ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

CYBERCRIME INVESTIGATION TO FACE THE INDUSTRIAL ERA 4.0 IN CRIMINAL LAW EVIDENCE

HIMAWAN BAYU AJI [1], BUDI SANTOSO [2] and DEDI PRASETYO [3]

[1, 2, 3] Doctoral Law Program, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang. Email: [1]himawanbayuaji@students.undip.ac.id, [2]budisantoso@gmail.com, [3]dediprasetyo@lecturer.undip.ac.id

Abstract

One of the problems faced by law enforcement to ensnare perpetrators of cyber crime is the problem of proving the guilt of the accused. This reality is a challenge for law enforcement to solve all problems that occur due to very rapid technological development. The research problem is how the process of proving cyber crime. A normative approach used to obtain secondary data through literature studies. Data analysis is carried out in a qualitative way. The results showed that in revealing a very complicated, complex, specific cyber crime case, telematics expert testimony as evidence on cyber crime in the criminal justice process is valid evidence according to law. In relation to the issues discussed regarding proving cyber crime using internet facilities, the legal provisions of evidence used still refer to the Code of Criminal Procedure (KUHAP) and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Keywords: Legal Protection, Consumers, Buying and Selling, Electronics, online transactions

A. INTRODUCTION

The advancement of information technology now and its possibilities in the future cannot be separated from the encouragement made by the development of communication technology and computer technology (Theohary & Rollins, 2015). The combination of communication technology and computer technology gave birth to the internet which became the backbone of information technology (ITU, 2009). The Internet is a new dimension in human life. The Internet is a tool for global dissemination of information, a mechanism for disseminating information and a medium for collaborating and interacting between individuals using computers without being hindered by geographical boundaries (Sitompul, 2012)

Technological developments at this time give rise to various communication media that are very fast in providing various information in a very short space and time. The invention of communication tools in the form of computers gave rise to a new communication system often called a network (network) that can be accessed via the internet using a computer. The presence of communication technology provides great convenience and benefits to humans as users, namely to help solve problems with activities carried out by humans from simple to complex levels of difficulty, this is to achieve effectiveness and efficiency in every problem-solving activity faced by humans, especially communication. The development of the internet in Indonesia was like unexpected before (Ardiyanti, 2016).

A few years ago the internet was known by a small number of people who had an interest in computers. However, in recent years internet service users have increased very rapidly, although there is an opinion that says that most internet users in Indonesia are only limited to entertainment and experimentation. Along with the rapid development of communication through the internet, there are also various crimes committed with internet media (Fitriani & Pakpahan, 2020).

It is undeniable that the use of the sophisticated and fast internet also gives rise to crimes that are very sophisticated and difficult to know the perpetrators. This is because the internet is an invisible (virtual) communication medium, so that criminals can easily eliminate traces without being clearly known. Apart from the benefits obtained by technological advances in the field of computers, lately problems arise when computer networks used by various parties are misused by certain parties for opposite interests, or known as computer crime (Arifah, 2011).

In other terms, this crime is better known as cyber crime or mayantara (cyber space) crime. The world is now without borders, so it has caused significant social changes that take place with so rapid changes in society due to the development of information and communication technology, so that the world has been likened to shrinking. Various events, including crimes, from different parts of the world, pictures and news can be presented instantly, some can even be presented in real teams (Brenner, 2007).

The phenomenon of cyber crime development is actually not only a national, reginal, or regional problem of a particular country, but has become an international concern because the reach of cyber crime is global (boarderless). That is why in various international forums such as the International Information Industry (IIIC) 2000 Mellenium Congress held in Quebec on September 19, 2000, the Information Technology Association of Canada was very concerned about this problem. Even the Data Protection Working Party of the Council of Europe states that cyber crime is part of the seamy side of the information society (Situmeang, 2020).

In connection with this, efforts to overcome it are carried out by criminalizing cyber crime. The presence of information network systems in the form of networks in these various fields also creates opportunities for other parties to access the network for their own interests which in turn can harm certain parties. A computer is a series or collection of electronic machines that work together and can carry out a series or series of jobs automatically through instructions or work given to them (Bunga, 2019).

