RECONSTRUCTION OF THE LEGALITY OF ELECTRONIC EVIDENCE IN THE INDONESIAN CRIMINAL JURISDICTION SYSTEM

Joko Sriwidodo
Dosen Tetap Pascasarjana Magister Ilmu Hukum
Universitas Jayabaya Jakarta
Email.jokosriwidodo@ymail.com

ABSTRACT

Electronic commerce is a broad concept covering every commercial transaction via electronic that results from and includes such as reproduction, telex, EDI, Internet and telephone. In short, e-commerce can be understood as a trade transaction of both goods and services via electronic media. The development of E-Commerce transactions cannot be separated from the rate of internet growth, because E-Commerce runs through the internet network. This research is a normative legal research conducted through library research (library research). The discussion in this study is that the legality of digital forensic evidence in the criminal procedural law system is to use several parts, including; 1). Digital forensics; and 2). Digital evidence. Also use 1). Computer forensics; 2). Mobile device forensics; 3). Forensic network; and 4). Database forensics. Several court decisions regarding electronic evidence using Law No. 11 of 2008 in conjunction with Law no. 19 of 2016 concerning Electronic Information and Transactions are 1). Prita Mulyasari case; 2). The case of Drs. Subagyo, M.Pd on charges of pornography; 3). Darul Kutni case on the charge of defamation;4). Florence Saulina Sihombing's case on charges of insult and defamation; 5). Grace Megasari Solaiman Case; 6). Riani's case; 7). The Jessica Kemala Wongso case. Some of these cases were cases that included ITE and were decided under the ITE Law.

KEYWORDS:

Electronic Transactions, Transactions, and Criminal

INTRODUCTION

In the settlement of a case in court, the evidentiary procedure is the most important step to prove the truth of an event or a certain legal relationship, or the existence of a right, which is the basis for the plaintiff to file a lawsuit in court. Through the evidentiary stage, the judge will obtain the bases for making a decision in settling a case. The occurrence of various changes caused by the development of the needs of society and the development of this law, affects the legal system prevailing in Indonesia. As it is understood, the legal system in Indonesia was initially oriented towards Continental European countries with civil law systems. This is because as a former Dutch colony, written law in Indonesia has been widely adopted from Dutch law based on the concordance principle, which until now there are still many positive laws. However, in its development, according to the development of society's needs, there has been a shift in the direction of the Indonesian legal system which is no longer fully directed towards Continental Europe with a civil law system, but is a combination with the common law system of the Anglo Saxon.

In the current era of free trade, which is accompanied by rapid advances in technology and industry, it has influenced various business sectors including trade and banking activities. Electronic transactions are increasingly being carried out, especially in the trade and banking sectors. Legal actions are no longer based on concrete, cash and communal actions, but are carried out in a virtual world in an indirect and individual way. This is also influenced by international relations in the era of globalization. As said, the interaction between the provisions of national law and the rules of international law will increase due to the development of international social relations. (Yuda, 2000).

There is an influence of the common law system on legal development in Indonesia. This can be seen from the increasing number of statutory regulations that are carried out partially in accordance with the legal needs of the community, as described above.

Changes have also occurred in the types of evidence that can be used in civil dispute resolution through courts, with the recognition and use of electronic evidence in the community. At the level of formal law, neither the HIR / RBg nor other regulations regarding civil procedures have yet to regulate electronic documents / data as evidence, in other words, the law of evidence in Indonesia has not accommodated the existence of electronic documents / data as evidence. Meanwhile, in its development it is now known that there is electronic evidence (considered as evidence) such as electronic data / documents linked to digital signatures and stamp duty regulations that must be

fulfilled by documentary evidence, witness examination using teleconference, as well as other evidence. such as radio tapes, VCD / DVD, photos, facsimile, CCTV, even SMS short message service system.

RESEARCH METHODS

This research is a normative legal research using normative case studies in the form of legal behavior, for example examining laws. The main point of the study is that the law is conceptualized as an appropriate norm or rule in society and becomes a reference for everyone's behavior. So that normative legal research focuses on the inventory of positive law, legal principles and doctrines, legal findings in inconcreto cases, legal systematic, comparative systems, comparative law and legal history. (Muhammad, 2004).

