Cyber Crime Measures in Indonesian government defense systems.

Prevention of mayantara crime must begin by providing an understanding to internet users about the limitations in expressing ideas, thoughts, status, statements, pictures, videos, memes and other content in various mass media and social media. The limit has been regulated in the ITE Law with the aim of controlling, supervising and disciplining the use of information technology that is increasingly developing and disturbing the public. Many cases of fraud, humiliation, murder, rape, kidnapping, confinement began with the use of the internet network with a variety of social media applications. Not only that, crime with the use of information technology can attack government sites, companies, banking and public private data. The presence of the ITE Law is expected to be able

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

to curb users of information technology, but do not insulate the democratic space of society that is free to express thoughts and opinions.

The substance of the ITE Law consists of several forms, namely: [23]

a. Economic cyber crime;
b. Electronic Funds Transfer (EFT) Crime;
c. Cybank Crime, Internet Banking Crime, On-Line Business Crime;
d. Cyber/Electronic Money Laundering; 5. Hitech WCC (white collar crime);
e. Internet fraud (Bank fraud, Credit card fraud, On-line fraud);
f. Cyber terrorism;
g. Cyber stalking;
h. Cyber sex, cyber pornography, cyber defamation, cyber (child) criminals.

After being published, the ITE Law is widely used by law enforcers to ensnare perpetrators of crimes related to pornography, humiliation, fraud and cases that affect various government sites, companies, banks and so on. For example, the case of defamation carried out by PritaMulyasari against Omni International Hospital. The case began when Prita wrote an e-mail to her friends (e-mail group) about the poor service of the Omni International Hospital. The contents of the e-mail were widely circulated in the community so that the hospital management took legal action on charges of defamation. The hospital considered that Prita's accusations were untrue and tendentious. Doctors and health workers at Omni International hospitals have carried out medical services professionally. Based on these facts, PritaMulyasari was arrested for allegedly violating Article 27 of the ITE Law.

Reflecting on the PritaMulyasari case, although in the end the defamation or defamation case against Omni International hospital was won by PritaMulyasai, but the concern of the community is that everyone is free to give opinions to someone, institution, institution or even the country through virtual media . However, someone must understand that this opinion should not damage someone's honor and good name so that the news leads to news of slander, lies and misleading.

One type of crime that often occurs in cyberspace is pornography (cyberporn). Many are found in the virtual world of writing, images, videos and other pornographic content. The most horrendous case in Indonesia relating to pornography is the circulation to the public video of NazrilIrham (Ariel Paterpan) with Luna Maya and Cut Tari. In the trial, it was found the fact that the nasty video was stored on a computer in the Grop Band Paterpan studio and distributed through the internet by Reza Rizaldy, Ariel Paterpan's own friend. Ariel Paterpan and Reza Rizaldy were prosecuted under Article 27 paragraph (1) jo. Article 45 paragraph (1) of the ITE Law because both of them intentionally and without rights distribute and / or transmit and / or make access to electronic information and / or electronic documents that have contents that violate decency. In the trial, the judge ruled that Reza Rizaldy had been proven guilty by distributing a perverted video of Ariel Perpan with Luna Maya and Cut Tari through the internet and sentenced to 2 years and 6 months (Supreme Court Decision, No. 68 / Pid / 2011 / PT.Bdg) [24].

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

The next astonishing case was the case of 4,600 sites from various countries carried out by Sultan Haikal M. Aziansyah who was still 19 years old and only graduated from Elementary School. Perpetrators intentionally infiltrate websites belonging to a particular person or institution, then offer cooperation to correct the weaknesses of the company's website (for example, the website www.tom.com and go-object.com) which may be entered by hackers. However, this warning and offer of cooperation is not cared for so that it causes players to get upset and hit related sites. Sites that are designed are not just company sites like PT. Global Network or Tiket.com, but the perpetrators also hit the government, police, military sites and so on. From the results of various sites, the perpetrators managed to get a profit of Rp. 4,124,000,982. Haikal allegedly fulfilled the elements of Article 46 paragraphs 1, 2 and 3 in conjunction with Article 30 paragraphs 1, 2 and 3, and / or Article 51 paragraphs 1 and 2 juncto Article 35 and / or Article 36 of the ITE Law and sentenced to 4 years in prison [25].

Another horrendous case is the Saracen case. Saracen are organized groups in Indonesia that intentionally spread false news, speeches of hatred and hostility in cyberspace. Spreading false news, hate speech and hostility aims to create political, legal and economic chaos in Indonesia [26]. Saracen have 20 members and have 9 million followers from 800,000 Facebook accounts from various countries [27]. They are paid to counter issues relating to political contestants in general elections. For contestants who do not pay or contribute to Saracens, this group will attempt to spread negative issues that contain hate content and SARA (ethnicity, religion, race and class) so that the credibility and prestige of the political contestants fall in the eyes of the public. On the contrary, a person or group who wants to pay or contribute to the Saracen will form a good opinion and the electability will increase [27].