The internet is a product of the development of information technology bringing enormous changes to the empowerment of information and telecommunications, in which it gave birth to a concept called information globalization, where the decreasing boundaries of space and time in interacting activities and various information about various things needed by humans, using the internet in which there is an internet service provider (ISP), Making one computer with another computer as if connected without being limited by place (Noor, 2005).

B. METHODS

This research is a legal research that relates the existence of existing laws and regulations that have been used as a reference with silverware in the field. The main research is carried out by literature studies to obtain secondary data on primary legal materials, secondary legal materials, and tertiary legal materials. Data analysis was carried out on all legal regulations related to the subject matter discussed and argued theoretically based on the concept of criminal law using qualitative analysis methods (Rahayu et al., 2020).

C. DISCUSSION

1. Models of Cyber Crime

In connection with the developments that occur today, many crimes that have emerged are cyber crimes. According to Setiadi , Senior Investigator at the Indonesian National Police Headquarters (Mabes Polri), terminalologically cyber crime that is popularly used by the community can be interpreted as cyber crime or not real. So it seems as if there is no crime or crime because a criminal act must be definitely the object and subject of the law, locus delicti and tempus delictnya. To explain the crime, the author uses the term cyber crime (Raharjo, 2005).

Acts that can be categorized as crimes in the field of cyber crime can be divided into 2 (two) categories, including:

1. A common crime that makes a computer a tool or means (auxiliary) to commit the crime. In this case, directly or indirectly computers play a role in the process of occurrence of other criminal acts, for example;

   a. Carding or credit card fraud/misuse, namely the illegal/unauthorized use of credit cards to order or buy goods via the internet by including someone else's credit card number for payment of the goods ordered.

   b. Internet banking fraud, namely through internet media transfers or withdrawals or banking transactions using the website of one of the banks and the banking world via the internet

   c. Threats/Terrorism, namely through the internet and extortion of other parties to achieve their goals.

   d. Pornography, which is the dissemination of pornographic images as well as call women through the internet (Ismail, 2009).

2. Crimes with target targets are computer facilities and information technology systems so that computers other than as targets / victims or generally known as the term kacking / cracing that attacks computer network operation programs for example:

   a. Dos Attack is attacking the operating system on every computer

   b. Defacing, which is changing (adding and subtracting) the appearance of a particular website / homepage illegally

   c. Phreking is an attack with viruses or worms and other malicious programs Bonet or robot Network, which is a network of machine owners will enter the computer center controlled by the perpetrator (Arief, 2000).

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

So far, the computer network security company has handled many cyber crime problems, some actions in the form of:

1. Theft and use of internet accounts belonging to others.

One of the difficulties of an ISP (internet service provider) is that their customers' accounts are stolen that are used illegally. What is stolen is only information so that the person who is stolen does not feel it. Theft will have an effect if the information is used by unauthorized people, as a result of this theft the user is charged for the use of the account (MR, 2012).

2. Hijack websites.

This activity is the activity most often done by crackers, namely changing web pages, better known as defaces. Piracy is done by exploiting security holes in a site (Handoko, 2017).

3. Probing dan Port scaning

One of the steps crackers take before getting into the targeted server is to conduct reconnaissance. The way this is done is to do port scanning or probing to see what services are available on the target server. The person concerned has not carried out search or attack activities, but the activities carried out are suspicious (Subagyo, 2018).

4. Virus

The spread of viruses is generally through email, and often people whose email systems are affected by viruses are not aware of this. Then this virus is sent elsewhere through its email.

5. Denail of Service (DoS) dan Distributed DoS (DoS) attack

DoS attack is an attack that aims to paralyze the target so that it cannot provide services. This attack does not commit theft, eavesdropping or falsification of data but with the loss of service the target cannot provide services so there is financial loss. A DoS attack is an improvement over a DoS attack by performing it from dozens of computers simultaneously. The resulting effect is more powerful than DoS attacks alone (Harjoko, 2010).

6. Crimes related to domain names (Domain name).

Domain names are used to identify a company or trademark. However, many people make a profit by registering someone else's company domain name and selling it at a higher price. Another problem is using a company's rival domain name to the detriment of other companies (Gultom & Elisatris, 2005).

