Ekasakti Journal of law and Justice
e-ISSN: 2987-436X | p-ISSN: 2987-7954
Volume 3, Issue 1, June 2025
Website: https://ejrev.org/law

Judge's Consideration of Evidence in the Crime of Illegal Access

Firdaus[1*], Bisma Putra Pratama[2]
[1,2] Universitas Ekasakti, Padang, Indonesia

[*]Corresponding Author: firdausbrigade42@gmail.com

Article Info

Article History
Revised : 2025-09-15
Accepted : 2025-10-17
Published : 2025-10-25

Keywords:
Consideration; Judge; Evidence

Abstract

The approach used is the Normative Juridical approach. The data used is secondary data collected through literature studies. The proof by the judge of the crime of illegal access in Decision Number 62/Pid.Sus/2020/PN Pti and Decision Number 10/Pid.Sus/2021/PN Pli is by means of evidence and corroborated by the judge's conviction through a criminal justice process. To determine that a criminal act has occurred, law enforcement officials must prove that the suspect has met the criminal elements suspected or charged. The evidence used is electronic documents and electronic information. The electronic documents in decision number 62/Pid.Sus/2020/PN Pti are print out data systems in the form of IMEI and MAC Address, printout transaction data and transaction data by the Shoppe seller account (seller) while in decision number 10/Pid.Sus/2021/PN Pli is 1 (one) bundle of printed credit delivery transaction reports through the Digipos application and 1 (one) sheet of screenshot prints of the DigiPos account. Application of Criminal Procedure by Judge where the defendant has been legally and convincingly proven guilty of committing a criminal act "Participating in deliberately and without the right to access the Electronic System belonging to another person in any way." Regarding the Crime of Illegal Access In Decision Number 62/Pid.Sus/2020/PN Pti, the judge sentenced the defendants to imprisonment for 9 (Nine) months each and a fine of Rp.100,000,000,000 (one hundred million rupiah) each with the provision that if the fine is not paid, it will be replaced with imprisonment for 3 (three) months each and Decision Number 10/Pid.Sus/2021/PN Pli judge impose a penalty on the Defendant therefore with a prison sentence of 2 (two) years and 6 (six) months and a fine of Rp300,000,000.00 (three hundred million Rupiah) with the provision that if the fine is not paid, it will be replaced with imprisonment for 6 (six) months.

INTRODUCTION

In addition to having a positive impact, the use of internet technology also has a negative impact, such as cybercrime. The Internet has made crimes that were once conventional (such as threats, theft, defamation, pornography, gambling, fraud and terrorism) now massive crimes, both committed individually and in groups with a very small risk of being caught with greater consequences for both society and the state[1].

The phenomenon of information technology crime is a relatively new form of crime when compared to other forms of crime that are conventional. Information technology crimes emerged at the same time as the birth of the technological revolution. As stated by Tubagus Ronni Rahman Nitibaskara, social interaction that minimizes physical presence is another

[1] Petrus Reinhard Golose, *The Development of Cybercrime and Efforts to Handle It in Indonesia by the National Police*, Banking and Central Bank Law Bulletin, Vol. 4 (2), 2016, pp. 29-47

DOI: https://doi.org/10.60034/q6ktxr03

characteristic of the information technology revolution. With this kind of interaction, the deviation of social relations in the form of cybercrime will adapt its form to the character[2].

In addition to *carding*[3], cyber crime can be in the form of *deface* as committed by Dani Hermansyah on April 17, 2004. Dani Hermansyah changed or changed the appearance of a website by changing the names of existing parties with the names of fruits on the www.kpu.go.id site which resulted in a decrease in public trust in the election that was taking place at that time. It is feared that in addition to the names of the parties that are changed, it is not impossible that the numbers of voters entering there will be unsafe and can be changed, even though the funds spent on the information technology system used by the KPU are very large.

