RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

The Functional Police Criminalistics Laboratory in Handling Hate Speech Crimes in Cyberspace

M.Wildan Sofi Ega Musthofa[*)]

[*)] Faculty of Law, Universitas Islam Sultan Agung Semarang, Indonesia, E-mail: wildanofa1325@gmail.com

Abstract. *The purpose of this research is to identify, examine and analyze digital forensics arrangements in proving criminal acts of hate speech in cyberspace, and the role of the National Police's criminal laboratory in cases of criminal acts of cyber-hate speech in the judicial process. The approach method used in this paper is normative juridical. The specification of this writing is descriptive analytical. Actions or crimes that need serious attention at this time are Hate Speech. Act No. 19 of 2016 concerning amendments to Act No. 11 of 2008 concerning Information and Electronic Transactions (ITE) is a lex specialis of the Criminal Procedure Code (KUHAP), because the ITE Law regulates new evidence which is an expansion from conventional evidence. Since 2000, it has been one of the beginnings of developing digital forensic capabilities at the Puslabfor Bareskrim Polri Headquarters. Highly inconsistent characteristics of electronic evidence, then electronic evidence cannot be directly used as evidence in a cybercrime case. Therefore we need a standard so that electronic evidence can be used as evidence in trials, namely by carrying out digital forensics. The use of digital forensics in the Criminalistics Laboratory of the National Police against electronic evidence is important to be carried out in a crime, especially ITE crimes.*

Keywords*: Criminalistic; Cyberspace; Hate; Speech.*

1. Introduction

Law enforcement is one of the efforts to create order, security and peace in society, especially prosecution after a violation of the law. Proof is the main thing in examination and prosecution after a criminal case has occurred.[1]This is because

[1]Dwi Fahri Hidayatullah, Gunarto, and Lathifah Hanim. Police Role in Crime Investigation of Fencing Article 480 of the Criminal Code (Study in Polres Demak). Journal of Sovereign Law Volume 2 Issue 4, (2019), p.457

through the stages of proof there is a process, method, act of proving to show the right or wrong of the defendant in a criminal case, especially in court proceedings.

In dealing with criminal cases that are not supported by at least two valid pieces of evidence, it is difficult for law enforcement officials to prove guilt or innocence

suspect/defendant. The process of investigation and investigation of criminal acts at the present time has progressed a lot with the development of modern science and technology. One of the impacts of the development of science and technology on the investigation and investigation of criminal acts is the establishment of a criminal laboratory.[2]

The Polri Criminalistics Laboratory is part of the Polri organizational structure which has the task or function of being a supervisor, executor of criminalistics or forensics, as a science whose application is to provide technical support in the investigation/investigation of criminal acts.[3] This is done through examination of evidence in a criminalistic laboratory as well as technically criminalistic examinations at the crime scene, in line with developments in reform and advances in science and technology.

The issue of hate speech has recently received more attention, both among the government, law enforcement and the community. The perpetrators of this crime did not only involve the lower middle class (society in general), but also involved figures or leaders in the community as well as users of social media facilities (social networks) in cyberspace networks (cyber space/cyber world) in Indonesia. As a social network is a website that allows users to build connections and relationships with other internet users.[4]

Electronic evidence has unique characteristics which are invisible, very fragile because it is easy to change, easy to damage because it is sensitive to time, easy to destroy, and easy to modify (engineering). In addition, electronic evidence can also be moved easily, and if you want to view or read it, you need the help of tools, both hardware and software. Seeing the very inconsistent characteristics of electronic evidence, electronic evidence cannot be directly used as evidence in a cybercrime case. Therefore we need a standard so that electronic evidence can be used as evidence in trials, namely by carrying out digital forensics.

[2]Abdussalam, 2006, Forensic Smart Book (Scientific Evidence), Jakarta: Restu Agung, p. 1
[3]Yeremias Tony Putrawan, Jawade Hafiz, and Aryani Witasari. Crime Investigation of the Trade of the Human Body Organs on Criminal Investigation Police (Case Study Police Report Number: LP / 43 / I / 2016 / Bareskrim dated 13 January 2016), Jurnal Daulat Hukum Volume 2 Issue 4, (2019), p.654
[4]Sinta Dewi Rosadi. 2015, Cyber Law; Aspects of Data Privacy According to International, Regional and National Laws. Bandung: Refika Aditama, p.7.