Muhammad Harsono Abdullah Saracen Group Admin and its members are prosecuted under Article 45A paragraph 1 & 2 juncto Article 28 paragraph 2 of the ITE Law because these tapering activities are legally and convincingly proven intentionally and without rights to spread false and misleading news aimed at inciting hatred or hostility certain individuals and / or community groups based on ethnicity, religion, race, and intergroup (SARA). The judge of the Pekanbaru District Court sentenced the Saracens to guilty with a sentence of 2 years and 8 months in prison [28].

He rapid development of information technology is also realized by perpetrators. Even certain crimes are more effectively carried out through the internet network compared to conventional methods. Someone can become a propaganda expert just by creating a personal blog, account or news site with a fake identity. The number of internet users in the world is a fertile field for terrorist groups to spread influence and recruit new members to join their groups. Coleman and McCahill said that most terrorist members from Saudi Arabia were recruited through the internet [29].

To prevent the circulation of hoaxes, speeches of hatred, radicalism, the government established a special division (National Siberian Agency) to deal with cybercriminals in charge of identifying sites, media, blogs, accounts and others that contain hoax news content, kebenciaan said. radicalism, the doctrine of terrorism, pornography and content containing ethnicity, religion, race and intergroup (SARA). The government urges twitter, google, youtube and other social media to isolate these content by implementing a trusted flagger system or other system [30].Baapna and Waimann said that if the government is serious in enforcing the law, making a sophisticated

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

identification system and increasing the punishment for mayantara criminals can prevent mayantara crimes [31], [32].

Although the government has created a system or program to block negative sites, the government must be consistent and sustainable to socialize the ITE Law to the public. Research conducted by Abi Bayu shows that more than 50% of the public still do not fully understand the substance of the ITE Law [33]. This is caused by the attitude of the people who are less concerned about the rules that apply in the ITE Law so that people often abuse the freedom of opinion in using social media.

Departing internet users from sharing cultural, age and professional backgrounds, socialization can be done by holding seminars, workshops, conferences and so on. But for internet users among adolescents, students and students, the methods taken are more current or by means of melenial such as using motion graphic animation media, social networking sites, below the line media such as posters and pins and using advertisements and documentaries . These various media are expected to be able to educate the public, especially the younger generation, to be wiser in expressing their opinions on various social media and to improve public literacy regarding the positive and negative sides of the use of the internet network. Communities need to cultivate confirmation when getting news by looking for news references from various official news sites.

In carrying out the socialization of the ITE Law, the government must collaborate and involve various parties such as educational institutions, law enforcement, traditional and religious figures, parents and entrepreneurs who struggle in the virtual world. Communities can contribute actively by reporting if they get or find hoax news, hate speech, radicalism from news sites and social media. The Government has launched the Content Complaint Ticketing System, where the public can file complaints against negative content and can see how far the follow-up process of the complaint is running [34]. In addition, people can take advantage of the hoax news report feature provided by social media such as the report status feature on Facebook, feedback features on Google, the report tweet feature on Twitter. Negative news content can also be reported to aduankonten@mail.kominfo.go.id or data.turnbackhoax.id page [35].

V. CONCLUSION

According to the research employing two organic compound models ibuprofen and diclofenac, we may conclude that wood decay fungus (trametes sp.) contains laccase enzyme. Laccase rough extract with 5 hours of reaction contact with the model compounds above is known to be able to serve as biomodification catalyst with hydroxylation reaction ability.Laccase enzyme belongs to the oxidoreductase group, thus with detection of hydroxyl group (-OH) in intermediate product, we may conclude that the model compounds designed in this research experience biotransformation. Based on the foregoing, we may conclude that the laccase rough enzyme of fungus trametes sp. species has the ability to modify organic compound, such as from diclofenac to hidroxy-diclofenac.

REFERENCES

1. M. A. Sanusi, *Hukum dan Teknologi Informasi*, 3rd ed. Jakarta: Gramedia Pustaka Utama, 2005.
2. R. Tongia, E. Subrahmanian, and V. S. Arunachalam, *Information and Communications Technology (ICT)*. 2005.

