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

Obstacles to Proving Criminal Acts of Interception in the Validation Process of Electronic Evidence in Cyber Crimes

Faqih Gustianto
Faculty of Law, Universitas Islam Sultan Agung, Semarang, Indonesia, E-mail: faqihgustianto.std@unissula.ac.id

Abstract. *The development of information and communication technology has given rise to increasingly complex forms of cybercrime, including the illegal interception of electronic systems and electronic information. In law enforcement practice, proving interception faces various obstacles, particularly in the validation of electronic evidence, the primary instrument in uncovering cybercrime. The research questions in this article are: (1) how is the process of proving interception in cybercrime based on Indonesian laws and regulations? (2) what are the obstacles encountered in validating electronic evidence in the investigation of interception; and (3) how these obstacles can be overcome to achieve legal certainty and effective law enforcement. The research method used is a normative juridical method with a statute approach, a conceptual approach, and a case approach. The data used is secondary data consisting of primary legal materials, secondary legal materials, and tertiary legal materials, analyzed qualitatively. The research results indicate that proving the crime of interception in cybercrime relies on electronic evidence as specified in the Electronic Information and Transactions Law (UU ITE), the Criminal Procedure Code (KUHAP), and other related regulations. Obstacles encountered in the process of validating electronic evidence include technical, legal, and institutional aspects. Technical obstacles involve difficulties in maintaining the integrity, authenticity, and integrity of electronic data due to the easily modified nature of digital data. Legal obstacles arise from the lack of uniform standard procedures for validating electronic evidence, including digital forensic mechanisms that are universally accepted in the judicial process. Meanwhile, institutional obstacles include limited human resources, digital forensic facilities, and coordination between law enforcement agencies. Efforts to overcome these obstacles include improving regulations related to electronic evidence, strengthening the capacity of law enforcement officers in the field of digital forensics, developing standard operating procedures for validating electronic evidence, and increasing cooperation between relevant agencies and institutions.*

Keywords: *Crime; Electronics; Evidence; Forensics; Interception.*

1. Introduction

Development technology information, internet and networking computer has makes public Can create room social new where they are One with others can meet and interact with each other One each other in cyberspace. Interaction crossing boundaries and going beyond room as well as time.[1] The emergence various pattern behavior crime new thing that develops in a silent world named *cyber,* it provides thinking new in development life development law to overcome it which is implications from progress technology and information. Development That gives external influence normal in a world without borders in space cyber. A world without territorial boundaries (*borderless)* makes global society characterized by with One strength transcending the boundaries of space and time so fast only with count instant. The era of technology in public digitalization has become dynamic with presence *interconnected network* (internet) that uses communication without paper (*paperless document)*.[2]

Development technology information and communication has give birth to transformation big in various aspect life, including in pattern crime that develops in society. The original crime nature conventional now transform become crime based technology information or known as crime cybercrime. Crime This own different characteristics compared to with crime conventional, among others, not knowing the boundaries of the region (borderless), using system electronic as means main, and leave digital footprint as tool proof main.

Confession to tool proof electronic in Indonesian law, has confirmed in Constitution Number 1 of 2024 concerning Amendments Second Constitution Number 11 of 2008 concerning Information and Electronic Transactions in Article 5 paragraph (1) is emphasized that:

"Electronic *Information and/ or Electronic Documents and/ or results print it is tool proof legitimate law.*"

Furthermore, Article 5 paragraph (3) also states:

"Electronic *Information and/ or Electronic Documents are stated legitimate if use Electronic System according to with the provisions stipulated in Constitution This*."

Provision the show that tool proof electronic has get legitimacy as tool equivalent evidence with tool proof conventional in system proof law Indonesian criminal law. However thus, the recognition normative This No necessarily remove problem in practice, especially related with validation and validity tool proof electronics.

---

[1]Darwis, N. (2019). "Criminology in the Policy Field : Cyber Security ". *Journal Aerospace Law Science,* 9(2), p. 25.

[2]Astuti, SA (2017). "Expansion Use of Electronic Evidence (*Evidence of Electronic*) Related Provisions on Valid Evidence of Deeds Crime in Cyberspace *", Pagaruyuang Law Journal,* 1(1), p. 47.

Deeds or action, actor, tool proof in action criminal normal can with easy to identify However No thus case in point for crimes committed with use means computers. The number of internet providers and increasingly many people start getting to know the internet makes the more many people start use it.[3]

Not so in the virtual world it can also be called the virtual world or *cyberspace.* Location becomes difficult determined when from his country perpetrator stealing foreign citizens ' data. Investigators also experienced difficulty in look for witnesses who saw or hear incident. Other difficulties arose in matter gather tool evidence. Collection tool proof This Lots need cost Because must use adequate (sophisticated) technology and operated by a person expert in his field.[4]

One of form crime complex and problematic mayantara problem Serious in proof is action criminal interception. Interception is basically is activity tapping or taking information electronic in a way No legitimate to system electronic or communication other parties. In law positive Indonesia, ban to interception arranged in Article 31 paragraph (1) of the Law Electronic Information and Transactions which states:

"*Everyone with intentionally and without right or oppose law do interception or tapping on Electronic Information and/ or Electronic Documents in something Computer and/ or Certain Electronic Systems belongs to someone else*."

But on the other hand, interceptions also often occur used as tool or method in enforcement law, in particular in disclosure action criminal certain. This is cause dilemma juridical, namely when results interception used as tool evidence, but the process of obtaining it No always fulfil standard strict procedures.