The aim of the author's research is to know, study and analyze digital forensics arrangements in proving criminal acts of hate speech in cyberspace, and the role of the Criminal Laboratory of the National Police in criminal cases of cyber hate speech in the judicial process.

2. Research Methods

To conduct an assessment in this writing the authors use the normative juridical method. Writing specifications are carried out using a descriptive analytical approach. The data used for this writing is secondary data. To obtain the data in this writing, secondary data collection methods were used which were obtained from library books, laws and regulations, as well as the opinions of legal experts. The data that has been obtained is then analyzed with qualitative analysis.

3. Results and Discussion

3.1. Setting Digital Forensics in Proving Hate Speech Crimes in Cyberspace

In the Circular Letter of the Chief of Police Number SE/6/X/2015 it is explained that hate speech can be in the form of criminal acts regulated in the Criminal Code (KUHP) and other criminal provisions outside the Criminal Code, which include insults, defamation good name, defamation, provoking, inciting, spreading false news. All of the above actions have the purpose or could have an impact on acts of discrimination, violence, loss of life, and/or social conflict; Furthermore, in letter (g) it is stated that hate speech is aimed at inciting and creating hatred against individuals or groups of people, in various communities that are differentiated from the aspects of ethnicity, religion, religious sect, belief or belief, race, inter-group, skin color, ethnicity, Gender, People with disabilities (disabilities), Sexual orientation.

In letter (h) it is stated that hate speech can be carried out in various media, such as in speeches on campaign activities, banners or banners, social media networks, conveying opinions in public (demonstrations), religious lectures, print and electronic mass media. , pamphlet.

As for the criminal construction in the regulation of Act No. 11 of 2008 concerning Information and Electronic Transactions, namely:

a. Article 28
    1) "Every person intentionally and without right spreads false and misleading news that results in consumer losses in Electronic Transactions".
    2) "Everyone intentionally and without rights disseminates information aimed at creating feelings of hatred or hostility towards certain

individuals and/or groups of people based on ethnicity, religion, race and inter-group (SARA)".

b. Article 45 paragraph (2)
"Anyone who fulfills the elements referred to in Article 28 paragraph (1) or paragraph (2) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 1,000,000,000.00 (one billion rupiah)".

Many digital forensic process models and methods have been developed by forensic practitioners and investigators, based on personal experience and expertise, on an ad hoc basis to achieve standardization at the crime scene. However, there is currently no standard formalizing the digital forensic investigation process, although efforts to standardize the process have started within the International Standardization Organization (ISO). Digital forensic investigations, hereinafter referred to as Digital Forensics Investigations (DFI), are the phases of linking extracted information and digital evidence to construct factual information for review by judicial institutions.[5]

In the digital and electronic world, the original evidence is not analyzed, which is why this evidence must be preserved. This is different from dissecting a victim's body. The term electronic evidence in Indonesia was introduced in 2001 with the emergence of electronic evidence in Article 26A of Act No. 20 of 2001 concerning Amendments to Act No. 31 of 1999 concerning Eradication of Corruption Crimes. Since then, almost all laws which regulate procedural law also contain rules which recognize the use of electronic evidence as evidence in trials, especially with the promulgation of Act No. 11 of 2008 concerning Electronic Information and Transactions.[6]This is explained in Article 5 Paragraph (1) of the ITE Law that: "Electronic Information and/or Electronic Documents and/or printouts are valid evidence". In Article 1 of Act No. 19 of 2016 it is explained in more detail the types of electronic evidence in the form of Electronic Information and Electronic Documents, including:

1) Electronic Information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mall), telegram, telex, telecopy or the like, letters, processed signs, numbers, access codes, symbols or perforations that have meaning or can be understood by people who are able to understand them.
2) Electronic Transactions are legal actions carried out using computers, computer networks, and/or other electronic media.