Based on the explanation above, the authors decided to use normative legal research methods to research and write a discussion of this research as a legal research method. The use of normative research methods in research efforts and conformity theory with the research methods required by the author.

In legal research there are several approaches, with this approach the researcher will get information from various aspects about the problem being tried to find answers. The approach method in this research is the regulatory approach approach (Marzuki, 2008). A normative research certainly has to use an invitation approach, because what will be examined are various legal rules that become the focus of the central theme of a study. Meanwhile, the data analysis carried out in this study was carried out with a qualitative approach that revealed as much data (legal material) as possible so that the problem was more transparent. The qualitative approach allows the researcher to elaborate the data obtained in a comprehensive manner and the results of the description are more accountable.

THEORETICAL FRAMEWORK

Electronic Transactions

The development and advancement of information and telecommunication technology in the midst of the current era of globalization has created the internet media, which is an international network used by millions of people by connecting via computers (Wright, Benjamin & Jane K , 1999). The development of information technology has changed the ways of doing transactions and opened up new opportunities for conducting business transactions (Haris Asnawi , 2004). The development of information technology indirectly causes very fast social changes and causes the world to become without borders. The advancement and development of this technology have unconsciously become an effective means of causing acts against the law. (Ahmad M Ramli , 2003).

In the theory of welfare law, it is stated that the state as the highest organization has the authority to determine the direction of policy in various fields of national life, which means that the participation of the state in determining the direction of policy in the fields of national life, especially in the field of economic law, with the aim of regulating directing activities and life society to conform to the principles of the nation's economy (CST Kansil & Christine Kansil , 2000).

The use of electronic media which is better known as the internet has been chosen by many people because of the various benefits and facilities it can provide, including companies and individuals who can conduct their business transactions in cyberspace without having to have face-to-face meetings in person (Burk , Dan L , 1993). Transactions that occur with possible legal subjects or parties who do not know each other and form a trade agreement that no longer relies on paper media with old shipping facilities, but now can be done in seconds on-line .

The internet is a major revolution in the world of technology, it is a mechanism for disseminating information and a medium for collaborating and interacting between individuals using computers without being hindered by geographic boundaries. The internet is a successful example of an investment, dedication and commitment to a research and development of information infrastructure (Ustadiyanto , 2001). Firmly, the emergence of the internet can be acknowledged and become a new support that facilitates the world of commerce. This fact further encourage and sensitize businesses on the importance of effectiveness and efficiency, so they started to move economic activities towards developing new trading models easier and more practical namely electronic transactions / e-commerce (electronic commerc).

If you look at the definition of e-commerce from ECEG Australia (Electronic Commerce Expert Group) is as follows: "Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, Internet. and the telephone ".

Electronic commerce is a broad concept covering every commercial transaction via electronic that results from and includes such as reproduction, telex, EDI, Internet and telephone.

In short, e-commerce can be understood as a trade transaction of both goods and services via electronic media. The development of E-Commerce transactions can not be separated from the rate of internet growth, because E-Commerce runs through the internet network.

In general, transactions based on paper based transactions are easy to handle because the evidence of the transaction (paper documents) cannot be modified without leaving traces or evidence that can be used to show that the modification has occurred. This is different from electronic transactions. Electronic transactions are part of a legal act carried out using computers, computer networks and / or other electronic media. Electronic transaction includes the contract digital, documents that have legal implications in the hard disk or floppy disk, the command electronic data transfer (eg EFT / Electronic Funds Transfer) messages (data messages) EDI / Electronic Data Interchange, the information on the Website The internet, electronic mail and so on include e-commerce transactions which are basically one form of agreement in electronic form.

The ITE Act

There is a view (Chris Reed , 1996) that the law of proof, including the law of proof in any criminal law system, is a difficult and complex subject of study. " The law of evidence is a subject which presents considerable difficulty and complexity ". This view contains the truth. In the criminal law system, for example, the makers of Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58), hereinafter referred to as the ITE Law, acknowledge that the views regarding the law of evidence as expressed above. In the General Elucidation of the Second Paragraph of the ITE Law, the main problems faced by the legal world are presented, considering that activities carried out through computer systems and communication systems both locally and globally (internet) use information technology based on computer systems, which are electronic systems that can seen virtually. The problem in question is often faced by judges in court to be able to have electronic evidence as evidence to be used in the criminal justice process, when it is related to the delivery of information, communication and / or transactions electronically, especially in terms of proof, evidence and strength of evidence. legal acts which of course also include acts in the field of criminal law, namely, among others, crimes committed through electronic systems, both off-line and connected to telecommunications technology network systems.