The National Law Development Agency in a publication identifies forms of actions related to activities in cyber space, including:

1. Joycomputing, defined as the act of someone who uses a computer illegally or without permission and uses it beyond the authority given.
2. Hacking, defined as the act of connecting by adding a new computer terminal to a computer network system without permission (unlawfully) from the legal owner of the computer network.

DOI: 10.5281/zenodo.10089088

3. The Trojan horse, defined as a procedure to add, subtract or change instructions on a program, so that the program in addition to carrying out the actual task will also carry out other tasks that are not legal.
4. Data Leakage, defined as leakage of confidential data carried out by writing confidential data into certain codes so that the data can be taken out without being noticed by the responsible party.
5. Data Daddling, defined as an act that changes valid or legitimate data in an illegitimate way, namely by changing data input and data output.
6. Waste of computer data, defined as an act done with a deliberate intent to damage or destroy floppy disk media and other storage media containing computer data or programs (Hafidz, 2014).

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, categorize some acts into cybercrimes. These acts include:

1. Crimes against domain names (Article 16).
2. Crimes against intellectual property rights and rights to confidential information in information technology activities (Article 19)
3. Crimes against personal rights (Article 22)
4. The crime of pornography (Article 41)

Understanding the description above, it is known that an act can be said to be a criminal act if there are laws that have regulated it at this time, cyber crime cannot be categorized as a criminal act because there is no law regulating it, but in this case in reality in the community an act can be categorized as a criminal act if the act harms and disturbs the community. So that cybercrime that does not yet have laws and regulations governing it can be categorized as a criminal offense because the act has caused a lot of harm to society and cybercrime can be criminalized so that there is legal certainty for a criminal act (Panjaitan, 2005).

Actions that have been regulated in law or that have occurred a lot and have been considered by the community as an act of *cybercrime* can be analyzed to formulate the determination of an act as an act of cyber crime by:

1. Explain the terms contained in the sense of cyberspace (*cyber crime*) such as computer programs, computer networks, internet, floppy disks, databases, passwords, electronic data, digital signatures, websites, input and output and others (Putri & Budiono, 2019).
2. Dividing actions in cyber crime (cyber crime) includes actions that occur in hardware. Software and in the network (network), whether the act, is carried out by a person or legal entity (Astuti, 2015).

DOI: 10.5281/zenodo.10089088

2. Evidence in Indonesian Criminal Law against Cyber Crime

Proof of a criminal act is a provision that contains outlines and guidelines on the ways in which the law proves the guilt charged to the accused, evidence is also a provision that regulates evidence that is permitted by law and that can be used by the Judge to prove the alleged guilt (Hiarij, 2012).

Evidence can be used as a central point in the trial process in Court, because in this evidence, the fate of the accused will be determined. If the results of proof by evidence prescribed by law are not sufficient to prove the guilt charged against the defendant, then the defendant is exempt from the law. Conversely, when the guilt of the accused can be proven, then the defendant is found guilty, and therefore sentenced to a crime. Proof is a method carried out by a party on facts and rights related to its interests (Lasmadi & Sudarti, 2021).

Proof of whether or not the accused committed the act charged is the most important part of criminal procedural law. To prove means to give certainty to the judge about the existence of certain events (Handoko, 2017).

The six main points that become measuring instruments in the theory of proof can be described as follows:

1. Basis of Proof

What is meant by Basis of Evidence is the basis used to obtain a truth to the facts. In other words, the basis of proof is the content / material of the evidence itself. It can be said that if the evidence is the container, then the basis of proof is the contents of the container.

2. Evidentiary Tools

Evidence Tools are tools used to describe or explain a criminal situation or event based on facts that occurred in the past for the purposes of criminal proceedings.

3. Deciphering of Evidentiary Tools

Deciphering Evidence is the methods used to describe an event or situation based on the use of evidence used to commit a criminal act. Deciphering Evidence plays a very important role in the examination of cases in court, because it is based on evidence that the Judge determines his conviction.

4. The Power of Proof

What is meant by the Power of Proof here is the evidentiary power of each piece of evidence. In criminal cases, usually the power of proof lies in the facts, where the proof is based on the truth of the facts that have been tested for truth by the Judge.

