JURNAL META-YURIDIS
No. P-ISSN : 2614-2031 / NO. E-ISSN : 2621-6450
Fakultas Hukum Universitas PGRI Semarang
Homepage: http://journal.upgris.ac.id/index.php/meta-yuridis/

Article History: *Received: 2023-06-07* *Accepted: 2023-08-04*
Published: 2023-08-31

ILLEGAL ACCESS THROUGH "WIRELESS FIDELITY" IN CRIMINAL LAW

Aida Dewi
Faculty of Law Widya Mataram University Yogyakarta, Indonesia.
Aidadewi170774@gmail.com

Hartanto
Faculty of Law Widya Mataram University Yogyakarta, Indonesia.
hartanto.yogya@gmail.com

Arvita Hastarini
Faculty of Law Widya Mataram University Yogyakarta, Indonesia.
arvitahastarini@gmail.com

Abstract: The internet is a sophisticated tool for exchanging information, various fields from law to medical sciences (medicine) have also used the internet on a large scale. The use of wireless fidelity is also quite attractive for those who need free internet access. But it is undeniable that in addition to some people hoping to use the free internet, it will also cause the desire of people who want to use it as a means of other crimes. The purpose of this study is to examine cases of internet data theft through wireless fidelity within the scope of criminal law. Our criminal law as the backbone, namely the Criminal Code, was used to study this problem (historical interpretation) and today there is a Telecommunications Law and an Electronic Information and Transaction Law. While using internet access without someone else's permission, is a violation of the law. Before entering into the study of how much loss quota (intangible objects) were stolen, the perpetrators had actually been able to be suspected by illegal access.

Keywords: Wifi, Access, Criminal, Law, ITE

INTRODUCTION

Basically, every technology is created to help humans. After technology is developed to be more effective and efficient to meet the intended needs, the old technology will be abandoned. The existence of technology (social media) for today's society seems irreplaceable. We seem to enjoy the freedom to communicate and access information. (Wahyu Widodo, 2019)

In the future, of course, personal/ individual to public dependence with various fields will be tied to dependence on the ITE world, including in the field of criminal law and sub-section ITE. A person's thoughts, intentions, and emotions can be manifested through bits. In fact, in cyberspace, many crimes that are more often called cyber crimes regulated in cyberlaw. Mayantara crimes in cyberspace can be in the form of conventional crimes or the actions of people who are then formulated/ criminalized as a new form of crime that only uses ITE means or that can only occur in cyberspace, but has a real impact. Therefore, cyberlaw is needed to be applied in cyberspace to maintain public order, including regulating sanctions for perpetrators of crime.(Widodo, 2013) The things described above will cause pro and con thoughts, but inevitably it will happen at least has begun in this era.

The combination of computer technology with telecommunications technology has been able to create networks (computer networks) that are global with various kinds of application developments, even in the field of education there are also various applications used by the Ministry of Research, Technology, and Higher Education. However, what needs to be added is that various applications, including those used for the public interest, should not overlap taoi integrated properly.

The increasing interest of people to use computers, both for office purposes and household purposes, resulted in greater dependence of people on these sophisticated equipment. This condition is a common symptom of any change. We can perceive that as technology continues to develop, it has a significant effect on the behavior and mentality of citizens. Advances achieved in the field of technology will also affect changes in people's lives. Each society will always change from time to time. The development of influences from outside the environment will also develop changes in the community, both positive changes and negative changes. (Andi Hamzah, 1987)

Interconnection-networking (internet) is all interconnected computer networks using the global system standard Transmission Control Protocol/ Internet Protocol (TCP/ IP) as a packet exchange mechanism (switching communication) to serve at least 5.16 billion world internet users by 2023, equivalent to 64.4% of the world's population. Cindy Mutia Annur, 2023) The largest network of internet networks is called the Internet (capital I). This way of connecting circuits by this method is called internetworking (between networks). Understanding the internet (interconnection networking) is called an open-global communication network, by connecting millions/ billions of computer networks using various types and types, for example: telephone, and satellite