The meaning of electronic systems according to the Third Paragraph General Elucidation of the ITE Law is a computer system in a broad sense, which does not only include computer hardware and software, but also includes telecommunications networks and / or electronic communication systems. The complexity faced by the law of proof can be seen from the sophistication of the objects that must be regulated by law, including, of course, the objects that must be regulated by the law of proof. When a crime occurs, the ITE Law stipulates that the crime is related to software or computer programs. The elucidation of the ITE Law contains the formulation that software that cannot be abandoned by law in legal matters of proof is a set of instructions embodied in the form of language, code, schemes, or other forms, which when combined with media that can be read on a computer will able to make a computer work to perform a special function or to achieve a special result, including preparation in designing these instructions.

There is an acknowledgment in the General Elucidation of the ITE Law that so far, the world of law, including the legal world of evidence used in the criminal law system, faces the complexity and complexity of human and community activities in the use of technology which is dominated by virtual nature, namely by path of interpretation.

The ITE Law has stipulated that forced measures that law enforcement officials can use to obtain electronic evidence is through searches and confiscation of Electronic Systems or through interception or wiretapping. Law enforcement officials use searches and confiscation when the investigator clearly knows the source of the electronic evidence (the location of the computer, laptop, USB, server belonging to the suspect, victim or witness). Meanwhile, based on the limitations stipulated in the law, interception or wiretapping can be used by law enforcement officials as a means of collecting information and information related to a criminal act (suspect, suspected criminal act, witnesses, location of the crime); this information can be used as evidence.

Electronic information or electronic documents, if not handled properly, can be changed, damaged or lost. If the information is lost and cannot be recovered, law enforcement officers cannot obtain electronic evidence; if the information is changed or damaged, the information in question cannot be used as evidence at trial. Therefore, law enforcement officials must seek, collect, and analyze information quickly and accurately.

Criminal Justice System

According to (Lloyd E. Ohlin and Frank J. Remington , 2020) argues that the Criminal justice system can be interpreted as the use of a systems approach to the administrative mechanism of criminal justice, and criminal justice as a system is the result of the interaction between statutory regulations , administrative practices and attitudes or social behavior. The understanding of the system itself implies an interaction process that is prepared rationally and efficiently to provide certain results with all its limitations.

Mardjono (2007) provides a limitation that what is meant by the criminal justice system is a crime control system consisting of police institutions, prosecutors, courts, and the correctional facilities for convicted people. Furthermore, it is argued that the objectives of the criminal justice system can be formulated: To prevent people from becoming victims of crime ; Resolving crimes that occur so that the public is satisfied that justice has been served and those guilty are convicted ; Make sure that those who have committed crimes do not repeat their crimes.

DISCUSSION

The Legality of Digital Forensic Evidence in the Criminal Procedure Law Evidence System

The development of information technology and computers (ICT) has progressed very rapidly, especially after the discovery of technology that connects computers (Networking) and the Internet. The increasing use of the internet has had positive and negative impacts on those who use it. From the positive side, the internet can penetrate the boundaries of time and space, where between users and service providers can do various things on the internet, regardless of distance and time difference. Meanwhile, on the negative side, external cultural influences can affect the culture of internet users themselves. Besides that, crime in cyberspace is also inevitable.

Various crimes and crimes involve directly or indirectly information and communication technology. The widespread use of computers, cell phones, e-mail, internet, websites, etc. has invited various malicious parties to commit crimes based on electronic and digital technology. Therefore, recently there is a known science of "computer forensics" or computer forensics, which is needed and used by law enforcement in their efforts to reveal criminal events through the disclosure of evidence based on entities or digital and electronic devices.

