International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 6, December 2017, pp. 3735~3744
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i6.pp3735-3744

The Authority of Government in Clearing Hatefull and Hostilities Electronic Information Based on Tribe, Religion, Race and Intergroup

I Gede Yusa[1], Dewi Bunga[2], Deris Stiawan[3]
[1]Faculty of Law, Udayana University, Bali, Indonesia
[2]Faculty of Dharma Duta, Denpasar State Hindu Dharma Institute, Bali, Indonesia
[3]Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya, Palembang, Indonesia

Article Info

Article history:

Received Jun 7, 2017
Revised Sep 12, 2017
Accepted Sep 25, 2017

Keyword:

Authority
Clearing hatefull
Electronic information
Government
Hostilities

ABSTRACT

The Act Number 19 of 2016 concerning the amendment of The Act Number 11 of 2008 concerning Information and Electronic Transaction governing the authority of government in clearing hateful and hostilities electronic information based on tribe, religion, race and intergroup. On the one hand, the government authority aims to protect the public interest and the integrity of the nation, but on the other hand, termination of access to information would restrict the right to freedom of opinion and the right to privacy of Internet users. This study was a normative legal research, which examined the basic authority for the government to shut down negative content in cyberspace. Legal materials were collected through library research. The analysis was conducted qualitatively. This study examined three issues, namely; spreading hatred and hostility in cyberspace, legality government to close the spreading hatred and hostility and electronic evidence in spreading hatred and hostility. Spreading hatred and hostility were criminal acts that used the Internet as facilities. Internet was used by extremists to disseminate his teachings, even being used to commit acts of terrorism (cyber terrorism). In maintaining the unity and integrity, then the government had the authority to shut down access to the unlawful electronic system. The closure should be accompanied by proof of electronic information that contains hatred and hostility based on tribe, religion, race and intergroup.

Corresponding Author:

I Gede Yusa
Faculty of Law, Udayana University,
Badung, Bali, Indonesia
Email: gedeyusa@rocketmail.com

Deris Stiawan
Faculty of Computer Science, Universitas Sriwijaya
Palembang, Indonesia
Email: deris@unsri.ac.id

1. INTRODUCTION

At the end of 2016, the government issued a policy in the field of information technology by revising and adding a number of articles of Act concerning Information and Electronic Transaction. The policy is regulated in The Act Number 19 of 2016 concerning the amendment of The Act Number 11 of 2008 concerning Information and Electronic Transaction [1]. One of the new provisions in the legislation is the government authority to block or order electronic system organizers to cut off access to electronic information that is unlawful, including social media accounts to spread negative content. The government

authority is the basis for providing protection to Internet users to gain the right information access. to electronic information that is unlawful, including social media accounts to spread negative content. The government authority is the basis for providing protection to Internet users to gain the right information access.

The authority of the government to shut down electronic systems that violate the law would be a new spirit to maintain the unity of the Indonesian nation. Various issues of discrimination that is spread through cyberspace proved to have led to the disintegration of the nation. In other hand, proposed by [2], and [3] describes principal problem in developing strategic approaches to cybersecurity is the dissonance between the easiness with which an attack can be conducted as opposed to growing challenges associated with their detection and prevention. Attacks against opponents often raised the issue of race, war and promotion policy program or a view [2], [4]. Differences in tribe religion, race and intergroup serve as the basis to bring down political opponents. The spread of hatred that is based on the classification of tribe, religion, race and intergroup is used to gain sympathy, support, or attack a person and a group of people. This issue is not only susceptible used in Indonesia but also in developed countries.

In this era of digitalization, the debate between adherents of different religions often occurs in social media. Discussion of issues in the social media has a great impact. Social media can shape public opinion and spawn a new social force that can drive policy which can be seen from the example case of Determination of Ahok (Jakarta governor candidate) as a suspect originated from the videos uploaded by Buni Yani (after editing). The case is the greater given the ongoing debate in cyberspace. In fact, the virtual world is used to plan and recruit a large mass demonstration.

The extremists use the internet to create a group to fight for the goal. In terms of cybercrime, this page is called hate sites. When translated loosely, then hate sites is one of the cybercrime utilizing internet sites as a means to channel resentment. The site is often used to attack each other and say some rude and vulgar managed by extremists [3]. Hate sites are used for religious insult and glorify the extremist teachings. These sites become a window in a criminal act of terrorism.