Another form of cybercrime is to take advantage of a server security system gap or *hole cross server scripting* (XXS) that exists on a site. XXS is an application weakness on the server that allows users to insert other command lines. Usually the command inserted is Javascript as a trap, so that the hole maker can get information about the data of visitors who interact on the site. The more famous a site they deface, the higher the sense of pride they get. This technique is also the mainstay when there is *a cyberwar* between Indonesian *hackers* and Malaysian *hackers* caused by the recognition of Reog culture by the Malaysian Government, resulting in the destruction of Indonesian and Malaysian government websites by hackers of both countries[4].

In Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions as a special legal norm, there are also new legal principles, which are different from the existing legal system as stipulated in the Criminal Code and the Criminal Code. One of them is about electronic evidence that has just been recognized as a valid evidence in the law of evidence in Indonesia; Where before this law was passed, in terms of proving this cyber crime always came up against the limitations of the scope of evidence while this cyber crime is increasingly frequent and requires actual proof[5] . The law on electronic transactions has also been updated with Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

The aspect of proving the crime of illegal access to computers is often constrained by certain obstacles. The existence of obstacles in proof will cause difficulties in ensnaring criminal acts by the perpetrator. In Indonesia, although there are already rules to eradicate internet crime, the prosecution of *cybercrime* cases is often obstacled, especially in the arrest of suspects and confiscation of evidence.[6] The tracking results can only find an IP address of an internet perpetrator. It will be even more difficult if you use an internet café because until now it is still rare for internet cafes to register their service users so that it is impossible to know who is using the internet at the time of a criminal act. [7]

---

2 Tubagus Ronny Rahman Nitisbaskara, *When Crime Is Sovereign: An Approach to Legal Criminology and Sociology*, Civilization, Jakarta, 2001, p.38

3 Bayu Septya Yuda, "Efforts to Counter the Crime of Credit Card Personal Data Theft (Carding) in Online Transactions", Bachelor of Law Thesis, Bandar Lampung: Faculty of Law, University of Lampung, Bandar Lampung, 2019, p.4

4 Aan Andrew Johanes Pahajow, 2016, Proof of Cybercrime and Efforts to Overcome It According to Positive Law in Indonesia, Lex Crimen, 5(2): 91-99, https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/11121 downloaded March 2, 2024

5 Sahuri Lasmadi. 2014. Regulation of Evidence in Cyber Crimes. Journal of Legal Sciences:1-23, https://online-journal.unja.ac.id/index.php/jih/article/view/1947 download March 12, 2024

6 Budi Suhariyanto, *Information Technology Crime (Cybercrime) Urgency and Arrangement of Legal Loopholes*, Raja Grafindo Persada, Jakarta, 2012, p.

7 Accessed from https://balianzahab.wordpress.com/artikel/penyidikan-terhadap-tindakpidana-cybercrime/. On July 20, 2024. .

Law enforcement officials in handling cybercrime cases always have difficulty in trying to prove, especially that it is important and crucial. It is not uncommon for victims, witnesses and perpetrators to remain silent until proving later becomes very important. Therefore, judges must be careful, careful and mature in assessing and considering evidentiary issues. Examine to the minimum limit the "evidentiary strength" or "*evidence"* of each piece of evidence Article 184 of the Criminal Code.[8]

The evidence also provides a strong argument basis for the public prosecutor to file a charge. Evidence is seen as objective, and provides information to the judge to draw conclusions about a case being heard. Especially in criminal cases, proof is essential because what is sought in criminal cases is material truth. [9] Proof of the crime of illegal access can be seen in Decision Number 62/Pid.Sus/2020/PN Pti and Decision Number 10/Pid.Sus/2021/PN Pli. In both cases, based on the evidence carried out, the Judge believed that the defendant was guilty of committing a criminal act "deliberately and without rights or unlawfully accessing the computer and/or electronic system belonging to another person in any way by violating, breaking through, exceeding or breaking the security system together or acting individually" in violation of Article 46 paragraph (3) *of the law* Article 30 (3) of Law of the Republic of Indonesia Number 19 of 2016 concerning amendments to Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions *in conjunction with* Article 55 paragraph (1) 1 of the Criminal Code. The main issue discussed is the proof and application of criminal penalties by the Judge against the perpetrators of the crime of illegal access in Decision Number 62/Pid.Sus/2020/PN Pti and Decision Number 10/Pid.Sus/2021/PN Pli?