From the perspective of the development of crime related to computer networks in the future is increasing. Both in quantity (amount) and quality (level of difficulty of the mode of crime). Of course, this must be balanced with how to resolve a criminal case related to computer networks in the criminal justice system room properly. With the hope that the community as a subject and at the same time a legal object can feel more justice and legal certainty. Related to this problem, the writer tries to analyze the legality of digital forensic evidence (Resa Raditio , 2014) in the criminal procedure law proof system, as according to Resa Raditio divides it into several parts as follows:

Digital Forensics

The definition of digital forensics in simple terms is the whole process of retrieving, restoring, storing, checking information or electronic documents contained in electronic systems or storage media, based on methods and with tools that can be scientifically justified for the sake of proof

In a Digital Forensic investigation the possibilities that will be obtained, namely: Data that has been deleted; information regarding modification times of creation, deletion of files; Can determine which storage devices are connected to a computer; What applications are installed, even if the application has been uninstalled by the user; Which websites have been visited.

Meanwhile, the process in digital forensics generally consists of the following activities: Identification or admissions administration is the recording of evidence to be examined, such as brands, models, serials; Acquisition is the activity of separating hard drives for imaging; Analysis is an activity of analyzing by linking the type of crime with evidence; Reporting is the overall result of activities in written form.

Electronic Information (IE) and Electronic Data (DE) stored in the CPU (Central Processing Unit) to be precise on the hard disk are very important evidence that can unmask a criminal case, but IE and DE have no meaning if they are not understood. "inside". To find out "what's up" on the hard drive, a digital forensic test was carried out. Of course, in this case what must be considered is the security of IE and DE so that they are still intact as the original and the digital forensic test equipment, including the human resources of the testers, have to be legally recognized in the international world.

Digital Forensics Branches

Digital Forensics includes several sub-branches that are concerned with the investigation of various types of devices, media or artifacts.

a. Computer Forensics The purpose of computer forensics is to describe the current state of digital artifacts, such as computer systems, storage media or electronic documents. Disciplines typically include computers, embedded systems (digital devices with basic computing power and onboard memory) and static memory (such as USB pen drives). Computer forensics can handle a wide variety of information, ranging from logs (such as internet history) to actual files on the drive.
b. Mobile Device Forensics Mobile device forensics is a sub-branch of digital forensics that deals with the recovery of digital evidence or data from mobile devices. It differs from Computer forensics in that mobile devices will have an inbuilt communication system (eg GSM) and usually, a proprietary storage mechanism . Investigations usually focus on simple

data such as call and communication data (SMS / Email) rather than in-depth recovery of deleted data. Mobile devices are also useful for providing location information, either from the inbuilt gps / tracking location or via a cell log site, which tracks devices within their range.

c. Forensic Network . Network forensics is concerned with monitoring and analyzing computer network traffic, both local and WAN / internet, for the purpose of gathering information, gathering evidence, or intrusion detection. Traffic is usually intercepted at the packet level, and is either stored for later analysis or filtered in real-time . Unlike other areas of digital forensic data networks are often stable and rarely logged, making the discipline often reactionary.
d. Database Forensics . Database forensics is a branch of digital forensics that deals with the study of database forensics and their metadata. The investigation uses database contents, log files and RAM data to build time-lines or recover relevant information.

Digital Evidence

The existence of evidence is very important in investigating cases of computer crime and computer-related crime because it is with this evidence that investigators and forensic analysts can uncover these cases in complete chronology, to then trace the whereabouts of the perpetrators and arrest them. Because the position of the evidence is very strategic, the investigator and forensic analyst must understand the types of evidence. It is hoped that when he comes to the Crime Scene (TKP) which is related to the case of computer crime and computer-related crime , he will be able to recognize the existence of the evidence for further examination and analysis.

The classification of digital forensic evidence is divided into:

a. electronic evidence. This evidence is physical and can be recognized visually, therefore investigators and forensic analysts must understand so that they can then recognize each of these electronic evidence when they are searching for evidence at the crime scene. Types of electronic evidence are as follows: 1) PC computers, laptops / notebooks, netbooks, tablets ; 2) mobile phones, smartphones ; 3) flash / thumb drive ; 4) floppydisk; 5) hard drive ; 6) CD / DVD 7) router, switch, hub 8) video camera, cctv 9) digital camera 10) digital recorder 11) music / video player.

b. digital evidence. Digital evidence This evidence is digital, which is extracted or recovered from electronic evidence. This evidence is in Law No. 11 of 2008 concerning Electronic Information and Transactions known as electronic information and electronic documents. It is this type of evidence that a forensic analyst must look for and then carefully analyze the relevance of each file in order to uncover the related crime case. With electronic evidence. The following are examples of digital evidence , namely 1) logical files , 2) deleted files , 3) lost files , 4) slack files , 5) log files , 6) encrypted files, 7) steganography files , 8) office files , 9) audio file , 10) video file, 11) image file , 1 2) email, 1 3) user ID and password, 1 4) SMS (Short Message Service), 1 5) MMS (Multimedia Message Service), 1 6) call logs