2. RESEARCH METHOD

This study is normative legal research, which examines the basic authority for the government to shut down negative content in cyberspace [5-7]. A broad range of malicious actions in cyberspace is routinely described as cyberwar. The identity of those who engage in these actions can be uncertain, and their intent is often ambiguous. This normative legal research examined library materials or secondary data that includes primary legal materials and secondary legal materials. Primary legal materials used are:

- The Constution of Republic of Indonesia of 1945 [8],
- The Act Number 8 of 1981 concerning Criminal Procedure Code [9],
- Act Number 11 of 2008 concerning Information and Electronic Transaction [10],
- Act Number 19 of 2016 concerning Act Number 11 of 2008 concerning Information and Electronic Transaction [1].

Secondary legal materials used are appropriate literature to the problems discussed in this study.

The collection of legal materials was done through literature covering the primary legal materials, in the form of legislation and secondary sources, such as literature books of jurisprudence and other legal writings relevant to the problems. The present study was conducted through the literature data sources identification stage, identification and inventory of legal materials. Analysis of legal materials was made qualitatively. The discussion is presented in the form of descriptive analysis.

3. RESULTS AND ANALYSIS

3.1 Spreading Hatred and Hostility in Cyberspace

In human life, there are many reasons can be put forward as the cause of a change in society, but a change in the application of the results of today's modern technology widely touted as one of the causes for social change. Advance in technology not only helps people to do their daily work or do business, but also assists law enforcement to uncover a crime. Some of the methods and results of the technology are used in exposing the crimes of which CCTV, interception, recording and so on.

Activities through electronic media system, also called cyber space, although it is virtual can be categorized as an act or a real legal act. Legally activities in cyber space can not be approached with the size and qualifications of conventional law only, because if this will be too much trouble and things that pass from the law. Activity in cyber space is a virtual activity which gives very real impact though the evidence is purely electronic appliance. The virtual space is used to commit a crime.

In terminological crimes based on information technology by using computer media as today, can be called in many phrases, namely computer misuse, computer crime, computer fraud, computer abuse, computer-related crime, computer-assisted crime or cyber crime. In Convention on Cybercrime mentioned some actions included in the cyber crime, namely:

1) Offences against the confidentiality, integrity and availability of computer data and systems.
a. Illegal access
b. Illegal interception
c. Data interference
d. System interference
e. Misuse of devices
2) Computer-related offences
a. Computer-related forgery
b. Computer-related fraud
c. Offences related to child pornography
3) Offences related to infringements of copyright and related right [11].

In uncovering cyber crime, there are some things to note that the impact of cyber attacks, identity, or political motivation of the attacker. [12]. The debate on tribe, race, religion and inter-group became one of the subjects that are often discussed on the Internet. In Indonesia, the act was usually preceded by a topic that raised the issue of religion. Proselytes one would argue with adherents of other religions of the truth of his religion. The debate is done by reviewing the holy verses that form the basis of the argument. In the debate, they did not hesitate to insult other religious teachings, and asked people to feud with other religions though such actions violate the law. Article 28 paragraph (2) of Act Number 11 of 2008 states "Every person intentionally and without the right to disseminate information intended to cause hatred or hostility individual and/ or a particular group of people based on tribe, religion, race and intergroup".

Hatred and hostility based on tribe, religion, race and intergroup lead to discrimination. Racial and ethnic discrimination are all forms of distinction, exclusion, restriction, or selection based on race and ethnicity, which lead to the removal or reduction of the recognition, acquisition, or exercise of human rights and fundamental freedoms in an equality in the field of civil, political, economic, social and culture. Elimination of racial and ethnic discrimination carried out under the principles of equality, freedom, justice, and human values are universal. Elimination of racial and ethnic discrimination aimed at creating kinship, brotherhood, friendship, peace, harmony, security, livelihood and life among citizens which are basically always coexist.

Performed works by Priscilla Marie Meddaugh and Jack Kay [13], Alexander Brown [14] hatred and hostility as hate speech and declare supremacist discourse situated in cyberspace varies from traditional hate texts in distinctive ways. Therefore, Brown suggests there are some special things about online hate speech that include anonymity, invisibility, community, instantaneousness, and harm [14].

