Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022 dated 07 December 2022
ISSN: 2747-2604
Volume 6 No. 1, March 2024, (149-162)

Law Enforcement against Cardsharing Perpetrators in Distributing Smartcard Private Keys on Television Services

Wahyu Wasono Dyan Aribowo[1)], Didik Endro Purwoleksono[2)] & Bambang Suheryadi[3)]
[1)] Faculty of Law, Airlangga University, Surabaya, Indonesia, E-mail: bepejeeska@gmail.com
[2)] Faculty of Law, Airlangga University, Surabaya, Indonesia
[3)] Faculty of Law, Airlangga University, Surabaya, Indonesia

Abstract. *The cybercrime has become popular case of which is serious enough for public and the law enforcers do not aside from badness happened at broadcasting service of satellite telecast subscribes to. Till now still require much business which is permanent ossified to finalize the case, this because of more and more and badness modus operandi complex world to be illusory especially by using or through internet as does cardsharing. Equally this term named "an authorized access to computer and service" causing is drawn explains its (the crime characteristic is thought to lay open this badness required expertise and experience of in information technology science. This study aims to know the law enforcement against cardsharing actors in distributing smartcard private keys on television services. The method uses normative research methodology with a qualitative approach. The data used is secondary data based on various reliable and verified sources, including scientific journals, books, online articles, and research reports relevant to the topic under study. Data analysis was carried out in three stages, namely data reduction, data presentation, and conclusion drawing. Based on the research concluded that cardsharing is an illegal activity so that criminal offenses can be imposed under Law No.36 of 199 concerning Telecommunications or even Law Number 19 of 2002 concerning Copyright. After the formation of the ITE Law, which is used as a reference for sanctions imposed on cardsharing offenders on the internet is Article 48 paragraph (2) of the ITE Law and for those who facilitate cardsharing actions, article 50 of the ITE Law applies which regulates criminal sanctions of imprisonment and / or fines with a greater criminal threat.*

Keywords: Cardsharing; Law Enforcement; Television.

1. Introduction

In general, broadcasts on pay television are broadcast by broadcast, but only paying subscribers can capture the broadcast. Therefore, cryptographic techniques are needed, which means hidden writing, namely the science of

secret writing[1]. Currently, there are many subscription TV broadcast users who do not pay dues to broadcasters officially, this is because they can receive subscription TV broadcasts by cardsharing through the internet network. Cardsharing, card shares, "sharing", or "CS" is a term for activities that describe the method of using smartcards over the internet network.[2] Cardsharing is an action by several clients to access subscription satellite television subscriptions via the internet network without rights (illegal) from one official subscription card (smartcard) distributed through the host / server provider via the internet[3]. As a result, broadcasts that are actually randomized and cannot be enjoyed, because they have been decrypted by the parent server, the receiver client can display broadcasts that can be enjoyed and open to the accomodation.

The use of Cardsharing itself is inseparable from the Internet network, where someone can receive all pay TV channels from subscription broadcasters using only an internet connection without paying dues to subscription television institutions[4], how with a card inserted by a provider who has become an official subscriber into the decoder, then the card can be shared / shared to other receivers via LAN / Ethernet through an internet connection access to remotely so that the decoder in which there is an official subscription card is used as a server while the other room as a client using a protocol software installed in it, which functions can contact directly to the server of the original service provider subscribed from the pay TV provider.

The legal issue that arises in the practice of cardsharing itself is that the act is done without rights and against the law. As mentioned on the website of Aora TV which is one of the satellite subscription broadcasting service providers that has been granted an operating license by the government, on the subscription terms page it has been expressly determined that Customers are only allowed to receive Services using official Receiving Equipment PT. Masterpieces. Customers are required to obtain the necessary Receiving Equipment from PT.