The positive impact is first, the internet as a communication medium is used

by internet users who communicate with other users in internet applications. For example: twitter, facebook, instagram, whatsapp, even miChat; Second, as a medium of data exchange using email, news groups, forums, where internet users around the world utilize it faster and cheaper than conventional information media. Third, as a medium for finding information, the internet helps humans who use the internet to get various desired information. For example, Google and Youtube as places to find information. Fourth, an easier and faster means for transactions and business by trading online. (Alcianno G.G, 2015)

In addition to the row of positive effects of the internet mentioned above, the internet also has a negative impact, the following are the negative impacts of the internet, namely first, pornography that is spread and with easy access to information including but not limited to pornography that makes internet users allegedly increase the number of criminal acts, for example related to immorality, defamation, fraud, gambling, or terrorism. Milder excesses are the impact of social pathologies. On the psychological side, the internet can also cause dependence and direct social interaction (social harmony). This can be overcome by education and healthy/ smart use of the internet. In the field of child and female protection, this has a quite worrying impact if no countermeasures are taken, the simple thing is that children are starting to be "addicted" to using gadgets/ cellphones, both at school and outside school.

Despite the positive and negative natural effects above, at least during this period, the flow of globalization of information is still growing in line with human civilization. Especially now when technological advances facilitate all human work and facilitate the entry of global world information flows with the internet. For that reason, the internet today requires people to include it in the list of basic human needs because (basically) everyone wants or needs the internet.

It must be realized that although indeed the level of speed and availability of internet networks in Indonesia still varies, and when people have not been able to reach to buy it, they can find a place that provides free access via wifi (Wireless Fidelity) in public facilities/places. That's why there are some people who want/ need the internet, then do everything possible to get free access or as cheap as possible. For example, using someone else's WiFi internet connection that radiates without the owner's permission, this event has clearly caused losses/ victims. Unbeknownst to the owner there are other people without permission, on the other hand, the owner who pays but someone else also uses. (Andrian Saputra, 2021) Maybe it doesn't really matter if people who subscribe to home wifi services have internet access with unlimited quota at a certain access speed (unlimited quota), but what if the internet access purchased is an internet wifi service that has a really limited quota (limited quota), it will certainly be very detrimental to users of the service because it can be used and spent by irresponsible people.

Indonesia is a country with a fairly large population of internet users and, actually this kind of case occurs a lot. Generally, the owner does not know about this theft because it is very

difficult to detect the perpetrators of theft, let's just say it is detected who is transmitting/ accessing on the laptop/ cellphone screen but the location of the position and who accesses illegally the location is not easily known to the general public. In fact, if the interpretation of the syllogism is carried out, this is the same as ordinary theft (KUHP) where the victim is materially harmed and in this case, the victim's loss is in the form of paying the cost of purchasing the wifi internet access service.

Article 362 of the Criminal Code as the backbone of the criminal law states that whoever takes something, which wholly or partly belongs to another person, to be possessed unlawfully, is threatened with a conventional criminal offense, namely theft. So using someone else's wifi internet without permission is included in the act of "taking" and using/enjoying. Then "internet access" on wifi can be interpreted as "goods". While other laws that can be used are Article 22 of the Telecommunications Law, namely: Everyone is prohibited from doing actions without rights, unlawful, or manipulating: access to telecommunications networks; and telecommunication services; and or to a special telecommunications network, which is threatened with a maximum penalty of 6 years and/or a fine of 600,000,000,-(IDR) But in this case the author immediately examines based on the latest law, namely the "ITE" Law.