Court Decisions Concerning Electronic Evidence

The following are several Court decisions related to electronic evidence in Law No. 11 of 2008 Jo Law No. 19 of 2016 concerning Electronic Information and Transactions:

First, the Judgment on Reconsideration No. 225 PK / Pid.Sus / 2011. September 2012 with the Defendant Prita Mulyasari on the charges of Article 45 Paragraph (1) Jo Article 27 Paragraph (3) of the Law of the Republic of Indonesia No. 11 of 2008 (Evidence of one e-mail / electronic mail). Judgment on Reconsideration No. 225 PK / Pid.Sus / 2011 canceled the decision of Cassation No. 822 K / Pid.Sus / 2010. dated June 30, 2011 and freed the Defendant from all charges of the Public Prosecutor, on the grounds that the cassation decision had a clear error from the cassation judge, according to the panel of judges for review, it was proven that the Defendant's act of sending electronic letters to his friends had absolutely no purpose to commit defamation. good, thus the illegal nature of the Defendant's act was not proven legally and convincingly. The Supreme Court's cassation decision previously canceled the decision of the Tangerang District Court and stated that the Defendant was legally and convincingly proven guilty of committing a criminal act intentionally and without the right to distribute and / or transmit and / or make access to electronic information and / or electronic documents that had an offensive content. and / or defamation, as well as imposing a criminal offense against the Defendant with imprisonment for 6 (six) months, provided that such punishment does not need to be served unless the judge's decision is determined otherwise because the Defendant has committed a criminal act before the probation period ends for 1 (one) year. In the case of the decision of the Tangerang District Court No. 1269 / Pid.B / 2009 / PN. Tng. December 29 2009 previously released the Defendant from all charges of the Public Prosecutor, with the consideration that even though the Defendant had sent e-mails to several of his friends with the subject "Fraud Omni International Hospital Alam Sutera Tangerang", including the written sentence "I also inform dr. Hengky. I also practice at RSCM, I don't say RSCM is bad, but be careful with

medical care from this doctor, and Dr. Grace's response, who said he is the person in charge of my complaint, is not professional at all and is not polite and ethical about customer service ". However, the sentence does not contain insulting and / or defamation, because the sentence is a criticism and is in the public interest so that the public can avoid hospital practices and / or doctors who do not provide good medical services to people who are sick who expect recovery. of the disease.

In case of Judicial Review No. 225 PK / Pid.Sus / 2011 Jo Tangerang District Court Decision No. 1269 / Pid.B / 2009 / PN. Tng, it means that the Panel of Judges has put aside electronic evidence in the form of e-mail (electronic mail) addressed to the Defendant to several of his friends - as evidence, in essence, the use of electronic evidence in such a way in bringing the defendant to an unbalanced sense of justice. with the intent and purpose of the Defendant to prepare and send the electronic letter.

Second, the Decision of the Lamongan District Court No. 62 / Pid.B / 2012 / PN. Lmg. dated May 28, 2012 on behalf of the Defendant Drs. Subagyo, M. Pd. with the charges of Article 29 in conjunction with Article 4 paragraph 1 letter e of Law No. 44 of 2008 concerning Pornography in conjunction with Article 64 Paragraph (1) of the Criminal Code, or Article 45 Paragraph (1) Article 27 Paragraph (1) of Law of the Republic of Indonesia No 11 of 2008 Jo Article 64 Paragraph (1) of the Criminal Code, (evidence of 2 units of HP loading pornographic images / photos) . The decision of the Lamongan District Court stated that the Defendant was legally and convincingly guilty of committing the crime of "Making and sending pornography as an ongoing act", and sentenced the Defendant to a 10-month prison sentence. This District Court decision has been upheld by the Surabaya High Court with its decision No. 391 / Pid / 2012 / PT. Sby dated 02 August 2012 and the Supreme Court decision No. 1710 K / Pid.Sus / 2013. January 20, 2014.