RESEARCH METHODS

The specification of the research is *descriptive analytical,* with a normative juridical approach supported by empirical juridical approaches. The types of data used are secondary data and primary data. Secondary data was obtained from document studies, primary data was obtained by means of interviews. The data obtained was then analyzed qualitatively.

RESULTS AND DISCUSSION

Judge's Consideration of Evidence in the Crime of Illegal Access

Illegal access or often referred to as unauthorized access is defined as a crime that occurs when a person enters or infiltrates a computer network system illegally, without permission, or without the knowledge of the owner of the computer network system in which he or she owns. Illegal access is one of the various types of cybercrime, several types of illegal access, namely: First, illegal access as one of the pure crimes, where people who commit crimes deliberately and deliberately and plan to destroy and steal an information system or computer system;

Second, illegal access as an act of gray crime, where this crime is not clear whether it is a criminal crime or not because he committed a break-in but did not damage or steal an information system or computer system; Third, illegal access that attacks individuals, namely crimes committed against others with the motive of revenge or prank that aims to damage the good name and provide personal satisfaction to the perpetrator; Fourth, Illegal access that attacks copyright. This crime is committed against the work of a person with the motive of duplicating, marketing, or altering something that aims for personal or public interest for the sake of material or non-material; Fifth, Illegal access that attacks the government. This crime makes the government an object with the motive of terror, hijacking, or damaging the security of a government that aims to disrupt the government system or destroy a country.

---

[8] Andi Hamzah; Budi Marsita, *Criminal Aspects in the Field of Online Transactions*, Sinar Grafika, Jakarta, 2015, p. 38

[9] Eddy Hiariej, *Theory and the Law of Proof*, Erlangga, Jakarta, 2012, p. 96

One example of a case of illegal access is in the case of decision number 62/Pid.Sus/2020/PN Pti, which was carried out by H (Supervisor of Marketing Agent of J&T express Pati 04 Central Java branch) and Z (Marketing Area Coordinator of Pati Express Pati 10 Central Java branch). They committed this act starting from the defendants knowing the application of the sprinter / courier of PT. J&T by trying one ID one by one randomly, after successfully logging in, the defendants accessed the sprinter application and then created a seller and buyer account on Shopee. then the defendants carried out fictitious transactions as if there were buying and selling, where after the transaction was completed with the choice of transactions using the COD (*Cash On Delivery*) method, in other words, the goods sent by the J&T courier would be paid in cash by the buyer when the goods arrived and the money was paid to J&T express which made the delivery.

Then the defendants input the receipt number/barcode scan on the purchase and sale receipt that was previously made, so that it is as if the courier has arrived at the destination address to deliver the goods/items to be sent and the money has been received by the courier, that with the barcode scan of the transaction receipt, the J&T Application system will respond to the results of the scan so that the transaction is completed and COD (*Cash On Delivery*) money/payment when receiving goods) can be disbursed/transferred to the Shopee online shopping seller's account (in this case to the account used by the defendants).

The defendants were not authorized to enter the J&T Sprinter/Courier application because the application was only owned by the J&T Sprinter/courier. As a result of the defendant's actions, PT. J&T Central Java Branch and PT. J&T Jakarta suffered losses with a total amount of approximately Rp. 129,340,435,- (one hundred and twenty-nine million three hundred and forty thousand four hundred thirty-five rupiahs);

Evidence in the trial examination process has a purpose for the public prosecutor, namely as a form of effort to convince the Judge, namely based on the existing evidence to declare a defendant guilty according to the letter or indictment record. The purpose of proof for the defendant or legal advisor is as an effort to convince the Judge, namely based on the available evidence to declare that the defendant is acquitted or released from prosecution or mitigating his crime. For the Judge, on the basis of the evidence, namely the existence of evidence in the trial, whether from the public prosecutor or legal advisor/defendant, the basis for making a decision is made.