Act. No. 19 of 2016 concerning ITE as amended by Law. No. 19 of 2016 (ITE) there is no article, that regulates the prohibition of stealing wifi internet and in the law only regulates the theft of electronic data belonging to other people in the form of accounts, passwords, data files, and others and has not regulated how about theft in the form of goods (intangible), namely wifi internet. Article 30 paragraphs (1), (2), and (3) of Law No. 11 of 2008 ITE as amended by Law No. 19 of 2016 (ITE) which can be related to cases of wifi internet theft. For the above reasons, the author chose this case to be investigated because many people are harmed in cases of wifi internet theft but victims do not know that they are victims, because the form of being harmed in this kind of act is classified as sophisticated and new technology that not all audiences easily understand.

MAIN PROBLEM

Based on the background description, a problem formulation can be taken about how the case of internet data theft through Wireless Fidelity is reviewed from the Criminal Law and the ITE Law, even though there is Law No. 36 of 1999 concerning telecommunications there are also articles that regulate but are less relevant in the development of advances in the world of information technology, so the author leaves aside.

METHOD OF RESEARCH

This research uses a type of normative legal research, namely legal research by examining secondary data materials (literature studies), using research on written legal materials. Then the data in the form of legal material that has been obtained is presented in the form of narrative text, and the description is arranged in a systematic, logical, and rational way. In the sense that all data obtained will be linked to each other according to

the study of the study of the study so as to form a complete unity. (Hartanto, et al, 2023)

RESEARCH RESULT AND DISCUSSION

In this era of globalization, the flow of information is very fast spreading, we can find out quickly what happens at the time and when legal events occur. That's all because of the internet network, the network is a digital network that connects devices with satellites that function to channel digital information between electronic devices. The internet makes it easy for everyone to access digital information whether it's in the form of writing, photos or images, until even videos we can see with our electronic devices in the form of *smartphones* and computers or laptops as long as the electronic devices are connected to the internet.

However, for the above reasons, human needs for the internet are getting higher and higher and giving rise to new products in the form of application programs that function as useful means of supporting the progress of the internet. Products in the form of application programs are the result of the development of "science and technology" which is made as a means for internet users to access in to public networks to search for data, transfer and find information. In addition to directly using the internet network from electronic devices such as *smartphones* and computers or laptops using certain providers that provide internet services, now internet devices appear that facilitate internet access to be shared, namely Wifi internet.

Wi-Fi (also written Wifi or WiFi) is a technology that utilizes electronic equipment to exchange data wirelessly (using radio waves) over a computer network, including a high-speed Internet connection. A device that can use Wi-Fi (such as a computer, video game, mobile phone, or digital audio) can connect to a network source such as the Internet through a wireless network access point. A Wi-Fi device can connect to the Internet when it is in the area of a wireless network connected to the Internet. Areas of one or more access points (interconnections) called *hotspots* can cover an area of several square/ *miles*. Wi-Fi provides services in private homes, large streets and shops, and public spaces through *Wi-Fi hotspots installed both free and paid. Business people, such as airports, hotels, and even small stalls, usually provide free* hotspots to attract visitors. Enthusiastic users or authorities who want to provide services or even promote businesses in certain places sometimes provide free Wi-Fi access. (Winarno Sugeng. 2010) Routers involving digital subscriber line modems or cable modems and WI-Fi access points, typically installed in homes and other buildings, provide Internet and internetwork access to all equipment connected to the router wirelessly or using a cable.

Because of the large number of internet users at this time raises various new complicated problems where crimes are committed using the internet (*cyber crime*). One of the crimes committed using the internet is about accessing unlawfully, both against wifi facilities and to obtain personal data of internet users, this crime is carried out with the aim of stealing internet user information. Criminal acts in the cyber / ITE field

were previously investigated based on the Criminal Code but in the development of the Law on ITE which is more appropriate to the times; In this regard, criminal law must keep up with the times. (Nelli Herlina, Dessy Rakhmawat, 2020)

Currently, a new legal regime known as cyber law has been born, which is taken from the word *Cyber* Law is a legal term related to the use of information technology, then there are those who call it the Law of Information Technology (*Law of Information Technology*). So in this writing *cyber* if identified with "cyberspace". The approach to protecting *cyberspace*, first is a technological approach and a legal approach (pre-emptive and preventive).