Cardsharing activities will certainly cause losses to subscription satellite television broadcasters that provide satellite television broadcast services, because television broadcast subscribers do not need to officially subscribe to providers and are burdened by fees when subscribing so that the broadcaster will lose potential revenue from dues charged to subscribers. Therefore, firm action is needed from the authorities to enforce the law of the cardsharing crime and in this thesis is intended to more deeply know the criminal provisions in the

[1] The Columbia Encyclopedia, Sixth Edition 2008 Columbia University Press.
[2] http://www.digitalworldz.co.uk/1949924-what-cardsharing.html, retrieved June 17, 2023
[3] http://www.ifwonline.com/clients/card-sharing.htm, retrieved June 17, 2023
[4] "Achnet Blog", *What is cardsharing and how does it work?*, http://blog.achnet.web.id/2011/12/apa-itu-cardsharing-dan-bagaimana-cara.html, retrieved June 17, 2023

field of information and electronic transactions that regulate cardsharing acts and identify who are the perpetrators of the cardsharing crime who can be subject to criminal liability.

Previous research stated that law enforcement in the criminal law process carried out in Indonesia (Positive Law) is currently using the Criminal Law Code (KUHP) which is the result of the thinking of the Indonesian colonizing country, namely the Netherlands. The criminal law brought by the Dutch until now still exists in Indonesia due to the absence of changes to the criminal law legislation, although criminal law has been partially changed. The criminal law contained in the Criminal Code currently used to criminalize a person who commits a criminal offense is Article 10 of the Criminal Code. The novelty of this research is the subject of the research, namely the cardsharing perpetrators in distributing smartcard private keys on television services. This research is new and has never been done before.

The importance of law enforcement in various aspects of human life including law enforcement on cardsharing offenders. So that the purpose of this research is to find out the various laws and regulations relating to the activity of distributing smardcard private keys on television services so that everyone can participate in law enforcement.

2. Research Methods

This research used normative research methodology with a qualitative approach. Normative research methodology is research that analyzes the reciprocity between legal facts and social facts in society. In addition, normative legal research methods are able to find solutions to legal vacuums, conflicts of norms, or vagueness of norms that occur in theories, principles, norms, rules or legal rules that exist in society. Normative research methods have consistency in directing legal research. The birth of the law is able to provide happiness and tranquility. The law is also considered capable of providing provisions that must be obeyed by the entire community. Meanwhile, a qualitative approach is a research approach used to understand complex phenomena in depth through descriptive and interpretive analysis of non-numerical data. This method emphasizes data collection in the form of narratives, words, or images that allow researchers to explore subjective meanings from the perspective of participants in a natural context.

The data uses in this study is secondary data obtained from various reliable and verified sources, including scientific journals, books, online articles, and research reports relevant to the topic under study. These sources were selected based on their credibility and reliability in providing accurate and up-to-date information. The data collection technique in this research is a literature study. This approach

involves searching, selecting, and analyzing various literature sources relevant to the research topic. Literature study allows researchers to develop a comprehensive understanding of the research topic by utilizing existing knowledge from various sources, such as books, scientific journals, articles, research reports, and online materials related to the topic under study.

Once the data was collected, the analysis process was conducted in three main stages. The first stage is data reduction, where relevant data is extracted and organized systematically to facilitate further analysis. Then, the data is presented using appropriate methods, be it in the form of tables, graphs, or clear narratives. Finally, conclusions are drawn based on the results of the analysis of the data that has been presented, which makes it possible to compile comprehensive findings and implications.

3. Results and Discussion

3.1. Prohibition of facilitating cardsharing over the Internet on subscription satellite television broadcast services (Pay TV)

The use of Information Technology, media, and communication has changed both the behavior of society and human civilization globally. The development of information and communication technology has also caused world relations to become borderless and caused significant social, economic, and cultural changes to take place so quickly. Information Technology is currently a double-edged sword because in addition to contributing to the improvement of human welfare, progress, and civilization, it is also an effective means of unlawful acts.