Hatred and hostility based on tribe, religion, race and intergroup can be cyber terrorists, that is the act of terrorism committed in cyberspace. Lewis who defines cyber terrorism as the use of computer network tools to shut down critical nation-Infrastructures (such as energy, transportation, government operation) or to coerce or intimidate a government or civilian population [15]. In the virtual world, cyber criminals and cyber terrorists use a computer as a tool to target other computers. Terrorists launch their attacks by using various methods. The result of some attacks does not only remain in the virtual world, but also impacts real life by the destruction of property or the loss of life. [16].

Internet media is used by extremists to carry out terror, recruit members and commit acts of terrorism. Spreading hatred is made freely through the recruitment of members in the organization of society. Spreading hatred and radicalization is no longer sporadic and closed. The statement was made publicly, through social media or video that is uploaded by the perpetrator intentionally. The statement was made publicly by presenting ideologies espoused by the group. The group did it openly and designate targets of the

action crime. Victims of hate crimes are not randomly at tacked by offenders, they are specifically picked out. Their ethnicity, sexual orientation or race is not merely a demographical statistic in connection with the crime, but it is the reason for their victimisation. This not only has a deep and long lasting impact on the victim, but also on their community and the wider community around them [17].

The hatred spreads more easily thanks to the technological sophistication. Extremist uses social media and their website to provide doctrines which are considered true by the group. Recruitment has constantly done, even the extremist group has a large political force and earn a place in society. They saw her as a hero who will direct the people, whereas the dissidents must be destroyed. This radicalism can be done for a legal vacuum is not spreading hatred as an act of terrorism. As a result, recurring acts of terrorism.

3.2 Legality Government to Close Spreading Hatred and Hostility

The growth of the Internet leads to concerns about its potential impact, including cyberhate [18]. Cyberspace is a place to express their opinions and thoughts. Everyone has the freedom of expression and information, which this freedom is part of human rights as stated in Article 3 of the Universal Declaration of Human Rights states "Everyone has the rights to life, liberty and security of person" and in Article 19 Universal Declaration of Human Rights states "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and Regardless of frontiers" [19]. This freedom does not hold up, so their use is limited by the provisions of the law (restriction by law) as contained in Article 19 International Covenant on Civil and Political Rights which states:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in point above carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (ordre public), or of public health or morals [20].

In Indonesian legislation, freedom of expression is a human right which is guaranteed by the constitution. In Article 28 E Paragraph (3) of the Constitution of 1945 stated "Everyone has the right to freedom of association, assembly, opinion and expression" [8]. Article 28F also stated "Everyone has the right to communicate and obtain information to develop personal and social environment, as well as the right to seek, obtain, possess, store, process and convey information by using all available channels" [8]. Electronic information is one or a set of electronic data, including but not limited to text, sound, pictures, maps, plans, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed that has meaning or can be understood by people who are able to understand.

Submission of electronic information also involves the right to privacy. As an expert in telecommunications law. Usually, personal information is presumed to be owned by its subject. Based on this idea, the Organisation for Economic Co-operation and Development (OECD) guidelines stipulate the individual participation principle as follows:

An individual should have the right:

(1) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.
(2) To have communicated to him, data relating to him within a reasonable time: (i) at a charge, if any, that is not excessive; (ii) in a reasonable manner; and (iii) in a form that is readily intelligible to him.
(3) To be given reasons if a request made under subparagraphs (1) and (2) is denied, and to be able to challenge such denial.
(4) To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended [21].

Talking about privacy issues on the internet, S.E. Kruck, et al [22] suggests there are three areas that need protection, which includes e-mail privacy, access and security and also personal informational and unsolicited marketing. In 2003, the European Union Court of Justice passed a law clarifying regulations with respect to publications containing defamatory or embarrassing contents. The European Court of Justice ruled that the posting of personal information, images or video clips of others without their consent violates laws based on the EU 1995 European Data Protection Directive, although it excludes some activities such as journalism. [23]. Photos and videos can be objects used by offenders to spread hatred. Such actions certainly invade personal privacy

Freedom of expression and gain access to information is a human right. States have an obligation to protect and fulfill the human rights, but that does not mean the country does not have the authority to restrict the rights of expression and gain access to information. State may restrict such rights outside the law and the values espoused by Indonesian nation. Restriction of rights by the state under Article 28J paragraph (2) of the Constitution of 1945 in Article 28J paragraph (2) of the Constitution of 1945 [8] stated as follows:

> *In carrying out the rights and freedom of every person shall be subject to the restrictions established by law with the sole purpose of securing due recognition and respect for the rights and freedoms of others and to meet the demands of a fair in accordance with considerations of morality, religious values, security and public order in a democratic society.*