Problem main in practice justice No only located on there or whether or not tool proof electronics, but more far in the validation process tool proof said. Validation tool proof electronic covers aspect authenticity, integrity, and reliability. Evidence electronic must fulfil the principle *of "*integrity", authenticity and availability *"in* order to accepted in the legal process".[5] Barda Nawawi Arief said system proof in law Indonesian criminal law remains emphasize importance the judge's belief based on the tools valid evidence according to Constitution.[6]

This matter means that although tool proof electronic acknowledged, still required mechanism proof that can be convince the judge about its validity. Problems become the more complex when associated with the interception process that

[3]Syah, RS, & Ali, D. (2019). "Policy Criminal Law in Crime Prevention Action Carding Crime According to Provision Constitution Number 11 of 2008 as Amended With Constitution Number 19 of 2016 Concerning Information and Electronic Transactions ", *Journal Scientific Criminal Law Students,* 3(4), p. 614.

[4] Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: A Review Aspects of Criminal Law.* Jakarta: Tatanusa, p. 103.

[5]Makarim, E. (2013). *Notaries and Electronic Transactions,* Jakarta: Rajawali Pers, p. 4.

[6]Arief, B.N. (2008). *Potpourri Criminal Law Policy : Developments compilation Concept of the New Criminal Code,* Jakarta: Kencana, p. 14.

produces tool proof electronics. In many case, results interception debated Because:

1) It's unclear legality of the interception process,
2) Not fulfilled procedure licensing,
3) Absence standard standard in the digital evidence validation process,
4) Vulnerability electronic data manipulation,
5) Limitation ability apparatus enforcer law in field digital forensics.

On the other hand, the Criminal Procedure Law regulates in the Criminal Procedure Code not yet in a way explicit arrange mechanism proof electronic in a way comprehensive, so that cause the absence of norms in practice. This is cause reliance on interpretations of judges and experts in determine validity tool proof electronics.

Another challenge arises in cross jurisdiction (*cross-border)*, where electronic data often stored on overseas servers. This is complicate the proof process Because need Work The same international through mutual *legal assistance* mechanism. Without Work The same the process of obtaining and validating tool proof electronic become hampered. Activities cyber although can be virtual categorized as actions and deeds real law. In juridical in matter room cyber Already not in place Again For categorize something with size and qualifications law conventional for can made into objects and actions, because If method this is what is taken will too Lots difficulties and things that escape noose law. Activities cyber is virtual activities that have a very real impact although tool the proof nature electronics. With thus subject the perpetrator must also qualified as a person who has do actions law in a way real.[7]

Use proof electronic No let go from various challenges, especially related with aspect security and legality. Electronic evidence obtained through hacking cause dilemma ethical and legal. In one side, evidence the can be very relevant and crucial in reveal truth or crime certain. On the side other methods his illegal acquisition cause question about validity and can So violate right privacy individual or entities that are victims of hacking. Therefore that, the court often have to consider whether evidence obtained in a way illegal can accepted or No.[8]

A number of cases in Indonesia show that proof action criminal interception No only face problem law, but also obstacles complex technical and structural issues, in particular in the validation process tool proof electronic like bada case following:

1) KPK Wiretapping Case – Verdict Decision Court Constitution Number 5/PUU-VIII/2010

[7]Barkatullah, AH (2019). *Electronic Transaction Law in Indonesia: As Guidelines for Facing the Digital Era of Business e-Commerce in Indonesia.* Bandung: Nusamedia, p. 76

[8] Trisnawati, T., & Hanifah, S. (2024). "The Development of Electronic Evidence from Hacking as Evidence in Criminal Acts ", *Multidisciplinary Indonesian Center Journal* (*MICJO*), 1(3), p. 1345.

This case in line with interception carried out by the authorities enforcer law in a way institutional. Wiretapping in matter This used as tool reveal action criminal law, in particular corruption, and has get legitimacy law through decision Court The constitution affirms that interception can done throughout regulated by law. From the corner view proof, case This relatively own level more difficulties low compared to with two cases others. This is caused by several factors, namely:

a. Interception carried out by institutions that have authority law,

b. The wiretapping process generally documented in a way systematic,

c. evidence electronics produced tend own clear chain *of custody,*

d. Validation can done through internal procedures and competent experts.

However Thus, the constraints still appear, especially related with legality procedure interception (whether has in accordance with principle *due process of law)* and potential violation right privacy.

2) Bjorka Case (National Data Leak)

Bjorka Case represent form crime modern mayantara which has characteristics anonymity high and cross jurisdiction. The perpetrator use identity disguise, exploit global infrastructure, and distribute data through various digital platforms. In the process of proof, the case This own level very high difficulty, because:

a. Identity perpetrator No clear (*anonymous actor)*,

b. Electronic evidence scattered and not centralized,

c. Frequent data located on a foreign server,

d. Interception process to perpetrator need Work The same international.

In addition to the validation process tool proof face challenge Serious remember difficult ensure authenticity data sources, difficult prove connection between perpetrators and devices used as well as prone to to manipulation or digital engineering. This case also shows that interception No Again in form classic (tapping communication), but develop become control and distribution of data illegal.

3) Online Fraud Cases (*Phishing & Social Engineering)*

Online fraud cases based on *phishing and social engineering* is form the most crimes occurs in society. The mode involving manipulation digital communication for obtain the victim's sensitive data, such as OTP, password, or information finance. From the perspective proof, case This own level difficulty medium until high, with characteristics as following:

a. Perpetrator often use identity false

b. Communication done via digital platforms (chat, email, marketplace)

c. Primary evidence in the form of screenshots, transaction logs and/ or recording communication.

