



# Determination of Confiscation of Evidence of Data in Cyber Crime



Ni Made Liana Dewi <sup>a</sup>, I Made Wahyu Chandra Satriana <sup>b</sup>

Manuscript submitted: 09 October 2021, Manuscript revised: 18 November 2021, Accepted for publication: 27 December 2021

## Corresponding Author <sup>a</sup>



## Abstract

The social order in the digital era is increasingly diverse through interaction and communication using high-tech devices. However, this often causes violations and disturbances to public order and harms others (cybercrime). Based on the background above, there is problem formulation in this research, namely what is the legal basis for determining data confiscation in cybercrime and what the mechanism for data confiscation in cybercrime is. The type of research used is normative, namely seeing and analyzing from the point of view of legislation and applicable norms, especially those related to the problems in this research. The result of discussion is that the legal basis for data confiscation in cybercrime is referring to Law no. 11 of 2008 concerning Information and Electronic Transactions (ITE). This law contains regulations regarding the management of information and electronic transactions at the national level, with the aim that information technology development can be carried out optimally, evenly, and spread to all levels of society in order to educate the nation's life, while the mechanism for confiscation of data in cybercrime begins with electronic data in the form of writing, images and sound or all three are intangible and cannot be seen/heard.

## Keywords

confiscation;  
cybercrime;  
data;  
determination;  
evidence;

International Journal of Social Sciences and Humanities © 2022.

This is an open access article under the CC BY-NC-ND license

(<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

## Contents

Abstract .....	1
1 Introduction .....	2
2 Materials and Methods .....	3
3 Results and Discussions .....	3
4 Conclusion .....	6

<sup>a</sup> Dwijendra University, Denpasar, Indonesia

<sup>b</sup> Dwijendra University, Denpasar, Indonesia

Acknowledgments .....	6
References .....	7
Biography of Authors .....	8

## 1 Introduction

Since 1983, courts in Indonesia have tried cybercrime cases based on the provisions of the Criminal Code (KUHP) by means of extensive interpretation of the provisions contained in the Criminal Code (KUHP). The interpretation is, for example, done by expanding the notion of "goods" so that intangibles are considered goods. In addition, the word "falsify," expands to include the notion of falsifying electronic data via the internet. "Currently the form of cybercrime in Indonesia is very sophisticated and even exceeds other countries. As mentioned by Widodo in 2009, Indonesia was allegedly the largest credit card counterfeiter in the world, and the following year Indonesia was ranked 11th as the country's area with the most software piracy" (Widodo, 2013).

Since before the enactment of Law Number 11 of 2008 concerning Electronic Transaction Information, criminal provisions outside the Criminal Code have also been used in adjudicating cybercrime cases, as long as they have specifically regulated (for example, Law Number 11 of 2008 concerning Electronic Transaction Information for adjudicating cases of defacing, Law 5 of 1999 concerning the prohibition of Monopolistic Practices and Unfair Business Competition to prosecute "piracy" of domain names). After Law Number 11 of 2008 concerning Electronic Transaction Information applies all provisions of criminal law, both in the Criminal Code (KUHP), Law Number 11 of 2008 concerning Electronic Transaction Information and Law No. others have been used to prosecute cybercrimes, among others in cases of illegal access, insults through online media, hacking, defacing. In some cases, fraud in buying and selling, fraud with the mode of prostitution, cases of defamation and humiliation, some use the media facilities for questioning on the internet (eg facebook, twitter), and some use SMS. Unfortunately, there are also many cases that should be adjudicated under the Electronic Transaction Information Law but are only tried under the provisions of the Criminal Code (KUHP). This process can have an unfavorable impact on the authority of Indonesia's cybercrime law enforcement, and reduce the quality of justice received by the community. Outline of capable cybercrime cases that will be tried in Indonesia (Dwiyatmi, 2006; Sunarso, 2009).