In the Act Number 19 of 2016 concerning amendment to The Act Number 11 of 2008 concerning Information and Electronic Transaction [1], there are provisions regarding the role of government. Such provisions strengthening the role of government in providing protection from any kind of interference from the misuse of information and electronic transaction by inserting additional powers to the provisions of Article 40 which states:

(1) The Government will facilitate the use of Information Technology and Electronic Transaction in accordance with the provisions of the legislation.
(2) The Government protect the public interest from any kind of disruption as a result of misuse of Electronic Information and Electronic Transaction disturbing public order, in accordance with the provisions of the legislation.
(2a) The Government shall take preventive dissemination and use of Electronic Information and/ or Electronic Documents which have a charge which is prohibited in accordance with the provisions of the legislation.
(2b) in the prevention as referred to in paragraph (2a), the Government is authorized to terminate the access and/or instruct the Electronic System Operator to terminate access to the Electronic Information and/or Electronic Documents which have a charge of violating the law.
(3) The government set the agency or institution has the strategic electronic data that must be protected.
(4) The agency or institution referred to in paragraph (3) shall make the Electronic Document and electronic backups and connect to a specific data center for data security interests.
(5) The agency or institution other than provided for in paragraph (3) create electronic documents and electronic backup in accordance with its data protection purposes.
(6) Further provisions on the role of Government as referred to in paragraph (1), paragraph (2), paragraph (2a), paragraph (2b), and paragraph (3) shall be regulated by government regulation [1].

The government is obliged to prevent the dissemination of electronic information that has a charge which is prohibited. The government is authorized to terminate the access and/ or instruct the Electronic System Operator to terminate access to electronic information that has a charge of violating the law. The prohibition against electronic information that shows hatred and hostility on the basis of legal interest. The interests of law is the basis for providing legal protection. In managing the virtual space, the government can do international cooperation. Sundaresh Menon and Teo Guan Siew [24] declare “a multilateral platform can set the stage for a joint international effort to promulgate common standards and key principles that govern international co-operation”.

Individual legal interests that became the basis of the authority of the government to shut down electronic systems that contain electronic information is the right to security. The right to security includes the rights that are protected physically and psychologically. One form of the right to security is the right to protection. Sanctuary meant the protection of self, family, honor, dignity and property, including the right to

recognition before the law as a private man. Hatred and hostility on the basis of religion, ethnicity, race and intergroup can threaten the safety of minorities.

Indonesian society is a multicultural society. The dissemination of hatred and hostility will cause conflicts in society. Action radicalism basically it is a phenomenon of religions. Based on historical search, this phenomenon is a phenomenon that is common in many religions, both of which can lead to religious violence or not. These relations occur directly or indirectly, that radicalism is always dealing with inter-religious anarchism. A fact that can be observed is that the radicalism associated asymmetrically with various dynamics of violence in every variation. Violence has a symbolic style and actual complexion. In theory, symbolic violence can occur in a society when there are groups that are directly or indirectly started using the symbols of language or discourse that causes discomfort in inter-religious tolerance. Instead, the actual anarchism can happen when a group of religious communities use power to force others to do something that is in accordance with her wishes. Violence can be done by the majority or minority, depending on the causes of the trigger.

Virtuality characteristics of cyberspace allows illegal content such as inciting hatred or hostility based on ethnicity, religion, race, and class, accessible, distributed, transmitted, copied, stored for disseminated back from anywhere and at anytime. In order to protect the public interest from any kind of disruption as a result of misuse of Electronic Information and Electronic Transaction, requires assertion Government's role in preventing the dissemination of illegal content to take action to cut access to Electronic Information and/or Electronic Documents which have a charge of unlawful so inaccessible Indonesia's jurisdiction and authority necessary for investigators to request information contained in the Electronic System Operator for the benefit of law enforcement crime in the area of information Technology and Electronic Transaction.

The authority of the government to restrict the electronic information in the virtual world aimed at preventing disintegration. The debate is motivated by differences in tribe, religion, race and intergroup would lead to conflict in society. The conflict would destabilize security. Disruption will affect the security and stability systemically to economic growth, stock prices, excursions and so forth. On the basis of the interests of the nation, the government has no legality to terminate the access and/ or instruct the Electronic System Operator to terminate access to electronic information that has a charge of violating the law.