Problems main in proof is proof electronic easy manipulated, no all platforms provide data access to investigator as well as limitations digital forensic capabilities in the field. Different with case Bjorka, the perpetrator in case This sometimes Still can tracked, especially If there is cash flow, bank accounts, trail transactions. However still there is constraint Serious in validation tool proof electronics, in particular in ensure authenticity communication, data integrity and interconnectedness between perpetrator and action.

If the third case the compared, then can arranged classification level difficulty enforcement law as following:

Table of Characteristics and Classification of Interception Cases

Case	Characteristics	Main Obstacles	Difficulty Level
KPK Wiretapping	Legal interception by the state	Procedures & legalities	Low – Medium
Phishing / Online Fraud	Manipulation digital communication	Validation evidence & identity	Intermediate – High
Bjorka	Crime global & anonymous cyber	Jurisdiction & identity perpetrator	High–Very High

Condition the show existence gap between *das sollen* (the rules) law that recognizes tool proof electronics) with *das sein* (practice enforcement the law that is being faced various constraint technical and legal). In other words, even though law has give base legitimacy, its implementation Still face various significant obstacles. This is what then become problem main in study this, namely Not yet existence studies that are specific and in-depth discuss constraint proof action criminal interception focused on the validation process tool proof electronic in crime mayantara. Some research previously tend discuss tool proof electronic in a way general, but not yet focus on aspects validation in crime interception.

2. Research Methods

In a way conceptual, method approach is method the point of view used in something study for study the object being studied. according to soerjono soekanto, approach study law is the method used for understand and analyze law, good as a norm or as behavior public.[9] according to peter mahmud marzuki, the approach in study law used for get information from various aspect about current issues researched. [10]in the research this method the approach used is approach juridical empirical approach this used for study law no only as written norms (*law in books)*, but also as practice in society (*law in action)*. this relevant because study this no only analyze provision law related interception and tools proof electronics, but also reviewing obstacles that occur in practice enforcement law. specifications study is description about type research used in study something problem. according to sugiyono study descriptive is research conducted for knows mark variables independent, good One variable or more without make comparison or

[9] Soekanto, S. (2012). *Introduction Legal Research,* Depok: UI Press, p. 4.
[10] Marzuki, PM (2017). *Legal Research : Edition Revision,* Jakarta: Prenada Media, p. 70.

connect with other variables.[11] Temporary that, according to Burhan Bungin, research analytical aim for explain connection because consequences and study more in something phenomenon. [12]in research this, specifications research used is descriptive-analytical, namely research that is not only describe phenomenon law related proof action criminal interception, but also analyzing obstacles that arise in the validation process tool proof electronic in crime mayantara. the type and source of the data in question in study is subject where the data comes from can acquired and owned information clarity about how take the data and how the data is processed. [13]data is element important in research used for answer problem study.

3. Results and Discussion

3.1. Effectiveness of Legislation Regarding Criminal Procedure Criminal Interception in Indonesia

Development technology information and communication has give birth to various form crime new ones that take advantage of system electronic as means and object crime. One of the form growing crime along with progress technology the is action criminal interception or tapping illegal to information electronics and/ or document Electronic. Interception is basically is action acquire, hear, record, alter, inhibit, or take notes transmission information electronics that are carried out without rights and conflicts with law. Existence action criminal This viewed as threat to right privacy, security information and confidentiality communication which is part from right basic man in a modern state of law.

Interception is actions that have characteristics special Because be in two dimensions different laws. On one side, interception is prohibited acts if done without rights, while on the other hand interception can used as instrument enforcement law if carried out by authorized officers based on provision regulation legislation. Development technology information has cause information electronic become object the law that has mark proof so that protection to confidentiality communication electronic become very important in system modern law.[14]

Arrangement about action criminal interception in Indonesia is basically spread in various regulation legislation and not yet arranged in One regulation which is comprehensive. Settings main about interception there is in Constitution Number 1 of 2024 concerning Amendments Second Constitution Number 11 of 2008

[11] Sugiyono, (2013). *Research Methods Quantitative, Qualitative, and R&D,* Bandung: Alfabeta, p. 14.
[12] Bungin, B. (2007), *Study Qualitative : Communication, Economics, Public Policy, and Social Sciences Others,* Jakarta: Prenada Media, p. 34
[13] Adrian, M. (2024) *Introduction to Research Methods Legal Science.* West Sumatra: Tri Edukasi Ilmiah Foundation, p. 25.
[14]Makarim, E. (2005), *Introduction to Telematics Law : A Compilation of Studies,* Jakarta: RajaGrafindo Persada, p. 102.

concerning Article 31 paragraph (1) of the Electronic Information and Transactions Law is emphasized that:

"*everyone with intentionally and without right or oppose law do interception or tapping on information electronics and/ or document electronic in something computer and/ or system electronic certain other people's property is prohibited acts.*"

Provision the show that Indonesian law in general firm give protection to confidentiality information electronic from action wiretapping that is not valid.

Article 31 paragraph (2) of the Law Electronic Information and Transactions also prohibits that:

"*Everyone with intentionally and without right do interception to transmission information electronics and/ or document electronics that are not nature public from, to, and in something computer or system electronic certain belongs to someone else.*"

The sound of the article the expand room scope protection law No only to content communication electronics, but also to the ongoing electronic data transmission process taking place. With thus, the law No only protect data that has been stored, but also data that is being exchanged through network communication electronics.