Seeing the current legal phenomenon, the development of science and technology that has been widely misused as a means of crime, it must always be anticipated with comprehensive legal regulations, with the hope that *cyber crime* can be overcome both conceptually in regulations and evidence systems. Furthermore, considering that law enforcement requires on the basis of that a person can be found guilty or not, in addition to his actions can be blamed on the basis of pre-existing laws (the principle of legality), also which actions are supported by the strength of valid evidence and can be held accountable (element of guilt). Such thinking is in accordance with Article I paragraph (1) of the Criminal Code "*Nullum delictum nulla poena sine praevia lege poenali"* which is no crime without fault". (Widodo, 2013)

Related to criminal law, Moeljatno defines it as part of the overall law of a country, hence the basics and rules for: (Moeljatno, 2008)

1. Determine the acts not to be done, which are prohibited, then certain criminal threats or sanctions for who violates them.
2. Determine when and in what cases those who have carried out such prohibitions may be charged or punished as threatened.
3. The method of criminal application can be carried out, if the person suspected of having violated the provision.

Due to the application of criminal law legislation related to the time and place of the act (Andi Sofyan, Nur Azisa, 2016), the principles of the limits of the enactment of criminal law according to locus *delictie* and *tempus delictie are known*. Regarding the tempus of the occurrence of criminal acts based on the principle of legality.

The principle of legality is a very fundamental principle, namely to determine whether a criminal law regulation can be applied to a criminal act that occurs; So if a criminal act occurs, it will be reviewed whether there are legal provisions and whether existing provisions can be applied to the criminal act that occurred. (Lidya Suryani Widayati, 2011) So in short, the principle of legality is related to the time of enactment of criminal law. In criminal law, the principle of legality implies that, it cannot be declared that the act can be criminalized, except on the strength of the criminal rules in the law that has existed first." (Prianter Jaya Hairi, 2016)

Moeljatno said that the principle of legality contains three meanings. First, there is no prohibition against criminal punishment if it has not been stated in a law in advance. Second, the determination of the occurrence of

crime should not use analogy (comparison). Third, arrangements in criminal law cannot be retroactive. (Moeljatno,2008) From the explanation above, we come to know that in determining an act or act, it can be said that criminal acts or criminal acts must go through a long and complicated study process. Because it is related to one's legal certainty, it should not be done carelessly.

Based on the explanation above, it will be analyzed related to the act of theft of internet access (wifi) in Indonesian criminal law. First, from the explanation of the theory at the beginning that in an act cannot be said to be a criminal act if it is not regulated in advance in writing in law. In the theft of wifi internet itself, the act of theft has actually been regulated in Article 362 of the Criminal Code regarding theft of objects. Meanwhile, in Article 30 paragraphs (1), (2), and (3) of Law Number 11 of 2008 Electronic Information and Transactions as amended by Law Number 19 of 2016 (ITE Law) there are regulations regarding access to computers and/ or electronic systems belonging to others intentionally and without rights or against the law. In this case there are two regulations that can apply, namely Article 362 of the Criminal Code and Article 30 paragraphs (1), (2), and (3) of the ITE Law.

The provisions of Article 362 of the Criminal Code have regulated "Whoever takes any thing, wholly or partly belonging to another person with intent to possess unlawfully, shall be punished with theft, with imprisonment for not more than five years". The Criminal Code is derived from Dutch colonial law, namely *Wetboek van Strafrecht voor Nederlandsch-Indie* (W.V.S.N.I). W.v.S. N.I is legally based on *Staatsblad* Year 1915 number 732 and entered into force on January 1, 1918. Therefore, the Criminal Code is still enforced accompanied by alignment of conditions in the form of revocation of articles that are no longer relevant. (Devosit Malensang, 2017) The problem is that when the Criminal Code is passed, the internet or wifi system has not been found, so it is necessary to conduct a study of Article 362 of the Criminal Code (KUHP).