In protecting the interests of the law, the government through law enforcement can impose sanctions for any person knowingly and without the right to disseminate information intended to cause hatred or hostility individual and/or a particular group of people based on tribe, religion, race, and groups. Pursuant to Article 45A paragraph (2) of The Act Number 19 of 2016, Any person who intentionally and without the right to disseminate information intended to cause hatred or hostility individual and/or a particular group of people based on tribe, religion, race and intergroup (SARA) as referred to in Article 28 paragraph (2) shall be punished with imprisonment of 6 (six) years and/or a fine of 1,000,000,000.00 (one billion IDR).

In the criminal procedure law applies fundamental principles, namely: *lex scripta* (criminal procedure code should be in writing, due to the nature keresmiannya), *lex certa* (criminal procedure code should be written clearly), *lex stricta* (interpretation of the law of criminal procedure should be carried out strictly). Suhariyanto [25] interpreting Article 28 paragraph (2) of Act Number 11 of 2008 concerning Information and Electronic Transaction as follows:

> *It needs two conditions that may occur in accordance with the text in the formulation of the article, which can be perpetrators of spreading information is not intended to provoke, but in reality such information may provoke the form creates a feeling of hatred and hostility, as well as journalists socio-political motivation initially just wanted to spread information without provoking purposes. If such circumstances, whether journalists can be imprisoned in this chapter? Obviously this will depend on the evidence in the trial. The second condition may be the opposite, ie spreading information aimed at spreading the provocation, then he wants to inflict hatred and hostility, but the reality on the ground this does not happen* [25].

Legal actions in the virtual world has a huge impact, it is because the access is not limited by space and time. Therefore necessary enforcement strategy to reduce the impact of information containing hate and

hostility. Government authority to terminate the access and/ or instruct the Electronic System Operator to terminate access to electronic information that has a charge of unlawful aimed at preventing a larger conflict.

3.3 Electronic Evidence in Spreading Hatred and Hostility

The law regulates all aspects of life in society. Frank basically says that the law must be characterized by liquid (fluidity) and bending (pliancy), because the legal issues are constantly evolving and difficult to predict demand laws to constantly adapt themselves to the realities of social, industrial, technological and political continually changed, so the law must not be permanent character, experimental and can not be calculated exactly. Issues of tribe, religion, race and inter-group becomes a problem in criminal law in Indonesia. This is not out of the condition of the pluralism of Indonesian society. Conflict discrimination against certain people can threaten the integrity of the state and nation. Enforcement of criminal law is always in contact with moral and ethical. Crimes are acts which violate the society's collective conscience; they violate its moral code, and this violation produces a punitive reaction. To put it another way, crimes are seen as moral outrages which lead to a demand that they be punished. [26]

The Act concerning Information and Electronic Transaction applicable in the territory of Indonesia based on the principle of territoriality. Based on this principle, any person who spread hatred and animosity, not limited to the Indonesian citizens and foreign citizens can be imprisoned according to the legislation. A very important element in law enforcement against any person who spread hatred and hostility is proof. In the criminal procedure law, the provision of evidence can be seen in Article 184 paragraph (1) Act Number 8 of 1981 concerning Criminal Procedure Code that:

Valid evidences are: a. witness statements; b. expert testimony; c. letter; d. instructions; and e. testimony of the defendant. Judging from the evidence as stipulated in the Criminal Code, the electronic information can be classified as a guide. Article 188 outlines the evidence leads, which is as follows:

(1) Directive is actions, events or circumstances, which is due to correspondence, both between one another, as well as the criminal act itself, indicating that there has been a criminal offense and the perpetrators;
(2) Directive referred to in paragraph (1) can only be obtained from:
   a. witness statements;
   b. letter;
   c. testimony of the defendant.
(3) An assessment of the strength of evidence of a hint in each particular state is done by the judge wisely more prudent after he entered the examination with full accuracy and thoroughness based on conscience [9]

Electronic information as evidence confirmed in Article 5 of Act Number 11 of 2008 on Information and Electronic Transaction. According to Article 5 of Act Number 11 of 2008 on Information and Electronic Transaction determined:

(1) Electronic Information and/or Electronic Document and/or prints with a valid legal evidence.
(2) Electronic Information and/or Electronic Document and/or printout referred to in subsection (1) is an extension of the valid evidence in accordance with the Law of Procedure applicable in Indonesia.
(3) Electronic Information and/or Electronic Records declared valid when using the Electronic Systems in accordance with the provisions stipulated in this Law.
(4) Provisions on Electronic Information and/or Electronic Documents referred to in paragraph (1) shall not apply to:
a. letter under the Act must be made in writing; and
b. letter along with the documents that under the Act must be made in the form of notaril deed or deed made by deed officials [10]

Electronic Information and/or Electronic Records is electronic evidence (digital evidence) which is recognized as valid evidence in the procedural law. Legitimacy of Electronic Information and/or electronic documents as evidence can be found in Article 5 of The Act Number 11 of 2008 concerning Information and Electronic Transaction and in some other legislation. In Article 44 of The Act Number 11 of 2008 concerning Information and Electronic Transaction stated:

Evidence in the investigation, prosecution and examination before the court according to the provisions of this Act are as follows:

a. evidence as stipulated in legislation; and

b. other evidence in the form of Electronic Information and/or Electronic Documents referred to in Article 1 number 1 and number 4 and Article 5, paragraph (1), paragraph (2), and paragraph (3). [10]

The existence of Electronic Information binding is recognized as valid evidence to provide legal certainty to the implementation of electronic systems and electronic transaction, particularly in evidence and matters relating to the legal actions carried out through the electronic system. Controlling crime involving digital technology and computer networks will also require a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders [27]. Meanwhile, there are some steps and techniques commonly used when attempting to penetrate a system, presented by [28]. Spreading hatred and radical doctrines have threatened sense of humanism internationally recognized. The main reason for setting the spread of hatred and radicalism acts as criminal acts carried out for the protection of the treatment of a potential offender to society as a whole. Law enforcement against the spread of hatred and hostility made to ensure legal certainty.

4. CONCLUSION

Spreading hatred and hostility in cyberspace, one of which is motivated by differences in ethnicity, religion, race and inter-group. Opinion containing hatred and hostility towards ethnic, religious, racial and inter-group published through the internet. The debate is often conducted through social media. The act is a criminal offense as stipulated in Article 28 paragraph (2) of The Act Number 11 of 2008 [10]. The spread of hatred and hostility that is a crime to use information technology as a facility. To reduce the dissemination of negative content, then the government could shut down electronic information laden hatred and hostility. The legality of the government to cover the content of discrimination provided for in Article 40 paragraph (2) of The Act Number 19 of 2016 [1]. The legality of this government has done to protect the public interest. Electronic evidence in spreading hatred and hostility is a valid legal evidence, including the printout. The evidence consists of evidence in electronic and digital evidence. The government should immediately blocked access to electronic information that spread hatred and enmity to prevent the disintegration.

REFERENCES

[1] The Act Number 19 of 2016 concerning the amendment of The Act Number 11 of 2008 concerning Information and Electronic Transaction (original version in Bahasa Indonesia).

[2] Nick Nykodym, Robert Taylor, Julia Vilela, "Criminal profiling and insider cyber crime," *Digital Investigation*, vol. 2, no. 4, 2005, pp 261-267.

[3] Vasilios Katos, Peter M. Bednar, "A cyber-crime investigation framework," *Computer Standards & Interfaces*, vol. 30, no. 4, 2008, pp. 223-228.

[4] F. Saidi, Z. Trabelsi, K. Salah, and H. B. Ghezala, "Approaches to analyze cyber terrorist communities: Survey and challenges," *Computers & Security*, vol. 66, 2017, pp. 66-80.

[5] P. Pawlak and C. Wendling, "Trends in cyberspace: can governments keep up?," *Environment Systems and Decisions*, vol. 33, pp. 536-543, 2013.

[6] J. A. Lewis, "Cyberwar Thresholds and Effects", *IEEE Security & Privacy*, vol. 9, pp. 23-29, 2011.

[7] Xiaohua Zhu, "The failure of an early episode in the open government data movement: A historical case study," *Government Information Quarterly*, vol. 34, no. 2, 2017, pp. 256-269.

[8] The Constitution of Republic of Indonesia of 1945 (original version in Bahasa Indonesia).

[9] The Act Number 8 of 1981 concerning Criminal Procedure Code (original version in Bahasa Indonesia).

[10] The Act Number 11 of 2008 concerning Information and Electronic Transaction (original version in Bahasa Indonesia).

[11] Convention on Cybercrime, European Treaty Series-No. 185, Budapest, 23.XI, 2001.