Constitution Electronic Information and Transactions also provide exception to prohibition interception said. Exceptions intended given in frame enforcement law based on request apparatus enforcer competent law in accordance with provision regulation legislation. Regulations This show that Indonesian law recognizes existence need interception as instrument investigation and evidence action criminal certain. Use means technology in the enforcement process law is consequence logical from development crime based technology information that is not Again can handled with method conventional.[15]

Constitution Electronic Information and Transactions, authority interception was also found in various Constitution sectoral. One of them is Constitution about Commission Eradication Action Criminal Corruption that gives authority to the Corruption Eradication Committee for do tapping in frame investigation, inquiry and prosecution case corruption. Regulation similar can also be found in Constitution Number 35 of 2009 concerning Narcotics that provide authority to investigator for do tapping to the alleged parties involved in action criminal narcotics. The existence of various arrangement the show that interception has be one of instrument important in system justice Indonesian criminal law.

Existence various regulations that govern interception precisely cause problem harmonization law. Regulations regarding procedures, mechanisms, timeframes time, supervision, and standard use results interception as tool proof Not yet fully

[15]Arief, BN (2012). *Action Mayantara Crime : Development of Cyber Crime Studies in Indonesia,* Jakarta: RajaGrafindo Persada, p. 37.

uniform. Effectiveness law is greatly influenced by factors substance law, namely to what extent the regulations legislation capable give certainty and avoidance occurrence norm conflict.[16] Interception spread in arrangement in various Constitution often cause difference interpretation in practice enforcement law.

Problems the the more complex when results interception used as tool proof electronic in the process of proof case criminal. Although Article 5 paragraph (1) of the Law Electronic Information and Transactions have confess information electronics and/ or document electronic as tool proof valid law, legitimacy results interception still depends on the legality of the acquisition process. In other words, the tool evidence obtained through interception only can own strength proof if obtained based on legal procedures and carried out by authorized parties. Therefore that, the settings law about interception No only related with prohibitions and authority wiretapping, but also related close with validity tool proof electronic in system proof Indonesian criminal law.

Interception in system law Indonesian criminal law has a unique and complex position Because be in two dimensions different laws. On one side, interception viewed as prohibited acts if done without right or oppose law, while on the other hand interception is also recognized as one of the instruments that can used by the authorities enforcer law in frame reveal action criminal certain. Characteristic position double the cause interception be one of ongoing issues develop in law Indonesian criminal law, in particular related with protection right privacy and interest enforcement law.

Interception without right is form violation to right on confidentiality communication and information electronics. Privacy rights as part from right basic human beings basically give protection to every form surveillance, wiretapping, and taking information personal without agreement the parties concerned. Therefore that, the state is obliged give protection law to every citizen of action interception carried out in a way arbitrary. Development technology information has causing data and communication electronic become part from right private that must get protection adequate law Because own mark high economic, social and legal.[17]

Position interception as prohibited acts in a way law confirmed through Article 31 paragraph (1) of the Law Number 11 of 2008 concerning Electronic Information and Transactions as has changed final with Constitution Number 1 of 2024. Provisions the state that everyone with intentionally and without right or oppose law do interception or tapping on information electronics and/ or document electronic in something computer and/ or system electronic certain other people's property is prohibited acts. Regulations the show that law Indonesian criminal law

[16] Soekanto, S. (2014). *Factors that Influence Law Enforcement,* Jakarta: Rajawali Press, p. 8.
[17] Makarim, E., *op.cit.* p. 96.

places interception illegal as action criminal offenses that can be charged sanctions criminal.

Interception also has position as instrument laws that can used for interest investigation, inquiry, and proof action criminal certain. this is based on considerations that development modern crime, in particular crime mayantara, corruption, narcotics, and terrorism, are often carried out through communication media electronic so that need method enforcement adaptive law to development technology. use means technology in the investigation process is part from policy law criminal offenses aimed at for adapt system justice criminal with development forms modern crime.[18]

Position interception as instrument enforcement law also obtains legitimacy through various Constitution sectoral. Commission Eradication Corruption, National Narcotics Agency, and apparatus enforcer law certain given authority do tapping within the limits determined by the regulation legislation. With Thus, Indonesian law does not fully forbid interception, but rather differentiate between interception carried out in a way legitimate based on authority law and interception carried out without right or oppose law.

Problems about position interception the more develop when results interception used as tool proof in the judicial process criminal law. In the beginning, the system proof in the Criminal Procedure Code (KUHAP) only know tool proof in the form of information witness, statement experts, letters, instructions, and information defendant. However, developments technology information cause birth expansion tool proof through Constitution Information and Electronic Transactions. Article 5 paragraph (1) of the Law Information and Electronic Transactions states that information electronics and/ or document electronics and/ or results print it is tool proof valid law. Provisions the become base law confession tool proof electronic in system proof Indonesian criminal law.

Position results interception as tool proof still cause debate law. Debate the related with legality of the acquisition process tool proof electronically. In the Decision Court Constitution Number 20/PUU-XIV/2016, Court The constitution in essence confirm that information electronics and/ or document electronic as tool proof must obtained with legal and enforceable ways in frame enforcement law on request apparatus enforcer competent law.[19] Decision the show that validity tool proof electronic No only determined by the content the information contained therein, but also determined by the legality of the process of obtaining it.

Court The Constitution also provides attention special to position interception in a state of law. In the Decision Court Constitution Number 5/PUU-VIII/2010, Court have an opinion that activity tapping is very sensitive action because in one side is

[18]Arief, BN, *op.cit.*, p. 41.
[19] Pramata, AG (2021). "Analysis The Strength and Probative Value of Electronic Evidence Post - Verdict Court Constitution Number 20/PUU-XIV/2016", *Verstek,* 8(3), p. 145.

restrictions to right basic humans, but on the other hand it is needed in the enforcement process law. Therefore that, the Court confirm that arrangement about tapping must done through law and not Enough only arranged through regulation implementer.[20] Based on decision said, can understood that position interception in system law Indonesian criminal law does not can released from principle protection right basic human. Interception only can justified if done based on legitimate authority, clear procedures, and adequate supervision. With Thus, interception is essentially is form restrictions right privacy only can done for interest more laws large and based on principle of due process of law.