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020

3. D. Karina and O. Mendoza, "The Vulnerability of Cyberspace - The Cyber Crime," *J. Forensic Sci. Crim. Investig.*, vol. 2, no. 1, pp. 1–8, 2017.
4. K. S. Nwizege, F. Chukwunonso, C. Kpabeb, and S. Mmeah, "The impact of ICT on computer applications," *Proc. - UKSim 5th Eur. Model. Symp. Comput. Model. Simulation, EMS 2011*, vol. 2, no. May 2014, pp. 435–439, 2011.
5. Y. Jewkes, *Handbook of Internet Crime*. United Kingdom: Willan Publishing, 2010.
6. D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Soc. Behav. Sci.*, vol. 182, pp. 590–595.
7. C. O. K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, "Is the responsibilization of the cyber security risk reasonable and judicious?," *Comput. Secur.*, vol. 78, pp. 198– 211, 2018.
8. L. M. M. Robinson, K. Jones, H. Janicke, "An introduction to cyber peacekeeping," *J. Netw. Comput. Appl.*, vol. 114, pp. 70–87.
9. J. D. S. A. A. Cain, M. E. Edwards, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45.
10. G. . McCracken, *The Long Interview*. London: Sage, 1998.
11. C. G. Cevilla, *Pengantar Metode Penelitian*. Jakarta: Universitas Indonesia Press, 1993.
12. K. M. Finklea, "the Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement.," *J. Curr. Issues Crime, Law Law Enforc.*, vol. 5, no. 1/2, pp. 13–20, 2012.
13. United National Office on Drugs and Crime, "Comprehensive Study on Cybercrime," in *Conference Support Section Organized Crime Branch Division for Treaty Affairs*, 2013, no. February, pp. 1–30.
14. M. Heidegger, *The Question Concerning Technology, and Other Essays*. London: Garland Publishing, 1977.
15. R. Bernardino, "Cyber Crime," Kupang, 2017.
16. T. APJII, "Saatnya jadi Pokok Perhatian Pemerintah dan Industri," *Buletin APJII*, pp. 1–7, 2016.
17. D. Andrianyanto, "Kawanan Haikal Peretas Ribuan Situs, Siapa Gantengers Crew Ini?," *Tempo*, 2017. [Online]. Available: https://m.tempo.co/read/863565/kawanan-haikal-peretas-ribuan-situs-siapa-gantengers-crew-ini/full&Paging=Otomatis. [Accessed: 07-Apr-2017].
18. F. Miftach, "Enterprise Hacking: Who Needs Exploit Codes?," in *Hack In The Box Security Conference*, 2007, pp. 1–65.
19. P. Batubara, "Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber," *Okezone News*, 2017. .
20. F. Yahya, "Hingga Juli 2018, Sudah Ada 668 Kasus Kejahatan Siber," *Okezone News*, 2018. .
21. S. Figure, "No Title No Title_2015," no. c, pp. 1–4.
22. ISTR, "Internet Security Threat Report - ISTR," *Symantec J.*, vol. 22, no. April, p. 77, 2017.
23. B. N. Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indoensia*. Jakarta: PT. Raja Grafindo Persada, 2006.
24. W. Alamsyah, "JURIDICAL ANALYSIS OF THE VERDICT THAT DECIDED ON THE ARTICLE WAS NOT SENTENCED IN THE INDICTMENT BE REVIEWED OF DEFENDANT'S RIGHTS (Case Study Of Bandung District Court Verdict Number:1401/Pid.B/2010/PN.Bdg)," *J. Has. Penelit. Mhs.*, vol. 1, no. 1, pp. 1–9, 2010.
25. R. Alvionitasari, "Haikal Tersangka Hacker Ribuan Situs, Polisi: Dia Pemuda Tertutup," *Tempo*, 2017.
26. L. Shaw, "Hate Speech in Cyberspace: Bitterness without Boundaries," *Notre Dame J. Law, Ethics Public Policy*, vol. 25, no. 1, pp. 279–304, 2011.
27. Z. Syahayani, "Saracen: Potret Bisnis Hoax di Indonesia," *Updat. Indones.*, vol. XI, no. 7, pp. 2–4, 2017.
28. D. Doly, "Pengaturan penyebaran ujaran kebencian dan isu sara ditinjau dari hukum konstitusi," *Info Singk. Huk.*, vol. IX, no. 17, pp. 1–4, 2017.
29. E. Kyt *et al.*, "Cybersecurity and Cyberwarfare: Ideas for Peace and Security," *Cent. Strateg. Int. Stud.*, no. July 2010, pp. 1–34, 2011.
30. Tim Viva, "Menkominfo Ancam Facebook dan Twitter," *Viva News*, 2017. .
31. J. H. and S. Bapna, "How Can We Deter Cyber Terrorism," *Inf. Secur. J.*, vol. 21, no. 2, pp. 102–114, 2012.
32. G. Waimann, *The Influential: People who Influnce People*. Albany: State University of New York Press, 1994.
33. A. B. Pranata, "Socialization of ITE Law Related to Freedom of Expression in Social Media Using Public Service Advertisement," Faculty of Computer Science, DINUS University, 2016.
34. N. K. Sa'diyah, "Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik," *Perspektif*, vol. 17, no. 2, pp. 78–89, 2012.
35. Yunita, "Ini Cara Mengatasi Berita 'Hoax' di Dunia Maya," *Kementerian Komunikasi dan Informatika Republik Indonesia*, 2017.

DOI: 10.37200/IJPR/V24I3/PR200925
Received: 19 Jan 2020 | Revised: 06 Feb 2020 | Accepted: 12 Feb 2020