Given that previously there were several global phases that developed in accordance with changing times, the first phase was starting from farming (agrarian), the second phase was the industrial phase or the French revolution, the third phase was entering the communication phase such as the use of telephones, and the fourth phase was information technology such as how to update people to communicate. And this fourth phase is what we are facing now. Therefore, technology also affects the culture that exists in society so that when there is a change in society there is an influence on people's mindsets and cultural differences also affect the morals of the community itself, in this case it is the law that plays a role in regulating the pattern of community behavior, in accordance with the statement of *ubi soceitas ibi ius* (where there is a society there is law) and until now it is still relevant to use. Even in traditional societies, there must be laws with shapes and patterns that are in accordance with the level of civilization of the community. A society without law can never be a good society.

Law has various functions, namely as a tool of social control, a tool of social maintenance, a tool of dispute settlement, a tool of social engineering, Roscoe Pound). From these legal functions, the government as a guarantor of legal certainty can be a means of utilizing modern technology. As one of the concrete evidences is the making of a policy in Law No.11 of 2008 concerning Electronic Information and Transactions.

In this Law in Article 1 the relevant definitions of cardsharing are as follows:

a. Electronic Information means one or a set of electronic data, including but not limited to text, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are able to understand them.

b. Information Technology is a technique for collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information.

c. Electronic Document means any Electronic Information created, transmitted, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs or the like, letters, signs, numbers, Access Codes, symbols or perforations that have a feeding or meaning or can be understood by people who is able to understand it.

d. 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.

e. Electronic System Implementation is the use of Electronic Systems by state administrators, Persons, Business Entities, and/or the community.

f. Electronic System Network is the connection of two or more Electronic Systems, which are closed or open.

g. An Electronic Agent is a device of an Electronic System created to perform an action on a particular Electronic Information automatically held by a Person.

h. Electronic Certificate is an electronic certificate containing an Electronic Signature and identity indicating the status of the legal subject of the parties to the Electronic Transaction issued by the Electronic Certification Operator.

i. A computer is a tool for processing electronic, magnetic, optical, or system data that performs logical, arithmatic, and storage functions.

j. Access is the activity of interacting with Electronic Systems that stand alone or in a network.

k. Access Code is a number, letter, symbol, other character or combination thereof, which is the key to be able to access the Computer and/or other Electronic Systems.

l. Sender is a legal subject sending Electronic Information and/or Electronic Documents.

m. The Recipient is a legal subject who receives Electronic Information and/or Electronic Documents from the Sender.

n. A person is an individual, whether an Indonesian citizen, a foreign national, or a legal entity.

o. Business Entity means an individual company or partnership company, both incorporated and unincorporated.

Regarding cardsharing, the act prohibited in the ITE Law is Article 32 paragraph (2) of the ITE Law states that Everyone intentionally and without rights or against the law in any way transfers or transfers Electronic Information and / or Electronic Documents to the Electronic System of Others who are not entitled, will be studied more deeply related to the activities of actors who share smartcard private keys through the internet network. Meanwhile, cardsharing hardware and software makers, as well as ticket server sellers to enjoy cardsharing services, article 34 paragraph (2) is used which states that everyone intentionally and without rights or against the law produces, sells, procures for use, imports, distributes, provides, or owns computer hardware or software designed or specifically developed to facilitate actions.

As explained in the introduction, to be able to enjoy subscription television broadcast services through cardsharing is to install a receiver device connected to a router cable equipped with a modem as a means to connect to the internet network. A cardsharing user / client requires electronic information in the form of Internet Protocol Server (IP Server), Port, ID / username, and Password entered in the secret menu on the receiver (Attached Picture), this is necessary because the receiver client will receive a smartcard private key transfer that will be sent by the cardsharing provider / server via the internet.