Third, the Decision of the Sekayu District Court No. 807 / Pid.Sus / 2013 / PN. Sky. dated 19 August 2014 on behalf of the Defendant Darul Kutni on the charges of Article 45 Paragraph (1) Jo Article 27 Paragraph (3) of Law of the Republic of Indonesia No. 11 of 2008, (Evidence one copy of the print out of the news on line media Radar Nusantara). The decision of the Sekayu District Court stated that the Defendant was legally and convincingly proven guilty of committing a criminal act intentionally and without the right to transmit electronic information and / or electronic documents that had defamation, and sentenced the Defendant to 1 (one) year imprisonment. 3 (three) months and a fine of Rp. 50,000,000, - (fifty million rupiah), provided that if the fine is not paid, it is replaced by a prison for 3 (three) months. This District Court decision was upheld by the Palembang High Court with its decision No. 145 / Pid / 2014 / PT.Plg. 12 November 2014 and by the decision of the Supreme Court No. 1435 K / Pid.Sus / 2015. January 20, 2016.

Fourth, Yogyakarta District Court Decision No. 382 / Pid.Sus / 2014 / PN.Yyk. dated March 31, 2015 on behalf of the defendant Florence Saulina Sihombing on the charges of Article 27 Paragraph (3) Jo Article 45 Paragraph (1) of the Law of the Republic of Indonesia No. 11 of 2008, (evidence of several copies of Twitter capture) . The court ruling stated that the Defendant was legally and convincingly proven guilty of committing a criminal act intentionally and without the right to distribute electronic information through telecommunications networks containing insulting and defamation, and sentenced the Defendant to a 2-month imprisonment provided that the crime was unnecessary. be served, except in the future with the judge's decision determined otherwise because the Defendant was guilty of committing a criminal offense before the probation period ended for 6 months, and a fine of Rp. 10 million if the fine is not paid and replaced with 1 month imprisonment. This District Court decision was upheld by the Yogyakarta High Court in its decision No. 26 / Pid.Sus / 2015 / PT.Yyk. July 28, 2015. The defendant accepted this Yogyakarta High Court decision and did not submit an appeal to the Supreme Court.

Fifth, the Decision of the West Jakarta District Court No. 469 / Pid.B / 2016 / PN. Jkt. Brt dated April 14, 2016 on behalf of the Defendant Grace Megasari Solaiman on the charges of Article 32 Paragraph (1) of Law of the Republic of Indonesia No. 11 of 2008, (Evidence one copy of Independent Audit / Minutes of Stock Opname Inventory of Goods and Proof of Purchase of Goods PT. Diva Sutan Kuliner Bar House Labiere in 2015) The West Jakarta District Court's decision stated that the Defendant was legally and convincingly guilty of committing an act criminal intentionally and without rights or against the law in any way changing an electronic information and / or electronic document belonging to a person, and sentencing the Defendant to imprisonment for 2 (two) years and 6 (six) months and a fine of Rp. 10,000,000, - (ten million rupiah), provided that if the fine is not paid, it is replaced by 1 (one) month imprisonment. This District Court decision was upheld by the DKI Jakarta High Court with its decision No. 204 / Pid / 2016 / PT. DKI. dated 22 June 2016 and the decision of the Supreme Court No. 2183 K / Pid.Sus / 2016. December 15, 2016.

Sixth, the Tasikmalaya District Court Decision No. 43 / Pid.Sus / 2016 / PN. Tsm. dated April 21, 2016 on behalf of the Defendant Riani on the charges of Article 46 Paragraph (1) Jo Article 30 Paragraph (1) Law of the Republic of Indonesia No. 11 of 2008 in conjunction with Article 55 Paragraph (1) to 1 of the Criminal Code, (Evidence includes one Samsung 17 Inc brand monitor unit, one CPU unit, one keyboard unit and one maouse unit). The Tasikmalaya District Court ruling stated that the Defendant was legally and convincingly proven guilty of committing a criminal act jointly

and without right or against the law of accessing computers and / or electronic systems belonging to others by any means, and imposing a sentence on the Defendant with imprisonment for 4 (four months. The District Court's decision was upheld by the Bandung High Court with its decision No. 171 / Pid.Sus / 2016 / PT. Bdg. August 2, 2016 and by the decision of the Supreme Court No. 2279 K / Pid.Sus / 2016. July 27, 2017.