Proof action criminal interception own position results interception own close relationship with validity tool proof electronics. Increasingly clear the legality of the interception process, then the more strong value proof tool proof electronics produced. On the other hand, if the interception process done without authority or no fulfil procedure applicable law, then results interception the potential lost strength proof and can was set aside by the judge in the trial process. Therefore That position interception in system law Indonesian criminal law does not only related with aspect prohibitions and authority, but also related directs with effectiveness proof in case criminal based technology information as with effectiveness arrangement action criminal based on a number of factors following.

1) Effectiveness Arrangement Criminal Act of Interception Based on Legal Factors

Theory of effectiveness enforcement law according to Soerjono Soekanto explain that factor law is one of the very determining elements succeed or whether or not something rule law implemented in society. Good law is law that is capable give certainty, justice, and benefit for public so that can implemented in a way effective by the authorities enforcer law and citizen.[21] With Thus, the effectiveness something regulation legislation is greatly influenced by the quality substance the laws that govern it.

Legal factors related with to what extent the regulations legislation in Indonesia is capable arrange in a way clear about definition interception, space scope prohibited acts, authority do interception, procedures implementation interception, as well as use results interception as tool proof in the judicial process criminal law. Clarity arrangement the become important Because interception is in a sensitive position, namely between protection right privacy citizens and interest enforcement law.

Arrangement about interception in Indonesia at the moment This Still spread in various regulation legislation. Regulations main there is in Constitution Number 1 of 2024 concerning Amendments Second Constitution Number 11 of 2008 concerning Information and Electronic Transactions Article 31 of the Law Electronic Information and Transactions are basically forbid everyone does

[20] Decision Court Constitution Number 5/PUU-VIII/2010.
[21] Soekanto, S., *op.cit.*, p. 8.

interception or tapping to information electronics and/ or document electronic belonging to someone else without right or oppose law. Provisions the become base criminalization to action tapping illegal in system Indonesian law.

Constitution Information and Electronic Transactions have not yet give comprehensive settings about mechanism interception. Law the more Lots arrange prohibitions and threats criminal, but not yet in a way details arrange procedure implementation interception, mechanism supervision, standards validation results interception, as well as protection to rights the party that becomes object interception. Condition This cause room sufficient interpretation wide in practice enforcement law.

Problems about incompleteness substance law the Once become attention Court Constitution in Decision Number 5/PUU-VIII/2010. In the decision said, the Court Constitution confirm that tapping is form restrictions to right basic man so that the settings must done through law. Court state that tapping touch right privacy a person who is guaranteed by the constitution so that the procedures and methods No Enough only arranged through the rules below Constitution.

Consideration Court Constitution the show that interception No just problem technical investigation, but also concerns protection right constitutional citizens. Therefore that, arrangement effective interception should capable give balance between need enforcement law and protection right privacy public.

If compared to with several other countries, Indonesia to moment This Not yet own Constitution specifically which comprehensive arrange about interception or wiretapping. Existing settings Still nature sectoral and distributed in various laws, such as Constitution Commission Eradication Action Corruption Crime, Law Narcotics, Law State Intelligence, as well as Constitution Electronic Information and Transactions. Conditions the cause occurrence fragmentation potential regulations cause difference interpretation in practice.

Problems substance law is also seen in the use of results interception as tool proof electronically. Although Article 5 paragraph (1) of the Law Electronic Information and Transactions have confess information electronics and/ or document electronic as tool proof valid law, but until moment This Not yet there is settings that are details arrange standard validation tool proof electronic results interception. In fact, in practice modern proof, validation tool proof electronic become very decisive aspect for ensure authenticity, integrity, and reliability of electronic data.

evidence electronic only can used optimally when supported by mechanisms clear authentication and validation so that data integrity can accountable in a way law.[22] Without existence clear standards, results interception potential questioned in the judicial process, both about legality his earnings and about authenticity of the submitted data as tool proof.

[22]Makarim, E., *op.cit.*, p. 287.

Weakness substance law the can seen in several cases that have ever happened in Indonesia. In the case of wiretapping involving Commission Eradication Corruption, debate emerging laws No only about content results wiretapping, but also regarding base laws and mechanisms its implementation. Likewise in case Bjorka data leak and various phishing and social *engineering* cases, authorities enforcer law often face difficulty when must prove connection between the electronic data obtained with identity perpetrator Because not yet existence standard proof real electronics uniform.

2) Effectiveness Arrangement Criminal Act of Interception Based on Law Enforcement Factors

Enforcement factors law own a very important role Because characteristics crimes handled different with action criminal conventional. In crime mayantara, the object being examined No Again object physical that can seen in a way directly, but electronic data, systems information, digital recordings, metadata, activity logs networks, and various form other digital evidence. Conditions the demand apparatus enforcer law for own ability more technical complex compared to with handling action criminal conventional.

Development technology information has change pattern crime at a time change need system justice criminal. Therefore that, the apparatus enforcer law sued for capable understand development technology so as not to left behind from perpetrator crimes that exploit technology information as means do action criminal.[23] Opinion the show that competence source Power man is very determining factor success enforcement law to crime base technology.