In the theory of proof According to the Law Negatively, it is said that the system of *proof negatief wettelijk* lies between two systems that face to face, namely between the *system of positive proof of wettelijk* and the system of *proof of conviction intimate*. This proof system is a middle ground proof system that is based on the judge's beliefs to a certain extent. The judge cannot make a decision until it is clear to him that the event/fact really occurred, that is, it is proven to be true, so that there is a legal relationship between the parties.[10]

Assessing the evidentiary strength of existing evidence, several evidentiary systems are known, namely:[11] First, Positive Proof according to the Law, which is a system of proof that is only based on the evidence listed in the law. Second, the evidentiary system is only based on the judge's beliefs. In this proof, what stands out is the subjectivity of the judge. Third, Evidence based on the judge's conviction is based on the judge's logical consideration. In this system of proof, "a statement in which it is impossible or otherwise" will apply, meaning that something that according to common sense will happen. And fourth, Proof according to the Law

[10] Adami Chazawi, *The Law of Proving Criminal Acts for Judges, Prosecutors, and Police*, Jakarta: RajaGrafindo Persada, 2012, pp. 45-46.

[11] M. Yahya Harahap, *Discussion of Problems and Implementation of the Criminal Procedure Code for the Examination of the Court of Appeal, Cassation, and* Review, Second Edition, Sinar Grafika, Jakarta, 2008, p. 278.

negatively. In this system, proof is based on the existence or absence of evidence obtained from evidence, where the evidence is judged to be convinced that a person is guilty or innocent.

Furthermore, Article 183 of the Criminal Code states that: "A judge may not impose a criminal sentence on a person unless with at least two valid pieces of evidence he obtains the belief that an act really occurred and that it is the defendant who is guilty of committing it". From the provisions mentioned above, it can be stated that the Criminal Procedure Code adheres to a system of proof of negative law prosecution. So that Article 183 of the Criminal Code adheres to determine whether a defendant is guilty or not and to impose a criminal sentence on the defendant, it must:[12]1. His guilt is proven by at least two valid pieces of evidence; 2. And on the basis of evidence with at least two valid evidence, the judge obtained the conviction that the criminal act really occurred and that the defendant was guilty of committing it.

In principle, Electronic Information can be differentiated but cannot be separated from Electronic Documents. Electronic Information is data or data collections in various forms, while Electronic Documents are containers of Electronic Information. Article 5 paragraph (1) of the ITE Law can be grouped into two parts. First, Electronic Information and/or Electronic Documents. Second, printed results from Electronic Information and/or printed results from Electronic Documents.[13]

The defendant in the two above decisions was designated as a suspect for violating the criminal act of Article 55 Paragraph (1) 1 of the Criminal Code. In the explanation, before entering the explanation, it must first be understood the definition of electronic evidence which is data that is stored and/or transmitted through an electronic device, network or communication system. This data is needed to prove a crime that occurred in court, not the physical form of the electronic device. Information technology itself is defined as a technique for collecting, preparing, storing, processing, announcing, analyzing and/or disseminating information, as determined in Article 1 paragraph (3) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008.

Seen in the two decisions above, the evidence used is in the form of *printouts* which are electronic documents. In terms of electronic information/documents as evidence, Law No. 11 of 2008 also recognizes *printouts* as valid legal evidence. This is stipulated in Article 5 paragraph (1) of Law No. 11 of 2008 which states that electronic information and/or electronic documents and/or their printed results are valid legal evidence.

On the basis of this evidence, namely the existence of the evidence in the trial, it makes the judge confident in giving a verdict on the two decisions. This is in line with the theory of Negative Proof According to the Law *(Negatief Wettelijke Bewijstheorie),* which is based on the rules of proof set by the Law, but it must be followed by the Judge's conviction. In the *theory of the Negatief Wettelijke Bewijstheorie* there are at least two pieces of evidence used to state that the defendant's actions are proven and coupled with the judge's belief in the existence of the acts committed by the defendant.