5. The burden of proof required by law to prove an indictment before a court (bewijslast).

Minimum evidence required in proof to bind the judge's freedom (bewijsminimum) (Amin, 2020)

In essence, proof begins from the moment of a legal event. If there is a criminal element (preliminary evidence that a criminal act has occurred), then from that process an investigation is carried out (a series of investigator actions to find and find an event that is suspected to be a criminal act in order to determine whether or not an investigation can be carried out in the manner provided for in this law) (Aulia, 2022)

In Law Number 2 of 2002 concerning the Police in article 1 number 13, investigation is a series of actions of investigators in terms and according to the manner regulated in this law to search for and collect evidence that with that evidence makes light of the criminal act that occurred and to find the suspect. Based on Article 184 paragraph (1) of the Code of Criminal Procedure (KUHAP), it is stated that valid evidence is: a. Witness Statement b. Expert Testimony c. Letter d. Instructions e. Defendant's Statement

Article 5 of the Law on Electronic Information and Transactions states that: Paragraph (1) Electronic information and/or printouts of electronic information are valid evidence and have valid legal consequences. Paragraph (2) Electronic information and/or printouts of electronic information as referred to in paragraph (1) are extensions of valid evidence in accordance with the applicable Procedural Law in Indonesia.

In relation to the issues discussed regarding cyber crimes that use internet facilities, the legal provisions used still refer to the Code of Criminal Procedure (KUHAP) and the Law on Electronic Information and Transactions Cyber crime has a different character from general criminal acts both in terms of perpetrators, victims, modus operandi and crime scenes so that it requires special handling and arrangements outside the Criminal Code (Darmadi, 2019).

The rapid development of information technology must be anticipated by the laws that regulate it where the police are law enforcement agencies that play an important role in law enforcement. In order for a criminal case to reach the level of prosecution and examination in a court hearing, it must first pass several actions at the investigator level (Kansil, 2014).

Basically, the criminal process goes through the following stages: (Atmasasmita, 2010):

1. Investigation stage by police
2. Prosecution stage by the Prosecutor (Public Prosecutor)
3. Examination stage in court.

In the investigation process, the investigating officers take a series of actions necessary to obtain evidence that will be needed in court. If there is insufficient evidence, or the incident turns out not to be a criminal offense or the investigation is stopped by law, the investigator is authorized to stop the investigation process, and vice versa if the evidence has been fulfilled and the event is not criminal, the investigator will continue the investigation process by making minutes (case filing) to be submitted to the public prosecutor (Maroni, 2018).

Mayantara crime (cyber crime) using internet facilities is very difficult to find and collect evidence to ensnare the perpetrators, both internet facility providers and gambling players themselves, because this crime is a cyber crime, where internet or computer network data is

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

difficult to penetrate by law enforcement officials, so that officials have difficulty in collecting evidence to ensnare perpetrators of criminal acts (Hamzah, 2011). If there are criminal elements (preliminary evidence that a criminal act has occurred) then from the process an investigation is carried out (a series of investigator actions to find and find an event that is suspected to be a criminal act in order to determine whether or not an investigation can be carried out in the manner provided for in this law) (Najih, 2014)

In Law Number 2 of 2002 concerning the Police in article 1 number 13, investigation is a series of actions of investigators in terms and according to the manner regulated in this law to search for and collect evidence that with that evidence makes light of the criminal act that occurred and to find the suspect.

The steps taken by the National Police in handling cyber cases or cases of destruction of computers through the network, are as follows (Alfian, 2017):

1. Making a Police Report, followed by the summoning of a Witness from the owner of the ISP (Internet Service Provider) who has known that the ISP is used by the perpetrator (hacker);
2. Examination at the Crime Scene (TKP) and internet café or café net used by the perpetrator, as well as to collect, track and/or confiscate electronic evidence (digital evidence) at the crime scene, such as hard disks;
3. Examining witnesses and experts who have expertise in the field of information technology, from or other institutions;
4. Examination of suspects, after being preceded by forcible arrest and/or detention, based on preliminary evidence and/or sufficient evidence;
5. Filing and application of criminal articles that can be alleged against suspects.

In carrying out investigation activities, sufficient preliminary evidence is needed, namely evidence to suspect a criminal act by requiring a minimum police report plus one piece of evidence. This is certainly related to the burden of proof that has been required by the Law in this case, namely at least two pieces of evidence (Eko Prasetyo, 2023).