The development of science, knowledge, technology, and art has ushered humans into the digital era which gave birth to the internet as a network, as well as a "symbol of connection between network subsystems into one super large network that can be interconnected (online) throughout the world. Even with internet technology, it is able to converge data, information, audio, and visual that can affect human life. The internet is said to be a symbol of exclusivity, because only people who are not "technologically savvy" can enjoy this era directly. the better the quality of people's mastery of information technology and its application in the internet field, the more exclusive these people feel. Therefore, nowadays many virtual masters of information technology application systems. For example, the "underground" community. Currently, the form of a computer as the basis of information technology, is not only in the form of a conventional computer (eg personal computer), but includes other portable equipment that has the characteristics of a computer, such as laptops, notebooks, cellphones, tablets. The order of society in the digital era is increasingly diverse, interaction and communication often only uses high-tech devices, so that criminal law as a regulation of life is often left behind with technological sophistication. However, criminal law must still exist in the digital era because it can be a means of social change, a means of control, and a means of protecting society in terms of achieving prosperity. "The legal aspects of the cyber legal regime are quite broad, namely in administrative, civil and criminal law. These three areas of law can be called cayber law (Sekretariat Negara, 2008; Indonesia & Indonesia, 1981).

In relation to the nature of criminal law, Andi Hamzah argued that the nature of criminal law as public law, among others, can be known based on that: a criminal act is still considered to exist by law, even though the act has received prior approval from the victim (such an act is considered not to violate the law). law, if viewed from private law), prosecution in criminal law does not all depend on the wishes of people who have been harmed by a crime, so that prosecutions are only carried out by state officials on behalf of the state; and costs in the criminal procedure are borne by the state, if the inmate is sentenced to a fine (then pays) and

there is confiscation of equipment and non-criminal proceeds (then handed over to the state) then the proceeds are considered as state income (Hamzah, 2008).

The term criminal law in the "information technology field" is a juridical term, meaning that the term has been contained in the legislation, namely in Article 43 paragraphs (1) and (2) of the Information and Electronic Transaction Law. In this provision, it is regulated about civil servant investigators and investigations in the field of information technology." On this basis, the author is interested in taking the title: "determination of data confiscation in cyber crime". Based on the above background, the formulation of the problem that will be discussed in this study can be formulated as follows: what is the legal basis for determining data confiscation in cyber crime and what is the mechanism for data confiscation in cyber crime (Werb et al., 2008; Ahmed et al., 2020).

## 2 Materials and Methods

The type of research used in this study is normative, namely seeing and analyzing from the point of view of the legislation and applicable norms, especially those related to the problems in this research. This type of approach is more directed to descriptive research which is a research method that seeks to describe and interpret objects as they are. Descriptive research can also form new theories or can strengthen existing theories. In addition, descriptive research is also research, where data collection is to compare research questions or hypotheses related to current circumstances and events. Presented by reporting the state of the object or subject under study in accordance with what it is. This study uses sources of legal materials: Primary legal materials, which include legal regulations such as Law Number 11 of 2008 concerning information and electronic transactions. Secondary legal materials are in the form of books, magazines, research results related to cybercrime. The technique of collecting legal materials used in writing this thesis is a literature study, namely: Researchers conduct research on various documents and library materials related to the problems being discussed in this study. The legal materials that have been collected are then analyzed based on the following stages: description, systematic and explanation. The description is intended to only describe the legal basis and mechanism for data confiscation in cybercrime. Systematization is intended to link one legal material with other legal materials so that it becomes a logical whole. Explanation is intended to analyze and provide an explanation of the legal materials (Manky, 2013; Ben-Itzhak, 2009).