The Criminal Application by the Judge Against the Perpetrators of the Crime of Illegal Access in Decision Number 62/Pid.Sus/2020/PN PTI and Decision Number 10/Pid.Sus/2021/PN Pli

The criminal justice system outlined by the Criminal Code is an "integrated *criminal justice system*". The integrated system is located on the basis of the principle of "*functional differentiation*" among law enforcement officials in accordance with the stage of the authority process given by law to each. Based on the integrated system, it is a joint function of law

[12] *Ibid*

[13] Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw*: *A Review of Aspects of Criminal Law*, Jakarta, PT. Tatanusa, 2012

enforcement officials, including the Police, Public Prosecutors, Judges, and Prisons which have their respective duties as follows: The judge's consideration is one of the most important aspects in determining the realization of the value of a judge's decision that contains justice (*ex aequo et bono*) and contains legal certainty, in addition to that it also contains benefits for the parties concerned so that the judge's consideration must be addressed carefully, well, and carefully. If the judge's consideration is not thorough, good, and meticulous, then the judge's decision derived from the judge's consideration will be canceled by the Supreme Court.

In both cases, the identity of the defendant is proven to be true and the defendant admits and justifies everything described about the identity of the defendant and in his physical and spiritual health, then the defendant can be held accountable for the actions he committed, thus the element of Everyone is fulfilled.

The element of deliberately and without rights or against the law accessing the computer and/or electronic system of another person in any way by violating, breaking through, exceeding or breaking the security system together or acting individually, Based on the facts revealed in the trial, along with the evidence submitted at the trial, that is, this element has been fulfilled.

The examination of a case also requires proof, where the results of the evidence will be used as a consideration in deciding the case. Proof is the most important stage in the examination at trial. Proof aims to obtain certainty that an event/fact submitted really occurred, in order to obtain a correct and fair judge's decision. The judge cannot make a decision until it is clear to him that the event/fact really occurred, that is, it is proven to be true, so that there is a legal relationship between the parties.

Freedom in exercising judicial authority is not absolute because the judge's duty is to uphold law and justice based on Pancasila, so that his decision reflects the sense of justice of the Indonesian people. Then Article 24 paragraph (2) emphasizes that: judicial power is exercised by a Supreme Court and the judicial bodies under it in the general judicial environment, the religious judicial environment, the military judicial environment, the state administrative judicial environment, and by a constitutional court.

Based on the judge's consideration, in the two verdicts of the crime of illegal access, the judge ruled that the defendants had been legally and convincingly proven guilty of committing a criminal act of "Participating in deliberately and without the right to access the Electronic System belonging to another person in any way". In Decision Number 62/Pid.Sus/2020/PN Pti, the judge sentenced the defendants to 9 (Nine) months in prison each and a fine of Rp.100,000,000,- (one hundred million rupiah) each with the provision that if the fine is not paid, it will be replaced with imprisonment for 3 (three) months each. And in Decision Number 10/Pid.Sus/2021/PN Pli, the judge sentenced the Defendant to imprisonment for 2 (two) years and 6 (six) months and a fine of Rp300,000,000.00 (three hundred million Rupiah) with the provision that if the fine is not paid, it will be replaced with imprisonment for 6 (six) months.

The verdict handed down by the judge in the two cases is in accordance with the theory of criminal responsibility, according to Simons, as the basis of criminal liability is the fault that is in the mind of the perpetrator in relation to the conduct that can be punished and based on that psychiatry the perpetrator can be reproached for his behavior. For the existence of fault in the perpetrator, several things related to the perpetrator must be achieved and determined in advance, namely:[14]

1. Responsible ability;
2. The relationship, the psychology between the perpetrators and the consequences caused (including behavior that is not contrary to the law in daily life;

[14] Oemar Seno Adji, *Professional Ethics and the Law of Criminal Responsibility of Doctors,* Erlangga, Jakarta, 1991, p. 34.

3. Dolus and culpa, mistakes are subjective elements of criminal acts. This is a consequence of his opinion that connects (unites) *straafbaarfeit* with error.