The elements of Article 362 of the Criminal Code are as follows:

1. The act of "taking";
2. What is taken is an "item";
3. The goods must be "wholly or partly the property of others"; and
4. Taking it must be done "with the intent to possess the item unlawfully".

From the above elements, Article 362 of the Criminal Code defines the crime of theft as the act of a person without permission and with the intention of possessing or controlling all goods belonging to another person where the goods are taken without permission from the legal owner and unlawfully. The internet is in the form of electronic data that cannot be felt touched or seen, because what can be seen and heard is in the form of internet data that has turned into images, text, video, and sound, so not the internet directly. Here the issue arises whether wifi internet can be categorized as goods.

With the determination of extensive interpretation of electricity theft cases, it means that the internet transmitted on wifi devices can also be categorized as goods. Although intangible, wifi internet is an item of

economic value and has become a basic need like other basic goods needed by the community. Thus, if the wifi internet connection is taken by someone else without permission, it is included in the category of theft and meets the elements of Article 362 of the Criminal Code.

Wifi internet is an item that has economic value, because to be able to use or access it, users first buy by paying for internet packages/ quotas (wifi) through the service provider company (*provider).* The wifi internet also has a limit (can run out) or commonly called a quota so that in its use the wifi internet is limited and if the wifi internet quota runs out users are required to buy a new wifi internet package or an *unlimited* version, which can still be used for certain features with drastically decreased (slow) speeds.

In article 362 of the Criminal Code, in addition to the element of "goods" in it, there is also an element of "taking". In theft, the element "taking" is defined as the time when the thief takes the item has not been controlled by the thief, then after his actions the item has been in the power of the thief. For example, mobile phone theft can qualify as stealing/theft if the cellphone is taken and then has changed hands completely or in the possession of the thief. In law faculties, examples are often used in the form of "electricity" which is an invisible item/ object, then the act of stealing by means of a cable connected from a power source/ power plug connected to the thief's device.

Wifi internet that cannot be seen and touched in this case is taken through *a wireless adapter or antenna because wifi internet is in the form of radio waves or* wireless networks (wireless networks). The way wifi internet works is that the data requested or sent by users through the "air" uses radio waves and then emitted by the *router*. So if the security system inside the *router* is successfully penetrated (accessed illegally) by the perpetrator of theft, then the wifi internet network can be captured by antennas or adapters in laptops, computers, *smartphones*, and other electronic devices after that the wifi internet can be used by the perpetrators, then in this case it is concluded that the element of "taking" has been fulfilled in the case of wifi internet theft.

Furthermore, the provisions of the articles in the ITE Law will be analyzed to be applied in wifi internet theft. Perpetrators of wifi internet theft commit actions in the form of access to other people's electronic device systems illegally or unlawfully. Where the device accessed illegally is an electronic device in the form of a *router* that functions to transmit a wifi internet connection. The perpetrators used the modus operandi of forcibly accessing the electronic devices in order to use the internet connection for free and without the owner's permission.

Thus, when related to Law Number 19 of 2016 on Electronic Information and Transactions, the emphasis is not on the theft but the part of *illegal access*. In Article 1 point 5 of the ITE Law, it is stated that an Electronic System is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information. From this definition, the wifi internet is included in the electronic system because its

function is to send and/ or disseminate and receive electronic information from an electronic device to another electronic device that is interconnected. Some criminal acts related to unauthorized access to computers and/or Electronic Systems belonging to others are regulated in Article 30 of the ITE Law, namely:

(1) Everyone intentionally and without rights or against the law accesses other People's Computers and/or Electronic Systems in any way.
(2) Anyperson intentionally and without rights or against the law access Computers and/or Electronic Systems in any way with the aim of obtaining Electronic Information and/or Electronic Documents.
(3) Everyone intentionally and without rights or against the law accesses the Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking the security system.