[5]0M.Nur Faiz, Comparative Study of Digital Forensic Investigations in Criminal Acts, Journal of INISTA. Vol 1 No 1, (2018), p.64
[6]Dewi, Mira Nila Kusuma, Legal Standing on Deed of Minutes of General Meeting of Shareholders (GMS) Through Electronic Media, Arena Hukum Journal, Volume 9 Number 1, (2016), p.122

3) Information Technology is a technique for collecting, preparing, processing, announcing, analyzing, and/or disseminating information.
4) Electronic Documents are any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or the like, which can be seen, displayed, and/or heard through a computer or Electronic System, including but not limited to in writing, sound, pictures, maps, plans, photographs, or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be understood by people who are able to understand them".

3.2.The Role of the National Police Criminal Investigation Laboratory in Cybercrime Hate Speech Cases in the Judicial Process

There are various stages in the digital forensics implementation process which can be broadly classified as follows:

1) Electronic Evidence Identification
   This is the earliest stage in digital forensics. At this stage identification is carried out where the evidence is located, where the evidence is stored and how it is stored to facilitate the next stage. Electronic media that can be used as evidence includes a computer system, storage media (such as flash drives, pen drives).
2) Electronic evidence storage
   Including to the most critical stage in forensics. At this stage, electronic evidence may be lost due to poor storage. This storage emphasizes that electronic evidence at the time it is found will remain, not change in form, content, meaning and so on in the long term. This is the ideal concept of electronic evidence storage.
3) Electronic Evidence Analysis
   Evidence that has been obtained is necessaryexplored back into a number of scenarios related to the act of investigation. This includes metadata checking. Most files have metadata that they contain added information about the file such as computer name, total edit time, number of editing sessions, where it was printed, how many times it was saved, date and time of modification. Then perform recovery by restoring deleted files and folders, unformat drives, re-create partitions, restore passwords, reconstruct web pages that have been visited, restore deleted emails and so on. The stages of analysis are divided into two, namely media analysis and application analysis on existing evidence.
4) Presentation
   Is a trial process where electronic evidenceauthentication and correlation will be tested with existing cases. The presentation here is in the form of showing electronic evidence related to the case being tried. The

presentation is made by presenting and explaining in detail the investigation report with evidence that has been analyzed in depth and can be accounted for in general in court. The reports presented must be cross-checked directly with the witnesses present, both witnesses who are directly or indirectly involved.[7]

The criminalistic laboratory develops evidence provided by digital development to deepen scientifically, which shows an effort to investigate whether the defendant's actions fall within the criminal element within the scope of hate speech crimes or not. The results of the investigation effort provide authentic evidence that can be used by the Public Prosecutor to be presented before the court to be considered by the judge.[8]

The forensic laboratory also brought out a statement from a digital forensic expert to provide a statement of his testimony with scientific expertise in the field of digital forensics to analyze electronic evidence in order to strengthen the judge's decision fairly and have legal certainty in accordance with the provisions of the law charged with the accused of hate speech throughout the world virtual.[9]

In digital forensics, there are certain principles that must be followed to ensure that electronic evidence can be guaranteed to be authentic and acceptable in court, including:

1) Basic/first principle
   A law enforcement agency and/or its officers are prohibited from modifying digital data stored in an electronic storage mediumwill be brought and accounted for in court. Storage media such as hard disks, floppy disks and flash drives, which are evidence, must be kept intact according to the Chain of Custody principle. The goal is that the electronic information stored on the media remains intact until it is brought to trial, and that its origin can be accounted for, especially from the manipulation of digital data.
2) Second principle
   A forensic analyst or forensic expertwill check and analyzing an electronic evidence must have clear authority, both formally and informally. That way, it is hoped that they can explain technically and practically their reasons for taking actions against the evidence storage media.
3) Third principle
   In the process of examining and analyzing the evidence storage media, there are technical and practical notes of the steps implemented, so that

[7]Hwian Christianto, The Norm of Unity as a Boundary for Criminal Acts of Spreading Hate Speech Through the Internet, Veritas et Justitia, Volume 6 Number 1, (2020), p.94
[8]Edwin Pardede, Criminal Law Policy in Efforts to Enforce the Criminal Act of Defamation Through Twitter. Diponegoro Law Journal, Volume 5 Number 3, (2016), p.356
[9]Reydi Vridell Awawangi, Defamation in the Criminal Code and According to Law no. 11 of 2008 concerning electronic transactions, Lex Crimen Vol. III No. 4, (2014), p.268

when a third party examines the evidencewill get the same results as the forensic analysis has done.