CONCLUSION

The judge's consideration of the evidence in the crime of illegal access in Decision Number 62/Pid.Sus/2020/PN Pti and Decision Number 10/Pid.Sus/2021/PN Pli is with evidence and corroborated by the judge's conviction through a criminal justice process. To determine that a criminal act has occurred, law enforcement officials must prove that the suspect has met the criminal elements suspected or charged. The evidence used is electronic documents and electronic information. The electronic documents in decision number 62/Pid.Sus/2020/PN Pti are print out data systems in the form of IMEI and MAC Address, printout transaction data and transaction data by the Shoppe seller account (seller) while in decision number 10/Pid.Sus/2021/PN Pli is 1 (one) bundle of printed credit delivery transaction reports through the Digipos application and 1 (one) sheet of screenshot prints of the DigiPos account.

Application of Criminal Procedure by Judge where the defendant has been legally and convincingly proven guilty of committing a criminal act "Participating in deliberately and without the right to access the Electronic System belonging to another person in any way." Regarding the Crime of Illegal Access In Decision Number 62/Pid.Sus/2020/PN Pti, the judge sentenced the defendants to imprisonment for 9 (Nine) months each and a fine of Rp.100,000,000,000 (one hundred million rupiah) each with the provision that if the fine is not paid, it will be replaced with imprisonment for 3 (three) months each and Decision Number 10/Pid.Sus/2021/PN Pli judge impose a penalty on the Defendant therefore with a prison sentence of 2 (two) years and 6 (six) months and a fine of Rp300,000,000.00 (three hundred million Rupiah) with the provision that if the fine is not paid, it will be replaced with imprisonment for 6 (six) months.

REFERENCE

Aan Andrew Johanes Pahajow, Proof of Cybercrime and Efforts to Overcome It According to Positive Law in Indonesia, Lex Crimen, 5(2): 91-99, https://ejournal.unsrat.ac.id/index.php /lexcrimen/article/ view/11121 download, 2016.

Adami Chazawi, *The Law of Proving Criminal Acts for Judges, Prosecutors, and Police*, Jakarta: RajaGrafindo Persada, 2012

Andi Hamzah; Budi Marsita, *Criminal Aspects in the Field of Online Transactions*, Sinar Grafika, Jakarta, 2015

Bayu Septya Yuda, "Efforts to Counter the Crime of Credit Card Personal Data Theft (Carding) in Online Transactions", Bachelor of Law Thesis, Bandar Lampung: Faculty of Law, University of Lampung, Bandar Lampung, 2019

Budi Suhariyanto, *Information Technology Crime (Cybercrime) Urgency and Regulation of Legal Loopholes*, Raja Grafindo Persada, Jakarta, 2012

Eddy Hiariej, *Theory and the Law of Proof*, Erlangga, Jakarta, 2012

Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw*: *A Review of Aspects of Criminal Law*, Jakarta, PT. Tatanusa, 2012

M. Yahya Harahap, *Discussion of Problems and Implementation of the Criminal Code for the Examination of the Court of Appeal, Cassation, and Review Sessions*, Second Edition, Sinar Grafika, Jakarta, 2008

Oemar Seno Adji, *Professional Ethics and Criminal Responsibility Law of Doctors,* Erlangga, Jakarta, 1991

Petrus Reinhard Golose, *The Development of Cybercrime and Efforts to Handle It in Indonesia by the National Police*, Banking and Central Bank Law Bulletin, Vol. 4 (2), 2016

Sahuri Lasmadi. Regulation of Evidence in Cyber Crimes. Journal of Legal Sciences:1-23, https://online-journal.unja.ac.id/index.php/jih/ article/view/1947, 2014.

Tolib Setiady, *Principles of Indonesian Penitentiary Law*, Alfabeta, Bandung, 2010

Tubagus Ronny Rahman Nitisbaskara, *When Sovereign Crime: An Approach to Legal Criminology and Sociology*, Civilization, Jakarta, 2001