Seventh, Central Jakarta District Court Decision No. 77 / Pid.B / 2016 / PN. Jkt. Pst. October 27, 2016 on behalf of the Defendant Jesica Kemala Wongso on the charges of Article 340 of the Criminal Code, (Evidence one CCTV footage). The decision of the Central Jakarta District Court stated that the Defendant was legally and convincingly proven guilty of committing premeditated murder and sentenced the Defendant to imprisonment for 20 (twenty years) years. This District Court decision was upheld by the DKI Jakarta High Court with its decision No. 393 / Pid / 2016 / PT. DKI. March 7, 2016 and Supreme Court decision No. 498 K / Pid / 2016. June 21, 2017.

Of the 7 (seven) decisions above, the author focuses more on the discussion of the Prita Mulyasari case. Prita Mulyasari sent to custody since May 13, 2009 related to his personal e-mail that contains a complaint on the service Omni International Hospital entitled "Fraud Omni Interna tional Hospital Alam Sutera Tangerang" (Kompas, 4-6-2009). This paper examines the articles of defamation that ensnare Prita. In connection with belediging (insult) as stipulated in Article 310-Article 321 of the Criminal Code, still maintaining this belediging can take various forms. There are those who insult, including insulting by writing. There are those who slander, report in defamatory and accuse slanderous. Almost all over the world the article related to humiliation is still being maintained. The reason is that the result of insulting in the form of defamation is character assassination and this is a violation of human rights.

Eddy Os Hiariej (2009), responding to the Indonesian chapter of humiliation that the articles on defamation is still dipertahan right. The reason is, in addition to producing a character assassination of defamation, it is also considered not in accordance with the traditions of the Indonesian people who still uphold eastern customs and culture. Therefore, defamation is a form of rechtsdelicten and not wetdelicten. This means that defamation has been considered a form of injustice before it is declared in the law -Invited for violating the rules of courtesy. Even more than that, defamation is deemed to violate religious norms if the substance of the defamation contains slander.

The factors behind differences are mental attitudes such as empathy. In the sociology of law, the disposition factor of conscience is closely related to the actions of a law enforcer. A police officer or prosecutor who worked with conscience (with conscience) will produce a different verdict than working only on the basis of book rule or text spell. The hypothesis on Prita's case was that if the case fell in the hands of a law enforcer with a conscience, the verdict could be different. Unfortunately, in universities (law faculties) in the world in general, not only in Indonesia there is no law enforcement course based on conscience. The Prita case and the Raju case (an imprisoned minor) can be an entry point to discuss the difference between the way to law with a conscience and without a conscience ("Meratapi Raju from Behind Bars", Kompas, 25-2-2006). Gerry Spence, a senior US lawyer, tries to answer public complaints about the incompetence of lawyers there in serving the public (The Death of Justice, 1997).

According to Spence, the lawyers ' inability lies not in their professionalism but in the sense of humanity that lawyers do not have . Since the students stepped into law schools, since then they have been trimmed and their human feelings dulled. As a result, the US public is treated without affection (care) only as a paying object. Spence bitterly said if you need help, don't come to the lawyer's office , but to the nurse. Nursing education curriculum is full of loving people (care).

The Prita case and the Raju case are soaked with human aspects. The way of law is by conscience pays great attention to these things. Each case is unique which requires a conscience to handle it. Law is not only based on text but also common sense and conscience. Here we are not just theorizing, but actually Indonesia has human beings based on conscience-based law, such as Bismar Siregar, Adi Andojo Soetjipto, Hoegeng, and several others.

Bismar Siregar has always said that I will prioritize justice over law. Adi Andojo memper bet on himself to raise the image of the Supreme Court of the sinking. Hoegeng is said to be so honest that he rivals the bumps and busts of the non-bribable cop. All tangible evidence that shows berukum based book rule is very insufficient and dibutuh right rule by conscience. How it takes Indone it that in exceptional circumstances at the moment.

Great English poet William Shakespeare in one play said "The first thing we have to do is to all the lawyers." I think this is aimed at legal experts who work like craftsmen without a conscience. Let us do our best, by punishing based on conscience so that incidents such as the Prita case and the Raju case will be the last in order to make Indonesia a quality rule of law.