4) Fourth principle
   A person who is responsible for case investigations, examinations and analysis of electronic evidence must be able to ensure that the process is carried out in accordance with applicable law and the previous basic principles and can be implemented properly. This is intended so that the results of the examination and analysis of electronic evidence do not contradict the applicable positive law so that they can be technically and legally accepted by the panel of judges at trial.[10]

The legal basis for using electronic evidence in court has become clearer after Law no. 19 of 2016 concerning electronic information and electronic transactions (UU ITE) Article 28 paragraph (1) and (2), UU ITE Article 5 paragraph (1) and (2) concerning print out (printed results) as legal evidence. Article 5 paragraph (3) of the ITE Law states that the validity of this electronic evidence is recognized by the judge when using an electronic system in accordance with the provisions stipulated in Article 16 paragraph (1) of the ITE Law. Article 43 paragraph (3) of the ITE Law which states that "Searches and/or seizures of electronic systems related to alleged criminal acts must be carried out with the permission of the Head of the local District Court".

4. Conclusion

Article 5 Paragraph (1) of the ITE Law has regulated Electronic Information and/or Electronic Documents as valid evidence, apart from Article 184 of the Criminal Procedure Code which has regulated valid evidence consisting of witness statements, expert statements, letters, instructions, and testimony of the accused. The criminalistic laboratory develops evidence provided by digital development to deepen scientifically, which shows an effort to investigate whether the defendant's actions fall within the criminal element within the scope of hate speech crimes or not. The results of the investigation effort provide authentic evidence that can be used by the Public Prosecutor to be presented before the court to be considered by the judge.

5. References

0M.Nur Faiz, Comparative Study of Digital Forensic Investigations in Criminal Acts, Journal of INISTA. Vol 1 No 1, (2018)

[10]Teguh Prihmono, Umar Ma'ruf, and Sri Endah Wahyuningsih, The Role of the National Police Forensic Laboratory as a Support for Scientific Investigations in the Criminal Justice System in Indonesia, Khaira Ummah Law Journal, Vol. 13. No. 1 (2018), p.227

Abdussalam, 2006, Forensic Smart Book (Scientific Evidence), Jakarta: Great Restu

Dewi, Mira Nila Kusuma, Legal Standing on Deed of Minutes of General Meeting of Shareholders (GMS) Through Electronic Media, Arena Hukum Journal, Volume 9 Number 1, (2016)

Dwi Fahri Hidayatullah, Gunarto, and Lathifah Hanim. Police Role in Crime Investigation of Fencing Article 480 of the Criminal Code (Study in Polres Demak). Journal of Sovereign Law Volume 2 Issue 4, (2019)

Edwin Pardede, Criminal Law Policy in Efforts to Enforce the Criminal Act of Defamation Through Twitter. Diponegoro Law Journal, Volume 5 Number 3, (2016)

Hwian Christianto, The Norm of Unity as a Boundary for Criminal Acts of Spreading Hate Speech Through the Internet, Veritas et Justitia, Volume 6 Number 1, (2020)

Reydi Vridell Awawangi, Defamation in the Criminal Code and According to Law no. 11 of 2008 concerning electronic transactions, Lex Crimen Vol. III No. 4, (2014)

Sinta Dewi Rosadi. 2015, Cyber Law; Aspects of Data Privacy According to International, Regional and National Laws. Bandung: Refika Aditama

Teguh Prihmono, Umar Ma'ruf, and Sri Endah Wahyuningsih, The Role of the National Police Forensic Laboratory as a Support for Scientific Investigations in the Criminal Justice System in Indonesia, Khaira Ummah Law Journal, Vol. 13. No. 1 (2018)

Yeremias Tony Putrawan, Jawade Hafiz, and Aryani Witasari. Crime Investigation of Trade of The Human Body Organs on Criminal Investigation Police (Case Study Police Report Number: LP / 43 / I / 2016 / Bareskrim dated 13 January 2016), Daulat Hukum Journal Volume 2 Issue 4, (2019)