Such electronic information is usually provided and sent via SMS by fly ticket selling agents (a term for cardsharing service provider agents). After entering the information, the receiver is then restarted and the receiver will then access the central server network and if the display says "Connection success", then it means that the receiver client has successfully accessed and connected to the cardsharing provider server via the internet. Furthermore, the receiver client is ready to receive the required information transfer continuously in the form of control word / private key smartcard that changes continuously every few seconds, to open the satellite broadcast description that is channeled through the client's satellite dish antenna. So that in the end the encrypted broadcast can be opened and can be enjoyed as usual.

The transfer of private code on the smartcard sent by the cardsharing provider's server is clearly done without any permission at all from the subscription satellite television broadcaster that has been determined by the government. If traced from the cardsharing provider, the private key they get is from being an official customer of one of the broadcasters, but the permission given by the institution is limited to only be enjoyed by the customer and not to be shared / transferred to others who are not entitled. For example, on the website of Aora TV, which is one of the satellite subscription broadcasting service providers that has been granted an operating license by the government, on the subscription terms page, it has been expressly determined that Customers are only allowed to receive Services using official Receiving Equipment PT. Masterpieces. Customers are required to obtain the necessary Receiving Equipment from PT. Karyamegah Adikarya or its authorized agent, and ensure that the installation of Receiving Equipment is carried out by PT. Masterpiece of the authoritative Adikarya. The Smart Card may only be used as part of the Receiving Equipment that has been installed and may not be transferred in any way or form to another Receiving Equipment.[5] So that the allocation of the smartcard and the private key contained in it is intended to only be given to authorized customers and is prohibited from being shared with other unauthorized people.

Related to the distribution of subscription television broadcasts in hotel rooms is usually done by redistributing subscription satellite broadcasts from an authorized subscriber receiver to then be unified in a multi-channel RF modulator UHF / VHF device[6] and formed into broadcasts using coaxial cable media via UHF / VHF networks which then the cable is distributed to hotel rooms through their respective televisions. This is not included in the scope of criminal acts that use internet technology / computer related crimes because the subscription television broadcast in the hotel room is obtained not by cardsharing so that it cannot be charged with articles in the ITE Law, but it can be

[5] http://www.aora.tv/page/term_condition, retrieved June 20, 2023
[6] http://www.megatron.biz/rfmodulator.htm, retrieved June 20, 2023

subject to articles in Law No. 19 of 2002 concerning Copyright, especially the prohibition on the redistribution of broadcasts protected by rights related to Copyright.

3.2. Apps that use smart cards

Smart cards are often used to secure data and ensure the security of transactions. In the telecommunications industry, the wireless telecommunications industry is the largest market that uses smart cards for security. A well-known example is the Global System for Mobile communication (GSM). GSM wireless phones have a Subscriber Identity Module (SIM card), which is a smart card wrapped in a small plastic that can be inserted in the phone slot. The SIM card identifies the user and provides an encryption key for digital voice transmission. Since the user's identity is programmed into the SIM card, the user can use not just one phone but multiple GSM phones with one SIM card.[7]Due to the success of wireless communication, the role of cellular phones is not just voice transmission. To maintain its advantage, telecom operators compete to provide additional services, such as mobile banking, mobile commerce, web access, and so on, all of which rely on smart cards to verify customer identity and ensure security in data transmission.

In banking industry, smart cards are used as secure credit/debit cards. It functions the same as a striped magnetic card (like some existing ATM cards). However, due to smart card computing capabilities, smart cards can handle off-line transactions and verification. Unlike striped magnetic cards, the data in smart cards cannot be copied easily so they cannot be misused. Smart cards as credit cards help prevent credit card fraud that usually costs around trillions of dollars a year. Now, the trend in payments and banking is e-purse or e-wallet applications. The card stores electronic money as a balance, then the balance can be increased and decreased.

In loyalty in commerce, smart cards can increase sales and customer satisfaction. The card stores loyalty points accumulated when the cardholder purchases goods. Cardholders can use points for discounts and rewards. The data in this card can also help merchants to find out the goods that buyers prefer and buyer behavior in buying.