CONCLUSION

Based on the above discussion, the researchers conclude as follows: 1. Legality of Digital Forensic Evidence in the criminal procedural law proof system is carried out in several parts, including; 1). Digital forensics with includes several sub-branches related to the investigation of various types of devices; a). Computer forensics; b). Mobile device forensics; 3). Forensic network; and 4). Database forensics. Various evidences used in digital forensic evidence are electronic evidence and digital evidence. 2. Some of the cases that have been decided in the case of cyber law cases are 1). The case of Prita Mulyasari on the charge of defamation, which was charged with using Article 45 paragraph (1) in conjunction with Article 27 Paragraph (3) of Law No. 11 of 2008 ; 2). The case of Drs. Subagyo, M.Pd on charges of pornography , who was charged with using Article 29 in conjunction with Article 4 Paragraph (1) letter e of Law No. 44 of 2008 concerning Pornography ; 3). The Darul Kutni case on the charge of defamation , which was charged using Article 45 Paragraph (1) in conjunction with Article 27 Paragraph (3) Law No. 11 of 2008 ; 4). The case of Florence Saulina Sihombing on the charge of insulting and defamation is charged with Article 27 Paragraph (3) in conjunction with Article 45 Paragraph (1) Law No. 11 of 2008 ; 5). The Grace Megasari Solaiman case , who was charged with Article 32 Paragraph (1) of Law no. 11 of 2008 ; 6). The case of Riani , who was charged with Article 46 Paragraph (1) in conjunction with Article 30 Paragraph (1) Law no. 11 of 2008 ; 7). Jessica Kemala Wongso's case with the charges in Article 340 of the Criminal Code .

SUGGESTION

1. Expand digital forensic evidence again, in the form of computers, mobile devices, networks and forensic databases, in order to strengthen the legality position of digital forensic evidence.
2. It is necessary to clarify the indictment in every case related to ITE, especially regarding defamation.

REFERENCES

1. Yudha Bhakti Ardhiwisastra, Interpretation and Construction of Law, Bandung: PT. Alumni, 2000, p. 55.
2. Abdul Kadir Muhammad. Law and Legal Research.Cet. 1. Bandung: PT. Citra Aditya Bakti. 2004. p. 52
3. Peter Mahmud Marzuki, Legal Research. Cet2. Jakarta: Golden. 2008. p. 29
4. Wright, Benjamin & Jane K.Wine, The Law of Electronic Commerce, New York, Aspen Law and Business, 1999, p. 2-6.
5. Haris Asnawi, Islamic Perspective E-Commerce Business Transactions, Yogyakarta: Magistra Insania Press, 2004, p. 42.
6. Ahmad M Ramli, Cyber Law and HAKI in the Indonesian Legal System, Bandung: Refika Aditama, 2004, p. 1.
7. C.S.T. Kansil & Christine Kansil, Tara Law of the Republic of Indonesia, Jakarta: PT Rineka Cipta, 2000, p. 20.
8. Burk, Dan L, Patents in Cyberspace: Territoriality and the Infringement of Global Computer Network, in Tulane Law Review, 1993, vol. 8 `` No. 1, p. 4.
9. Riyeke Ustadiyanto, E-Commerce Framework, Yogyakarta: Publisher Andi, 2001, p. 1.
10. Report of the Electronic Commerce Expert Group to the Attorney-General, Electronic Commerce: building the legal framework, March, 1988, available at: http://www.law.gov.au/ aghome / advisory / eceg / single.htm.
11. Chris Reed, Computer Law, Third Edition, Blackstone Press Limited, London, 1996, p. 274.
12. Lan Walden, Computer Crimes and Digital Investigation, p. 203.
13. Lloyd E. Ohlin and Frank J. Remington, Discretion in Criminal Justice; The Tension Between individualization and Uniformity, Albany, State University of New York Press, 1993. Quoted in Joko Sriwidodo, Development of the Criminal Justice System in Indonesia, Yogyakarta, 2020, p. 1
14. Resa Raditio, Legal Aspects of Electronic Transaction Engagement, Proof of and Dispute Resolution, Yogyakarta: Graha Ilmu, 2014, p. 94-98.
15. Eddy OS Hiarej, Criminal Law Teacher, Faculty of Law UGM, wrote the Prita Mulyasari case entitled "Understanding Defamation," Kompas, June, 2009