One of frequent obstacles faced apparatus enforcer law is limitation ability technical in do identification, security, and analysis tool proof electronics. Not all investigator own background behind or adequate training in the field of digital forensics. As a result, the data collection process tool proof electronic often face various obstacles, start from error procedure foreclosure device electronics, error in the data extraction process, until inability guard integrity tool digital evidence obtained from location incident.

Problems the become the more important Because in case interception, quality proof is highly dependent on ability apparatus in guard authenticity and integrity of electronic data. Evidence electronic own different characteristics with tool proof conventional because it is very easy duplicated, moved, modified, even deleted without leave easy trail recognized by lay people. Therefore that, the apparatus enforcer law must own ability special in handle digital evidence so as not to happen damage or data changes that can be influence mark the proof.

Limitations ability technical factors enforcer law is also related with coordination inter-agency enforcer law. In the system justice Indonesian criminal law, the process of proof No only involving investigator police, but also involves prosecutor

[23]Arief, BN *op.cit.*, p. 52.

prosecutor general public, digital forensic experts, and judges who will evaluate tool proof at the trial. If there is difference understanding about validity tool proof electronics among law enforcement officers law said, then the proof process can become No effective.

System justice criminal is something a system consisting of on interconnected subsystems related and mutual influence. Success system the determined by the level coordination and synchronization between institution enforcer law.[24] With thus, the weakness coordination between investigators, prosecutors and expert forensics potential cause problem in proof case interception.

Factor constraints enforcer law can also seen from development very fast technology. The perpetrator crime mayantara often use technology that continues to growing, such as network *virtual private network* (VPN), encryption communications, overseas servers, cloud computing technology, to application communication that applies end-to-end encryption system. Condition the often causes ability apparatus enforcer law left behind compared to with methods used perpetrator.

Phenomenon the seen in various case crime mayantara that occurred in Indonesia, including case data leak carried out by Bjorka. In this case the apparatus enforcer law face difficulty for identify perpetrator in a way certain because use identity anonymous, cross- border digital infrastructure, as well as location data storage that is external indonesian jurisdiction. conditions this show that success proof in case mayantara No only determined by the existence of tool evidence, but also by ability apparatus for browse and connect tool proof the with perpetrator.

The same problem also often occurs appear in cases of phishing and social engineering. Although there is proof in the form of catch screen conversations, transaction data electronic, or communication log, apparatus enforcer law still must prove Who the perpetrator behind account or device certain. In many case, perpetrator use identity fake account loans, as well as account container that makes the identification process difficult. Therefore that, quality investigations are highly dependent on the ability apparatus in do digital analysis and digital profiling of perpetrator.

If analyzed use theory effectiveness enforcement law so factor enforcer law show that effectiveness arrangement action criminal interception in Indonesia is still face various obstacles. Obstacles the covering limitations competence technical apparatus in digital forensics field, not yet evenly distributed training related proof electronics, differences understanding about validation tool proof electronics, as well as challenge development more technology fast compared to ability adaptation apparatus enforcer law. Conditions the cause implementation

[24] Muladi. (2002). *Democratization, Human Rights Humans and Legal Reform in Indonesia.* Jakarta: The Habibie Center, p. 112.

arrangement interception in practice Not yet fully capable answer complexity proof crime the increasingly large mayantara develop.

Effectiveness arrangement the Not yet can walk optimally when No balanced with improvement capacity source Power man apparatus enforcer law. Therefore that, strengthening digital forensic competency, improvement training technical, as well as harmonization understanding between institution enforcer law become very important needs in effort increase effectiveness proof action criminal interception in crime mayantara.

3) Effectiveness Arrangement Criminal Act of Interception Based on Law Enforcement Factors

Action criminal interception and crime mayantara factor facilities and infrastructure own a very important role because the proof process is very dependent on technology. Different with action criminal conventional which is generally relying on goods proof physical, proof action criminal interception more Lots rely on electronic data, digital devices, recordings communications, system logs, metadata, and various form other digital evidence. Therefore that, ability apparatus enforcer law in acquire, secure, inspect, and validate tool proof electronics are greatly influenced by availability adequate digital forensic facilities.

Digital forensics is a scientific process that is used for identify, collect, maintain, analyze, and present digital evidence so that can used in the legal process. [25]The process needs device hardware and devices special software that is capable guard data integrity since first acquired until submitted as tool evidence in court. Without support facility said, the risk damage, loss, or electronic data changes become the more big.

One of facilities that have role important in proof crime mayantara is digital forensics laboratory. Laboratory This used for do data extraction from device electronics, metadata analysis, data recovery that has been deleted, activity log check system, to the authentication process tool proof electronics. The existence of digital forensics laboratory becomes very important Because results examinations carried out in the laboratory the often become base for investigators, prosecutors and judges in evaluate validity tool proof electronics.

Availability digital forensic laboratories in Indonesia are still face various limitations. Not all regional police unit own complete digital forensic facilities. In many cases, examination tool proof electronic Still must conducted in the laboratory certain ones that have ability technical more high, such as laboratory forensics level center or laboratories located in cities large. As a result, the inspection process tool proof electronic often need a longer time compared to with inspection tool proof conventional.

[25] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.).* Burlington: Academic Press, p. 7.

Proof action criminal interception also requires device soft special for do electronic data analysis. various device soft forensics used for browse digital activities, identifying data changes, extracting communication electronics, as well as do verification to authenticity information electronics. One of the challenge the biggest in digital forensics is ensure that tools used capable produce data that can be accountable in a way scientific and legal. [26]Therefore that, quality device software and methods examination used own influence direct to validity results inspection.