In today's transportation system, smart cards can replace tickets, replacing coins for parking and toll roads. Smart cards provide many advantages in managing many small transactions and attract the attention of buyers with friendly and faster transactions.

[7] Kuni Kiswati, http://kkiswati.wordpress.com, accessed June 22, 2023

In the healthcare sector, smart cards can reduce the complexity of organizing patient insurance information and medical history. The card can store insurance administration data. Cards can also store patient medical data, provide up to date and reliable medical information, and allow information sharing between doctors, hospitals, and pharmacies.

On the internet, user authentication and controlled access are the reasons for choosing to use smart cards. There is an increasing use of smart cards with public key cryptographic systems. Smart cards carry the cardholder's private key and a digital certificate which are 2 components that verify the identity of the cardholder. In a public key encryption scheme, the private key is known only to the cardholder, and then paired with a large number of public keys. The private key is used in conjunction with the public key for digital signatures and verification. Digital certificates are issued by the organization that provides the certificate proving the authenticity of a public key. Applications that use smart cards for authentication include controlling Web access, digital signatures on e-mail, secure online transactions, and others. In our immediate environment, such as offices or universities, multi-application smart cards can provide control of entrance and computer access, provide a level of network access to Web sites and internal servers, store and process administrative data, and enable financial transactions (food payments, snack purchases at vending machines, ATM withdrawals and deposits, etc.).

The use of smartcards on set-top boxes is also identical to the function of using the smartcard mentioned above, namely identifying subscriber status and providing decryption service control over broadcasts sent by satellite via encrypted subscriber satellite dishes, so that television broadcasters can control and ensure only subscribers can enjoy subscription satellite television broadcasts. While on the Aora TV website, it is also said that "Smart Card" is an official card containing a microchip, which if inserted into an IRD (Integrated Receiver Decoder) will give Customers access to and receive Services legally from PT. Karyamegah Adhikarya (provider Aora TV) [8]

3.3. Criminal Liability of Cardsharing Perpetrators in Sharing Smartcard Private Keys via the Internet on Subscription Satellite Television Services (Pay TV)

The concept of criminal liability departs from the principle of "no crime without fault". That principle is a very fundamental principle in accounting for actions that have committed criminal acts. The understanding of the principle shows that a person cannot be punished if he has no fault, either intentional or negligence. So, the principle departs from "liability based on fault."

[8] http://www.aora.tv/page/term_condition, accessed on 22 June 2023

The principle contained in Article 35 paragraph (1) reads: "No one shall be convicted without guilt" In the sense of criminal acts including criminal liability. Criminal acts only refer to the prohibition of actions that have been stipulated in a law and regulation. Whether the maker who has committed the prohibited act is then also criminalized, depends largely on the issue of whether he in committing the act can be accounted for or not. In other words, whether it has faults or not.

Guilt is the state of the soul of the person who commits the deed and its relation to the deed done is such that the person can be reproached for doing the deed. If the maker does have a mistake in committing the crime, he will certainly be criminalized. However, if he has no fault, even if he has committed a prohibited act and the act is punishable with a crime, he will certainly not be criminalized. The principle of no-fault crime is thus a fundamental principle in holding the maker accountable for having committed a criminal act. That principle is also the basis on which penalties are imposed on makers.

As is known that for the perfect cardsharing action requires various tools / parties, including:

a. Cardsharing emulator software (Ccam) connected to the parent server. This software is in charge of sharing the information that has been entered, namely the private code taken from the card reader that has read the official customer's smartcard. This software has a role to forward / transfer information from the provider server to be distributed / shared to clients whose addresses are connected to the main server via the internet.

b. Card Reader that has been modified to be able to provide electronic information in the form of private code that will be shared with clients connected to the internet.

c. Satellite receivers on cardsharing clients / users who have the ability to receive access codes enter the IKS (Internet Key Sharing) embedded in the receiver.

d. Server usage information providers that provide tickets / access to receive cardsharing services, usually divided into several agents who provide subscription services to prospective clients for a certain period of one month that provide server information and usernames to enter the cardsharing provider server network.