In investigating a cyber crime case, an investigator can use standard investigative tools, including: a. Information as a basis for a case Information can be obtained from observation, testing electronic evidence stored on a hard disk or even still in memory. For investigators, it is very important to obtain information through crime scene search (investigation at the crime scene) that relies on computers. b. Interview and Interrogation This tool is used to obtain information from parties involved in cybercrime. This interview involves obtaining information by asking questions to witnesses, victims, and others who may have relevant information to solve the case. While interrogation involves obtaining information by giving questions to suspects and witnesses.

The technique is carried out with a sympathetic approach which includes: a) Logical approach Using reasons to convince the suspect to confess his actions; b) Indifference By pretending not to require a confession because the investigator already has enough evidence even without a confession. This is effective in cases with multiple suspects, where the information concerned is confronted with each other; c) Facing-saving approach: By allowing the suspect to give reasons for his actions and show understanding why he or she committed the act. c. Instruments The usefulness of technology in obtaining evidence (Harahap, 2010).

In the case of cybercrime, the use of data recovery techniques to find "deleted" and "erased" information on disks is one type of instrument. In addition, other traditional examples include forensic techniques for collecting and analyzing evidence and DNA analysis (Handoko, 2017).

6. Compile a case report

After all physical evidence has been collected and documented and interrogation has been conducted, the steps to be taken are the preparation of a case report that contains: a. Investigation report; b. Criminal case investigation report followed up from the investigation report; c. Documentation of electronic evidence d. Laboratory reports from computer forensics experts; e. Affidavits from witnesses, suspects, and experts; f. Crime scene reports, photographs and video footage; g.Print out of related digital evidence.

7. Examination of the case file by the Public Prosecutor

The public prosecutor provides direction to the investigator on the weaknesses of the case file and additional information or evidence that needs to be obtained or clarification of facts in order to strengthen the charges and prepare witnesses for the trial process if the case is transferred to court.

8. Making the decision to sue

If the case file is declared complete, the public prosecutor conducts prosecution of the suspect in a trial that depends largely on the jurisdiction and procedures prescribed by law. In this stage, the choice of the type of claim is determined based on the law of evidence stipulated in the Code of Criminal Procedure (Susatyo, 2023)

In the prosecution process, a prosecutor acting as a public prosecutor makes an indictment, which in the indictment is based on evidence that has been examined, examined and stored by the prosecutor. In accordance with the evidence system adopted by the Criminal Code, the prosecutor in preparing his charges must also be guided by the contents of Article 183 of the Criminal Procedure Code, namely that there are at least two pieces of evidence that are valid according to the Law, which if they meet the requirements of the case are forwarded to the examination process at the court hearing.

In relation to cyber crime, using internet facilities, the prosecutor's office coordinates with the police as investigators to ensnare the perpetrators of criminal acts, but if strong evidence is not found, as well as provisions or laws governing the crime, the perpetrators can stop the investigation and prosecution process (Moelyatno, 1955).

Based on the description above, it can be analyzed that the way that must be taken by the police and the Prosecutor's Office in the event of a cyber crime is to investigate the case by looking for web ip addresses and looking for electronic evidence. Because the web ip address is the first strong evidence in the disclosure of cyber cases (Vilic, 2017).

According to article 5 of the Law on Electronic Information and Transactions which reads: (1) Electronic Information and/or Electronic Documents and/or printouts are valid legal evidence. (2) Electronic Information and/or Electronic Documents and/or printouts as referred to in paragraph (1) shall constitute an expansion of valid evidence in accordance with the applicable Procedural Law in Indonesia. (3) Electronic Information and/or Electronic Documents are declared valid if using Electronic Systems in accordance with the provisions stipulated in this Law. There is a new legal breakthrough because Electronic Information and/or Electronic Documents and/or printouts are an expansion of valid evidence in accordance with the Procedural Law (Wibawa, 2017).

But to "validate" the electronic evidence before the court is to process the electronic evidence from the electronic form produced from the computer system into output printed into paper media. Namely, the electronic evidence is changed in hardcopy form, that is, printed, without any modification from humans. Then to strengthen it, the print out can be submitted to expert witnesses for analysis and validity before the court (Jannah & M. Naufal, 2012).