The elements of Article 30 paragraph (3) of the ITE Law are as follows:

1. Intentionally and without rights or against the law;
2. Access computers and/or electronic systems;
3. In anyway by breaching, breaking through, exceeding, or breaking into a security system.

From the above elements, Article 30 paragraph (3) of the ITE Law formulates that the actions of any person who intentionally and without rights or against the law access computers and/ or electronic systems in anyway by violating, breaking through, exceeding, or breaking into a security system is prohibited and threatened with criminal sanctions. In the act of wifi internet theft in accordance with the explanation of the modus operandi in the previous problem formulation that in committing wifi theft, the perpetrator first breaks into the security system on *the router* connected to an electronic device to be able to access the victim's wifi internet. Wifi internet is included in the electronic system. Perpetrators of theft access to wifi internet intentionally and without rights or against the law or can also be called unauthorized access (*Illegal access*).(Widodo, 2013) Thus, wifi internet theft meets Article 30 paragraph (3) of the ITE Law because the perpetrator makes unauthorized access (*illegal* access) to the *router's electronic system* by breaking into the security system to be able to use wifi internet. With the fulfillment of the elements in Article 30 paragraph (3) of the ITE Law, it automatically also meets the elements in Article 30 paragraphs (1) and (2) of the ITE Law.

In connection with this analysis, wifi internet theft meets Article 30 paragraphs (1), (2), and (3) of the ITE Law. In criminal law, if the act meets the elements of more than one rule of criminal law, it is included in the idealistic *concursus*. *Idealistic concursus* or *endaadse samenloop* or concomitant regulation stipulated in Article 63 paragraph (1) of the Criminal Code which states, "if an act falls under more than one criminal rule, then only one of those rules is imposed; if it varies, the one imposed that contains the most severe principal criminal threat". The criteria of *idealistic concursus* are concurrent

and equal nature of the actions performed.

There are three models for determining which types of sanctions will be imposed on perpetrators. First, if the criminal sanctions stipulated in several criminal law rules violated by the perpetrator are the same weight and type, then it is enough to be convicted using only one of them, and generally look for things that relieve the accused. Second, if the criminal sanctions contained in several violated criminal law rules differ in weight and type, then the most severe weight and type are imposed. Third, if the criminal sanctions contained in some criminal law rules violated by the perpetrator are contained in the provisions of the general criminal law and the provisions of the special criminal law, then the criminal sanctions imposed are those contained in the provisions of the special criminal law. (M. Abdul Kholiq, 2002)

In Article 30 of the ITE Law, there are three paragraphs, all of which have similar elements, namely in the element of unauthorized access carried out on computers and/ or electronic systems carried out in a certain way. With this consideration, in accordance with *the idealistic concursus offense,* one of the criminal rules with the most severe threat is imposed. Article 46 of the ITE Law which regulates criminal threats, Article 30 of the ITE Law states that Article 30 paragraph (3) has the most severe threat. The provisions of Article 46 paragraph (3) of the ITE Law read: "Any person who fulfills the elements as referred to in Article 30 paragraph (3) shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of IDR 800,000,000.00 (eight hundred million-IDR)". Thus, it can be concluded that in the act of wifi theft, if proven the perpetrator is subject to Article 30 paragraph (3) of the ITE Law. Meanwhile, in the current development of Indonesian law, the principle of *idealistic concursus* is rarely used because it is oriented as if the law is retaliatory, but rather emphasizes law with *a restorative* nature.