[12] Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis, Theodoros Apostolopoulos, "Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare", *Information & Computer Security*, Vol. 24 Issue: 1, 2016, pp.38-52.

[13] Priscilla Marie Meddaugh and Jack Kay, "Hate Speech or "Reasonable Racism?" The Other in Stormfront", *Journal of Mass Media Ethics*, vol. 34, no. 2, 2009, p. 251-268.

[14] Alexander Brown, "What is so special about online (as compared to offline) hate speech?", *Ethnicities Sage Journals*, May 19, 2017 pp. 2-12.

[15] James A. Lewis, 2002, *Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Trategic and International Studies, Washington D.C., p. 1.
[16] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, Hossein Taji, "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime", *Computer Law & Security Review*, Vol. 29, Issue 3, 2013, pp. 207-215.
[17] Jenny Ardley, "Hate Crimes: A brief review", *International Journal of Sociology and Social Policy*, Vol. 25 Issue: 12, 2009, pp.54-66.
[18] Laura Leets "Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace?", *Communication Law and Policy*, Vol. 6, No. 2, 2001, 287-317.
[19] Universal Declaration of Human Rights. UN General Assembly in Paris on 10 December 1948.
[20] International Covenant on Civil and Political Rights. General Assembly resolution 2200A (XXI) of 16 December 1966
[21] Kiyoshi Murata, Yohko Orito, "Rethinking the concept of the right to information privacy: a Japanese perspective", *Journal of Information, Communication and Ethics in Society*, Vol. 6 Issue: 3, 2008, pp.233-245.
[22] S.E. Kruck, Danny Gottovi, Farideh Moghadami, Ralph Broom, Karen A. Forcht, "Protecting personal privacy on the Internet", *Information Management & Computer Security*, Vol. 10 Issue: 2, 2002, pp.77-84.
[23] J. Alberto Castañeda, Francisco J. Montoso, Teodoro Luque, "The dimensionality of customer privacy concern on the internet", Online Information Review, Vol. 31 Issue: 4, 2007, pp.420-439,
[24] Sundaresh Menon, Teo Guan Siew, "Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation", *Journal of Money Laundering Control*, Vol. 15 Issue: 3, 2012, pp.243-256.
[25] Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya (Information Technology Crime (Cyber Crime) Setting Urgency and Legal Gap)*, Raja Grafindo Persada, Jakarta, p. 177-178.
[26] Ian Marsh, John Cochrane and Gaynor Melville, 2004, *Criminal Justice An introduction to philosophies, theories and practice*, Routledge, London, p. 30.
[27] Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime", *Policing: An International Journal of Police Strategies & Management*, Vol. 29 Issue: 3, 2006, pp.408-433.
[28] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," *International Journal of Online Engineering*, vol. 13, pp. 125-132, 2017.

BIOGRAPHIES OF AUTHORS

I Gede Yusa, was born in Klungkung July 20, 1961. The author is a lecturer of Constitutional Law at the Faculty of Law Udayana University since 1985. He was Chairman of Constitutional Law Section in 2006-2010 and 2014-2016. Being Vice Dean student affair of the periode 2016-2020. The author is also the Chairman of the Association of Lecturers Constitutional Court Procedural Law (APHAMK) Bali Province from the 2010 until now. The author graduated from S3 in Universtas Brawijaya, Malang in 2011. He is able to contacted at gedeyusa@rocketmail.com.

Dewi Bunga, was born in Denpasar, February 8, 1987. The author graduated from LLB and LLM in the Legal Studies Program Udayana University as the best graduates. Since 2015, the author became a permanent lecturer in criminal law at the Faculty of Dharma Duta, Denpasar State Hindu Dharma Institute. The author is active in various legal research activities. Some of her works have been awarded at national and international levels. The author provides legal counseling and legal consultations to the public, either through seminars, TV, radio, or on various occasions. The author can be contacted via email bunga8287@gmail.com.

Deris Stiawan holds Ph.D from Universiti Teknologi Malaysia in 2013. He is senior lecturer in Faculty of Computer Science, Universitas Sriwijaya, Indonesia. Deris is a senior member of IAES, member of IEEE, MALTESAS, IAENG and his professional profile has derived to computer and network security fields, focused on network attack and intrusion prevention/detection system. In 2011, He holds Certified Ethical Hacker (C|EH) & Certified Hacker Forensic Investigator (C|HFI) licensed from EC-Council USA.