In the process of examination in the court session, the Judge assesses the strength of the evidence presented by the public prosecutor in his indictment. The judge in this case is guided by the negative evidence system according to the Law, namely Article 183 kUHAP which determines a minimum of two pieces of evidence accompanied by conviction. Problems sometimes in a criminal case process have difficulty getting an absolute truth because of the lack of available evidence, or also the existing evidence is not supportive to solve the case so that it results in many cases that are not resolved and accumulate at the investigation / police level (Hertoni, 2016). The number of cases that accumulate is usually stalled at the police level because prosecutors in this case usually reject case files submitted by investigators due to lack of evidence that corroborates the charges (Syamsuddin, 2008).

Given that a crime is committed always so as not to be known by others, the perpetrator of the crime tries his best to eliminate evidence, this is a preventive effort to avoid justification from evidence both at the investigation level and at the examination level. Therefore, the role of proof is very important in criminal proceedings so that it can be said that proof is at the heart of criminal procedural law (MONTEIRO, 2021).

Understanding the above description can be analyzed that to prove an act of cyber crime in a trial. For this reason, in the system of evidence, the trial must be based on a positive legal proof system. The law stipulates in a limited way which evidence the judge can use. If the evidence has been used lawfully as stipulated by law, the judge must establish the legal circumstances of the evidence, even if the judge is found to believe that what should be considered proven is not true. The system seeks to get rid of all the judges' subjective judgments and bind judges to harsh evidentiary rules. "This system is also called formal proof theory (formele

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

bewijstheorie)” (Rifai, 2011).

For proving cases in cyberspace in court must also use an evidentiary system based on the judge's belief in a logical reason (la conviction raisonee) this proof system, the judge plays an important role here. A judge can only sentence a defendant if he has believed that the act in question has been substantiated. The belief must be accompanied by reasons based on a series of thoughts (logic). "The judge is obliged to elaborate and explain the reasons on which he is based on his conviction of the defendant's guilt” (Boyoh, 2015).

This evidentiary system recognizes the existence of certain evidence but is not stipulated in a limited manner by law. Such evidence clearly shows that an evidence is not evidence, at least at least two pieces of evidence must be accompanied by the Judge's Conviction. Even if there is enough evidence but the judge is not sure or the judge is convinced but the evidence is not enough, the judge cannot sentence the defendant. In Wetterlijk's Negatief theory, there is a clear relationship between evidence and the judge's conviction where the judge is bound by the rules of the law and he obtains confidence that evidence has been given so that punishment can be imposed (Siahaan, 2006).

Based on the description above, it can be analyzed that it is not simple to apply the rule of law to perpetrators involved in cyber crime. This is because the internet is cross-border in nature. Many parties intersect with each other and this will make it difficult in the process of examination in court. Therefore, solutions must be found so that perpetrators involved in cyber crime can be presented to the green table (Setiawan, 2018).

Which law applies is actually not as difficult as it has been so far, perpetrators involved in cyber crime can be sentenced to criminal punishment in accordance with applicable provisions (positive law) according to the citizenship status of the perpetrator is located. Then it is also possible for foreigners who commit criminal acts in Indonesian territory to be convicted using Indonesian criminal law (Maggalatung, 2014). This is in accordance with the principle of passive nationality. What must be done if we want to use Indonesian law to catch foreign perpetrators is to make an extradition treaty with the perpetrator's country of origin. The reason is, in the process of investigation and investigation, cybercrime cannot be done alone and needs to be coordinated with Interpol, FBI, and others.

D. CONCLUSION

The results showed that in revealing a very complicated, complex, specific cyber crime case, telematics expert testimony as evidence on cyber crime in the criminal justice process is valid evidence according to law. In relation to the issues discussed regarding proving cyber crime using internet facilities, the legal provisions of evidence used still refer to the Code of Criminal Procedure (KUHAP) and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions

The testimony of telematics experts in the process of examining mayantara criminal cases, both at the investigation examination stage and at the examination in court hearings is very important and needed, especially to assist investigators, public prosecutors or judges in

The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

revealing a very complicated, complex cyber crime case that is specific. In relation to the issues discussed regarding proving cyber crime using internet facilities, the legal provisions of evidence used still refer to the Code of Criminal Procedure (KUHAP) and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which are valid evidence according to law

Bibliography

1) Alfian, Muh. (2017). Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan. *Jurnal Kosmik Hukum*, *17*(2).