CONCLUSION

Indonesian criminal law regulations cover cases of wifi internet theft. These regulations are as stipulated in:

a. Article 362 of the Criminal Code is *lex generalist*. Wifi internet can be interpreted extensively as one form of "goods" which is an element of Article 362 of the Criminal Code, just like the flow of "electricity" and "Wifi", although intangible and cannot be seen and felt, but has economic value to be said as "goods" because to be able to use or enjoy wifi internet services users must buy a wifi internet package first.
b. Article 30 paragraphs (1), (2), and (3) of the ITE Law are *lex specialist*. Where it is not about theft but emphasized on unauthorized access (*illegal access*) that is done intentionally. Because in the act of wifi internet theft, the perpetrators do make unauthorized access to the electronic system by penetrating security to be able to find out the *username* and *password* used to access the wifi internet. Thus, with the lightest to heaviest degree, Article 30 paragraphs (1), (2), and (3) of the ITE Law can be imposed on perpetrators. Future

suggestions need to be examined the theft of wifi used to cross the trail/ money laundering mode.

REFERENCES

[1] Alcianno G. G. (2016). *Pengenalan Teknologi Internet Serta Dampaknya*, Jurnal Sistem Informasi, Vol 2, No 2,p.72-73

[2] Annur, Cindy Mutia. *Jumlah Pengguna Internet Global Tembus 5,16 Miliar Orang pada 2023*, https://databoks.katadata.co.id/datapublish/2023/02/03/jumlah-pengguna-internet-global-tembus-516-miliar-orang-pada-januari-2023. Diakses 3 mei 2023

[3] Hairi, P.J. (2016). *Kontradiksi Pengaturan Hukum Yang Hidup Di Masyarakat Sebagai Bagian Dari Asas Legalitas Hukum Pidana Indonesia*, Negara Hukum, Vol 7 No. 1, p.90.

[4] Hamzah,A. (2008). *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, p.27.

[5] Hartanto, *et.al.* (2023). *The Implementation Of Restorative Justice In Law Enforcement In Its Acceptance Of Law Enforcement*, JURNAL META-YURIDIS, Vol (6) No.1 Maret,p.95

[6] Herlina, N. Dessy Rakhmawat. (2020). "Proses DanKendala Penyidik Polresta Jambi Dalam Mengungkap Tindak Pidana Penipuan Melalui Media Elektronik," Sains Sosio Humaniora,Vol. 4, No. 2 Desember, p.511

[7] Hiariej, E.O.S. (2014). *Prinsip-Prinsip Hukum Pidana,* Cahaya Atma Pustaka, Yogyakarta, p.338.

[8] Kitab Undang-Undang Hukum Pidana (KUHP)

[9] Malensang,D.(2017). *Implementasi Hak Untuk Hidup Berdasarkan Undang-Undang Dasar 1945*, Lex Privatum, Vol. 5 No. 2, p.21

[10] Moeljatno. (2008). *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, p.31.

[11] Kholiq, M.A. (2002). *Criminal Law Lecture Manual*, Faculty of Law, University of Indonesia, Yogyakarta, p.242-243

[12] Saputra, A. *Hukum Menggunakan Wifi Tetangga Tanpa Izin*, Republika, https://www.republika.id/posts/23229/hukum-menggunakan-wi-fi-tetangga-tanpa-izin, diakses 11 Mei 2023

[13] Sofyan, A. Nur Azisa. (2016). *Buku Ajar Hukum Pidana*, Pustaka Pena Press, Makassar, p.17

[14] Sugeng, W. (2010). *Jaringan Komputer dengan TCP/IP,* Modula, Bandung, p.162

[15] Sunarso,S. (2009). *Hukum Informasi dan Transaksi Elektronik,* PT. Adhi Mahasatya, p.227.

[16] UU No. 36 tahun 1999 tentang Telekomunikasi

[17] UU No. 19 Tahun 2016 perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[18] Widayati, L.S. (2011). P*erluasan Asas Legalitas Dalam RUU KUHP*, Negara Hukum, Vol. 2, No. 2, November, p.308

[19] Widodo,W. (2019). *Hoax Di Indonesia : Suatu Kajian*, Jurnal Meta-Yuridis Vol. 2 No.1, p.70

[20] Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta, p.27
[21] *Widodo. (2013). Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus,* Aswaja Pressindo, Yogyakarta*, p.5-11*