Other related problems with facilities and infrastructure development very fast technology. The perpetrator crime mayantara Keep going utilise technology new for hide identity and activities they. Use technology encryption, communication based *end-to-end encryption,* data storage based on *cloud computing,* network *virtual private network* (VPN), up to the use of overseas servers becomes challenge alone for apparatus enforcer law. In the condition Thus, the facilities available investigations must capable follow development technology so as not to left behind from methods used perpetrator.

Limitations facilities and infrastructure are also seen in handling various case crime mayantara which involves data in amount big. In the case of data leaks carried out by Bjorka, for example, the authorities enforcer law faced with the need for analyze data in scale large spread across various system electronics. Situation the need support infrastructure technology strong, good information from side capacity storage, capability data analysis, as well as system security adequate information.

Problems similar also appears in cases of phishing and social engineering. In matters said, investigators often must browse digital footprints spread across various communication platforms, social media, applications message instant, until system banking electronics. The process need device capable analysis integrate various data sources so that they can produce the whole picture about activity perpetrator. If available facilities limited, then the identification and proof process become more difficult done.

Success use tool proof electronic in the legal process it is very dependent on the ability system for guard authenticity and integrity of electronic data. Therefore that, besides need clear regulations, proof electronics also require support technology that is capable ensure that the data obtained No experience change during the inspection process. This is show that factor facilities and infrastructure own very close relationship with validity tool proof electronics.

Effectiveness arrangement action criminal interception in Indonesia is still face various obstacles. Obstacles the covering Not yet evenly distributed digital forensic facilities, limitations device analysis electronics, high cost procurement

[26] Garfinkel, S. (2010). "Digital Forensics Research: The Next 10 Years."*Digital Investigation,* 7, pp. 65.

technology investigation cyber, as well as quickly development technology used perpetrator crime mayantara. Condition the causes the process of identification, collection, and validation tool proof electronic Not yet can implemented optimally throughout Indonesia.

Effectiveness arrangement action criminal interception No only determined by quality regulation and competence apparatus enforcer law, but also greatly influenced by the availability of adequate facilities and infrastructure. Without support modern and widespread digital forensic facilities, the process of proof action criminal interception will still face various potential obstacles reduce effectiveness enforcement law to crime mayantara.

3.2. Identification Process Perpetrators and Evidence in the Case Criminal Act of Interception in the Scope Mayantara

Identification is one of the stages important in the enforcement process law criminal Because functioning determine and ensure connection between perpetrator, event criminal, victim, and goods evidence found in something matter. In perspective law criminal, identification No only interpreted as a process of recognizing someone, but also as a series action scientific and juridical aims get certainty about identity subject and related objects with action criminal. Therefore Therefore, the success of the investigation process is very dependent on the accuracy identification carried out by the authorities enforcer law.

Identification can understood as a process of recognition or determination identity based on characteristics certain things that can differentiate somebody or something object with others. Identification is a process for find and determine need or existing deficiencies through activity data collection and analysis so can obtained accurate information about object being studied.[27] Although definition the originate from field management training, in a way conceptual identification still emphasizes the process of collecting and processing information to obtain certainty about something condition or object certain.

Identification own deeper meaning specific. Identification is a scientific process for determine identity somebody or something object based on characteristics possessed so that can used for interest investigation and evidence. [28]The process can done through various methods, such as inspection fingerprints finger, DNA examination, administrative data matching, analysis documents, as well as digital forensic examination in case based technology information.

Position identification in system justice Indonesian criminal law is very important Because be one of base for apparatus enforcer law in determine direction investigation. According to M. Yahya Harahap, the investigation aims for search and collect evidence to make bright something action criminal as well as find the

[27] Darmawan, D., *et al.* (2021). "Planning Data Collection as Identification Need Training Institution Training."*Journal of Nonformal Education and Community Empowerment,* 2(1), p. 72.
[28] Idries, AM (2013). *Implementation Knowledge Medical Forensics in the Investigation Process.* Jakarta: Sagung Seto, p. 45.

suspect.[29] For reach objective said, investigators must moreover formerly do identification to all over related elements with action criminal, including identity perpetrators, modus operandi, tools used, and goods evidence found. With Thus, identification become step decisive start success of the proof process at the stage next.

Identification process generally done through inspection physique to perpetrators, witnesses, victims, and goods evidence found at the scene incident case. Investigator can use fingerprints fingers, photos, CCTV footage, document identity, as well as information witness for ensure identity someone who is suspected involved in action criminal. The evidence found was also relatively easy recognized Because shaped physical and can observed in a way directly. Therefore that, the identification process in crime conventional more Lots based on material evidence and presence physique perpetrator.

Development technology information has change characteristics action criminal and give rise to challenge new in the identification process. In crime mayantara (*cybercrime)*, perpetrator No always present in a way physical onsite incident, but rather do his actions through network computers and systems electronic crime mayantara is form crimes that exploit technology information as means, objects, and environment occurrence action criminal. Characteristics the causing the identification process in crime mayantara become more complex compared to with crime conventional.

Complexity the appear Because identity perpetrators in the room cyber often disguised through use account fake, changing IP address, foreign server, network *virtual private network* (VPN), as well as various technique anonymization others. As a result, identification No Again only focused on identity physique someone, but also have to capable connect certain digital activities with responsible individual answer on activity in the condition thus, investigators no enough only depend on method identification conventional, but rather must use digital forensic approach for browse footsteps electronics left by the perpetrator.

Through digital forensics investigator can do identification to account, device electronics, metadata, activity logs network, as well as communication suspected electronics related with action criminal. Therefore that, identification in crime mayantara No only aim find Who the perpetrator, but also the aim build connection between perpetrator with digital activities that become object investigation.