2) Amin, R. (2020). *Hukum Pembuktian Dalam Perkara Pidana Dan Perdata - Rahman Amin - Google Books*. CV. Budi Utama. https://books.google.co.id/books?hl=en&lr=&id=pvbkDwAAQBAJ&oi=fnd&pg=PP1&dq=kebenaran+pembuktian+hukum+perdata&ots=aU-Bi0yUaO&sig=N_Ji3GZ_ls81m7eSqABtoVWUmYs&redir_esc=y#v=onepage&q=kebenaran%20pembuktian%20hukum%20perdata&f=false

3) Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1).

4) Arief, B. N. (2000). *Tindak Pidana Mayantara, Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja Grafindo Persada.

5) Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *15*(3).

6) Astuti, S. A. (2015). Law Enforcement of Cyber terrorism ini Indonesia. *Jurnal Rechtsidee*, *2*(2).

7) Atmasasmita, R. (2010). *Sistem Peradilan Pidana Kontemporer*. Kencana Prenada Media Group.

8) Aulia, M. I. (2022). *Kebenaran Materiil Dalam Pembuktian Tindak Pidana Zina (OVERSPEL).* https://repository.uinjkt.ac.id/dspace/handle/123456789/62183

9) Boyoh, M. (2015). Independensi Hakim Dalam Memutus Perkara Pidana Berdasarkan Kebenaran Materiil. *Lex Crimen*, *4*(4). https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/8936

10) Brenner, W. (2007). *Cybercrime: Re-Thinking Crime Control Strategies, dalam Yvonne Jewkes*. Willan Publishing.

11) Bunga, D. (2019). Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. *Fakultas Hukum Universitas Gadjah Mada*. https://www.cybersecurityintelligence.com/blog/fbis-cybercrime-

12) Darmadi, A. A. N. O. Y. (2019). Konsep Pembaharuan Pemidanaan Dalam Rancangan KUHP. *Urnal Ilmu Hukum*, *6*(2).

13) Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *Analisa Penyalahgunaan Media Sosial Untuk Penyebaran Cybercrime Di Dunia Maya Atau Cyberspace*, *20*(1).

14) Gultom, D. M. A. M., & Elisatris. (2005). *Cyber Law (Aspek Hukum Teknologi Informasi)*. Rafika Aditama.

15) Hafidz, J. (2014). Kajian Yuridis Dalam Antisipasi Kejahatan Cyber. *Jurnal Pembaharuan Hukum*, *1*(1).

16) Hamzah, A. (2011). *Bunga Rampai Hukum Pidana dan Acara Pidana.* Ghalia Indonesia.

17) Handoko, C. (2017). Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime Di Pengadilan. *Jurnal Jurisprudence*, *6*(1), 1. https://doi.org/10.23917/JURISPRUDENCE.V6I1.2992

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

18) Harahap, M. Y. (2010). *Pembahasan Permasalahan Dan Penerapan KUHAP, CetKe-13*. Sinar Grafika.

19) Harjoko, A. T. P. (2010). *Cyber Crime dalam Perspektif Hukum Pidana*. Universitas Muhammadiyah Surakarta.

20) Hertoni, M. (2016). Independensi Hakim Dalam Mencari Kebenaran Materiil. *Lex CRIMEN*, *5*(1). https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/10600

21) Hiarij, E. O. (2012). *Teori dan Hukum Pembuktian*. Erlangga.

22) Hukum Dan Dinamika Masyarakat, J., & Masyarakat, ; Jurnal Hukum Dan Dinamika. (2023). Kriteria Alat Bukti Elektronik yang Sah dalam urgensi pembaharuan Kuhap. *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat*, *21*(1), 51–65. https://doi.org/10.56444/HDM.V21I1.4035

23) Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(03).

24) ITU. (2009). *Understanding Cybercrime Guide, ICT Appliccation dan Cybersecurity Division*.

25) Jannah, H. S., & M. Naufal. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. *Jurnal Al-Mawarid*, *XII*(1).

26) Kansil, F. I. (2014). Sanksi Pidana dalam Sistem Pemidanaan Menurut KUHP dan di Luar KUHP. *Lex Crimen*, *3*(3).