Cardsharing is one of the activities that is negative and detrimental to other parties, namely accessing unlawfully and without rights to a computer system. Cardsharing is used for purposes that are harmful, both public interest, and

personal interest. These acts result in material and immaterial losses (time, value, services, money, goods, dignity, confidentiality of information, and broadcasting services) that tend to be greater than conventional crimes.

According to Heru Sutadi, crimes related to information technology can be divided into two major parts. First, crimes aimed at damaging or attacking computer systems or networks. Second, crimes that use computers or the internet as a tool in carrying out their crimes. The second is more accurately classified including cardsharing acts that must be subject to criminal liability on the maker.

Accountability in criminal law adheres to the principle of "no crime without fault". Therefore, it cannot be separated between guilt and accountability for deeds. Only the person who made the mistake can be held responsible for the non-crime he committed.

The elements in criminal liability of cardsharing perpetrators via the internet include. The presence of an element of error in the context of cardsharing involves several criteria that must be met. Firstly, it entails committing criminal acts in accordance with the principle of legality. In the case of cardsharing, this clearly depicts actions that constitute crimes capable of harming others, particularly subscription satellite broadcasting service providers. Additionally, the perpetrator must be above a certain age and deemed responsible, as specified in Law No. 3 of 1997 concerning the Juvenile Court. This law stipulates that individuals subject to trial must be between the ages of 8 and 18. Being considered capable of responsibility involves various aspects, such as the ability to determine intentions, recognize societal norms, and understand the implications of one's actions. Furthermore, the commission of cardsharing involves willfulness or negligence, which encompasses intentions, knowledge, will, planning, and purpose. These factors include actions taken via the internet with the intention of extracting private keys from servers and distributing them to unauthorized clients, as well as a deliberate plan to exploit subscription rights for unlawful gain. Consequently, there is no room for forgiveness or excuse for the actions of cardsharing perpetrators.

Cardsharing perpetrators are subject to criminal liability as stated in article 48 paragraph (2) of the ITE Law, namely:

Any person who fulfills the elements as referred to in Article 32 paragraph (2) shall be sentenced to a maximum imprisonment of 9 (nine) years and/or a maximum fine of IDR 3,000,000,000 (three billion rupiah)

Meanwhile, parties who facilitate cardsharing are subject to more severe criminal liability, namely as stated in article 50 of the ITE Law, namely:

Any person who fulfills the elements as referred to in Article 34 paragraph (1) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of IDR 10,000,000,000,000 (ten billion rupiah)

If referring to the criminal provisions in the articles above, the following can be explained:

a. The criminal system is a "cumulative alternative crime", this is seen by the regulation of "imprisonment and/or fines". This means that in addition to imprisonment, which is a crime that must be imposed, the judge can choose whether in addition to imprisonment also imposing a fine or simply imprisonment without a fine.

b. The longest prison sentence is regulated. In accordance with the concept of the Criminal Code, the shortest sentence is 1 (one) day. As stated in article 48 paragraph (2) and Article 50 of the ITE Law, this is in accordance with what is known as Algemeene Strafminima and Algemene Strafmaxima which is meant by Algemeene Strafmaxima, which is the general maximum limit that the general prison sentence is a maximum of 15 years. There are penalties of more than 15 years, this is in certain cases. While Algemeene Strafminima is the general minimum limit that imprisonment is at least 1 (one) day (Article 12 of the Criminal Code).

Receiver corporations that can receive electronic information in the form of private keys on smartcards from servers via the internet are subject to criminal liability as stated in article 50 of the ITE Law, namely:

Any person who fulfills the elements as referred to in article 34 paragraph (1) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of IDR 10,000,000,000,- (ten billion rupiah)

The formulation specified in the article applies to any corporation that intentionally and without rights or unlawfully produces, sells, procures for use, imports, distributes, provides, or possesses computer hardware or software designed or specifically developed to facilitate acts as referred to in Articles 27 to 33.