Identification own very important position Because related direct with proof element action criminal. Investigator must capable identify who did it interception, device what is used, system which electronics to be targets, and How connection between perpetrators and tools proof electronics found. Failure in the

[29] Harahap, MY (2016). *Discussion Problems and Application of the Criminal Procedure Code: Investigation and Prosecution*. Jakarta: Sinar Grafika, p. 109.

identification process can cause tool evidence obtained lost relevance or even No can used for prove involvement somebody in action alleged crime.

4. Conclusion

Effectiveness Regulation Legislation Concerning Criminal Procedure Criminal Interception in Indonesia basically has available through various regulation legislation, including the Law Electronic Information and Transactions, Telecommunications Law, Law State Intelligence, Law Narcotics, as well as a number of regulations sectoral others. Existence regulations the show that the country has give base law for protection communication electronic at a time give authority certain to apparatus enforcer law for do interception in frame enforcement law. There is no law yet comprehensive settings about interception and validation tool proof electronic cause emergence difference interpretation in practice enforcement law. Identification Process Perpetrators and Evidence in Case Criminal Act of Interception in the Scope Mayantara own different characteristics with action criminal conventional. Identification perpetrator No Again based on the existence physique someone, but rather done through search digital identity, activities electronics, IP addresses, metadata, activity logs system, as well as various other digital footprints. Therefore that, the identification process needs a digital forensic approach that is capable of connect activity electronic certain with individuals who can asked accountability criminal. On the other hand, identification goods proof No only done to device electronics used in action criminal, but also against information electronics and documents electronics stored in it.

5. References

Journals:

Ashari, A. (2017). “Peranan Barang Bukti Dalam Proses Perkara Pidana”. *Al Hikam*, 1(3).

Astuti, S. A. (2017). “Perluasan Penggunaan Bukti Elektronik (*Evidence of Electronic*) Terkait Ketentuan Alat Bukti Sah atas Perbuatan Pidana di Ruang Mayantara (*Cyberspace*)”, *Pagaruyuang Law Journal*, 1(1).

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*, Article 1–13.

Darizta, *et al*. (2023). "Barang Bukti dalam Hukum Pembuktian di Indonesia." *Lex Stricta: Jurnal Ilmu Hukum*, 2(2).

Darmawan, D., *et al*. (2021). “Perencanaan Pengumpulan Data sebagai Identifikasi Kebutuhan Pelatihan Lembaga Pelatihan.” *Journal of Nonformal Education and Community Empowerment*, 2(1).

Darwis, N. (2019). “Kriminology Pada Bidang Kebijakan : Cyber Securty”. *Jurnal Ilmiah Hukum Dirgantara*, 9(2).

Garfinkel, S. (2010). “Digital Forensics Research: The Next 10 Years.” *Digital Investigation*, 7.

Hamdi, S., & Efendi, S. (2022). "Konsep Keadilan Delik Pembunuhan Dalam Hukum Positif Indonesia dan Hukum Islam", *Maqasidi: Jurnal Syariah Dan Hukum*, 2(2).

Pramata, A. G. (2021). "Analisis Kekuatan dan Nilai Pembuktian Alat Bukti Elektronik Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016", *Verstek*.

Rohman, *et.al*. (2024). "Sistem Pembuktian Dalam Hukum Pidana Indonesia Dan Tantangan Dalam Proses Peradilan", *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3).

Syah, R. S., & Ali, D. (2019). "Kebijakan Pidana Dalam Penanggulangan Tindak Pidana Carding Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik", *Jurnal Ilmiah Mahasiswa Bidang Hukum Pidana*, 3(4).

Trisnawati, T., & Hanifah, S. (2024). "Perkembangan Alat Bukti Elektronik Hasil Peretasan (Hacker) Sebagai Alat Bukti Dalam Tindak Pidana", *Multidisciplinary Indonesian Center Journal* (*MICJO*), 1(3).

Wibawa, I. (2016), "Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme)", *Masalah - Masalah Hukum*, 45(4).

Books:

Adji, I. S. (2009). *Korupsi dan Penegakan Hukum*. Jakarta: Diadit Media.

Adriaman, M. (2024) *Pengantar Metode Penelitian Ilmu Hukum*. Sumatera Barat: Yayasan Tri Edukasi Ilmiah.

Ali, M. (2015). *Dasar-Dasar Hukum Pidana*. Jakarta: Sinar Grafika.

Arief, B. N. (2007). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, Jakarta: Raja Grafindo Persada.

Arief, B. N. (2008). *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan penyusunan Konsep KUHP Baru*, Jakarta: Kencana.

Arief, B. N. (2012). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: RajaGrafindo Persada.

Arief, B. N. (2016). *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana.

Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*, Jakarta: Sinar Grafika.

Asshiddiqie, J. (2010). *Konstitusi dan Konstitusionalisme Indonesia*. Jakarta: Sinar Grafika.

Bakhri, S. (2015). *Sistem Peradilan Pidana Indonesia*. Yogyakarta: Pustaka Pelajar.

Barkatullah, A. H. (2019). *Hukum Transaksi Elektronik di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia*. Bandung: Nusamedia.

Internet:

Komdigi, (2015), "Penyelarasan Draft RUU Tata Cara Intersepsi", diakses melalui https://www.komdigi.go.id/berita/berita-kominfo/detail/penyelarasan-draft-ruu-tata-cara-interseps, Accessed on 12 January 2026, at 14:13 WIB.

Nanda Akbar Gumilang, "Pengertian Identifikasi: Proses, Bentuk, dan Contohnya" Accessed from https://www.gramedia.com/literasi/indentifikasi/, accessed 14 January 2026, at 20:36 WIB.