27) Lasmadi, S., & Sudarti, E. (2021). Pembuktian Terbalik Pada Tindak Pidana Pencucian Uang. *Jurnal Ilmu Hukum*, *5*(2). https://ejournal.uksw.edu/refleksihukum

28) Maggalatung, A. S. (2014). Hubungan Antara Fakta Norma, Moral, dan Doktrin Hukum Dalam Pertimbangan Putusan Hakim. *Jurnal Cita Hukum*, *2*(2).

29) Maroni. (2018). *Hukum Birokrasi Peradilan Pidana*. CV. Anugrah Utama Raharja.

30) Moelyatno. (1955). *Perbuatan Pidana dan Pertanggungjawaban dalam Hukum Pidana.* UGM Press.

31) Monteiro, J. M. (2021). Putusan Hakim Menurut Perspektif Sosio-Legal. *Jurnal Hukum Yurisprudinsia*, *22*(2), 8–21. http://publikasi.undana.ac.id/index.php/jhy/article/view/h899

32) MR, A. (2012). Yuridiksi dan Transfer of Procedding Dalam Kasus Cybercrime. *Tesis, Program Studi Magister Hukum Universitas Indonesia*.

33) Najih, M. (2014). *Politik Hukum Pidana; Konsepsi Pembaharuan Hukum Pidana dalam Cita Negara Hukum. Cetakan pertama.* Setara Press.

34) Noor, A. F. (2005). *Tinjauan Yuridis terhadap Cybercrime di Indonesia*.

35) Panjaitan, H. I., & Dkk. (2005). *Membangun Cyber Law Indonesia Yang Demokratis*. IMLPC.

36) Putri, C. C., & Budiono, A. R. (2019). Konseptualisasi Dan Peluang Cyber Notary Dalam Hukum. *Jurnal Ilmiah Pendidikan Pancasila Dan Kewarganegaraan*, *4*(1), 29–36.

37) Raharjo, B. (2005). *Keamanan Informasi Berbasis Internet*. PT. Insan Indonesia.

38) Rahayu, D. P., SH, M., & Ke, S. (2020). Metode Penelitian Hukum. *Yogyakarta: Thafa Media*.

39) Rifai, A. (2011). *Penemuan Hukum Oleh Hakim Dalam Perspektif Hukum Progresif*. Sinar Grafika.

40) Setiawan, B. (2018). Penerapan Hukum Progresif oleh Hakim Untuk Mewujudkan Keadilan Substantif Transendensi. *Kosmik Hukum*, *18*(1), 159–179. https://doi.org/10.30595/kosmikhukum.v18i1.2338

41) Siahaan, L. O. (2006). Peran Hakim Dalam Pembaruan Hukum Di Indonesia Hal-Hal Yang Harus Diketahui (Proses Berfikir) Hakim Agar Dapat Menghasilkan Putusan Yang Berkualitas. *Jurnal Hukum & Pembangunan*. https://doi.org/10.21143/jhp.vol36.no1.298

ISSN 1533-9211

DOI: 10.5281/zenodo.10089088

42) Sitompul, J. (2012). *Cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana*. PT. Tatanusa.

43) Situmeang, S. M. T. (2020). *Cyber law*. CV Cakra.

44) Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan & Bela Negara*, *5*(1), 89–108.

45) Susatyo, F. A. (2023). Kriteria Alat Bukti Elektronik yang Sah dalam urgensi pembaharuan Kuhap. *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat*, *21*(1), 51–65. https://doi.org/10.56444/hdm.v21i1

46) Syamsuddin, A. (2008). *Integritas penegak hukum: hakim, jaksa, polisi, dan pengacara*. Penerbit Buku Kompas.

47) Theohary, C. A., & Rollins, J. W. (2015). *Cyberwarfare and Cyber terrorism: In Brief.* Congressional Reseach Service.

48) Vilic, V. (2017). *Cyber terrorism on The Internet and Social Networking: A Threat to Global Security. International Scientific Confrence on Information Technology and Cata Related Research Serbia*. Singidunum University.

49) Wibawa, I. (2017). Cyber Money Laundering (Salah satu bentuk White Collar Crime abad 21). *YUDISIA*, *8*(2), 241.