The problem in this ITE Law is that it applies criminally to corporations that commit criminal acts in the ITE field as stipulated in article 52 paragraph (4) of the ITE Law, because of the problems that arise. The ITE Law does not provide a firm explanation of what "corporation" itself means. In Chapter I, General Provisions, Article 1 recognizes only the terms:

1. The implementation of the electronic system is the utilization of the electronic system by the State Operator, Person, Business Entity, and / or the community (Article 1 point 6).

2. Persons are individuals, whether Indonesian citizens, Foreign Nationals, or Legal Entities (Article 1 point 21).

3. Business Entity is an individual company or partnership company, both legal and unincorporated (Article 1 number 22).

Thus, according to Didik Endro P. said that a common thread can be drawn that according to the ITE Law, what is meant by a corporation is whether it is a business entity. If this is so, article 52 paragraph (4) should expressly stipulate "... carried out by Business Entities...". But even this still raises the problem, which is what if the crime is committed by an organized group of people? So it will be difficult to be entangled with the provisions of article 52 paragraph (4), because they are not categorized as business entities, but if they are categorized as corporations this is not regulated in the ITE Law.

4. Conclusion

The law enforcement against cardsharing actors in distributing smartcard private keys on subscription television services is crucial to maintain system integrity and fairness in the television broadcasting industry. With a clear prohibition in Law No.11 of 2008 on Electronic Information and Transactions, as well as related articles in the ITE Law, the government has a legal basis to take firm action against cardsharers. It involves a series of tools and actions that violate copyright and system security, harm broadcasters and service providers, and threaten the integrity and security of users' personal information. Consideration of the principles of legality and criminal liability is important in enforcing the law, with strict sanctions in the ITE Law, the government can suppress cardsharing activities and protect the public interest and the subscription television broadcast industry as a whole.

5. References

Books:

Judhariksawan, (2010), *Hukum Penyiaran,* Cetakan ke-1, PT. Rajagrafindo Persada, Jakarta, June

The Columbia Encyclopedia, (2008), Sixth Edition, Columbia University Press

Wagito, (2007), *Jaringan Komputer Teori dan Implementasi Berbasis Linux*, Gava Media, Yogyakarta

Zulkarimein Nasution, (2006), *Modul Satelit Komunikasi:* Perabot Baru Masyarakat Modern,

Website

Achnet Blog", Apa itu cardsharing dan bagaimana cara kerjanya?, http://blog.achnet.web.id/2011/12/apa-itu-cardsharing-dan-bagaimana-cara.html, accessed on 17 June 2023.

http://www.aora.tv/page/term_condition, accessed on 20 June 2023

http://www.aora.tv/page/term_condition, accessed on 20 June 2023

http://www.aora.tv/page/term_condition, accessed on 22 June 2023

http://www.digitalworldz.co.uk/1949924-what-cardsharing.html, accessed on 17 June 2023

http://www.ifwonline.com/clients/card-sharing.htm, accessed on 17 June 2023

http://www.megatron.biz/rfmodulator.htm, accessed on 20 June 2023.

Kuni Kiswati, http://kkiswati.wordpress.com, accessed on 22 June 2023.

Regulation:

Law no. 11 of 2008 concerning Information and Electronic Transactions (State Gazette of 2002 Number 58, Supplement to State Gazette No. 4843)

Law no. 32 of 2002 concerning Broadcasting (State Gazette of 2002 Number 139, Supplement to State Gazette No. 4252)

Decree of the Minister of Communication and Information of the Republic of Indonesia Number: 366/DJPPI.4/ KOMINFO/03/2012 Dated March 28 2012 concerning Names of Subscription Broadcasting Institutions (LPB) via Satellite