## 3 Results and Discussions

Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE). Is not a Special Crimes Act, because this Law does not only contain criminal law, but contains regulations regarding the management of information and electronic transactions at the national level, with the aim of developing information technology in an optimal, equitable and spread-out manner. All levels of society in order to educate the nation's life. This is done to meet the demands and needs of the rapid development and advancement of information technology, which causes changes in the activities of human life in various fields which directly affect the birth of new forms of legal action. The development of information and communication technology brings positive and negative effects, like a double-edged sword. The use of technology and information and communication on the one hand contributes to the improvement of human welfare and civilization. On the other hand, technological advances can be used to carry out acts that are against the law, which attack various legal interests of people, society and the State (Chazawi, 2015). In line with that, criminal law must follow it, if not, the development and progress of information technology, which has factually affected the changes in human life and civilization activities, will have a very bad impact, therefore in the Law on Information and Electronic Transactions are also regulated regarding criminal law, especially regarding criminal acts. Criminal law, especially regarding criminal acts through the threat of criminal witnesses, is very strong. Because in every undabf, it always includes criminal law, including the law on information and electronic transactions.

An act can be punished if it has fulfilled the elements of a criminal act, in other words the act is an act that is against the law and contrary to applicable legal norms. This can provide guarantees for human rights, legal

certainty, and limit the authority of the authorities. But besides that, the principle of legality does not provide protection for collective interests and can be a stumbling block for judges to convict someone based on a bad act that has been committed. Article 1 paragraph (1) of the Criminal Code states that: "An act cannot be punished, except based on the strength of the provisions of existing criminal legislation" or often referred to as the *nullum delictum principle* *noela poena sine pravia lege poenali*. This principle is a certainty that a regulation is not retroactive and has extensive legal sources. This means that, if there are no special regulations relating to cybercrime cases, then the crime cannot be prosecuted (Lee et al., 2013; Chamberlain, 1984).

An accused person may be subject to criminal sanctions in almost any jurisdiction where there is an internet connection. A government can have broad leeway to decide where to prosecute online criminals because crimes can be committed where the defendant is, where the victim is, and all jurisdictions to which the defendant's actions have been electronically exposed. However, in reality the principles of traditional law can be applied on the internet. Even if the connection is short, the computer is physically located in a certain place, the defendant started the crime from a certain place, and the victim is in a certain place. The challenge is to identify the location (Chelh et al., 2006; Kapoor & Nemat-Nasser, 1998).

Regarding the confiscation of evidence in the settlement stage of defamation or insulting cases, it is adjusted to the category of actions that have been carried out by the defendant according to Article 39 paragraph (1) of the Criminal Procedure Code, namely: criminal acts, objects that have been used directly to commit a crime or to prepare it, objects that are used to hinder the investigation of a criminal act, objects that are specifically made or intended to commit a crime, other objects that have a direct relationship with the criminal act committed. A criminal sentence cannot be carried out if there is no valid evidence that can convince and strengthen that there has been a criminal act and it is the defendant who actually did it. Legal evidence according to Article 184 of the Criminal Code is: witness testimony, expert testimony, letters, instructions, testimony of the defendant.

The parties entitled to submit reports or complaints according to Article 108 of the Criminal Procedure Code are: Everyone who experiences, sees, witnesses and or becomes a victim of events which constitute a criminal act has the right to submit reports or complaints to investigators and or investigators both verbally and in writing. Knowing a conspiracy to commit a crime against public peace and security or against life or property rights must immediately report the matter to investigators or investigators. it to the investigator or investigator. Against criminal acts of defamation or humiliation through social networks, prosecution can be carried out by the public prosecutor. To be able to carry out a prosecution, the completeness of the case file must contain evidence that strengthens the justification for the existence of the crime which is then followed up with the preparation of an indictment. Detention can be carried out if the subjective, objective, and formal requirements have been met. Subjective requirements attached to the perpetrator of a crime, while the objective element relates to the circumstances in which the crime must be committed by the perpetrator (Feinstein & Horwitz, 1997; Sutherland et al., 2004).

In the judicial process, the obstacle is the difficulty of collecting evidence and submitting evidence in court. Perpetrators have many *modus operandi* in misusing computers, causing difficulties in fulfilling the material requirements for filing a lawsuit. If it does not meet the provisions as intended, it is said to be null and void. This is confirmed in the Criminal Procedure Code (KUHP) Article 143 paragraphs (2) and (3) which states that: "(2) The public prosecutor shall make an indictment which is dated and signed and contains: full name, place of birth, age or date of birth, gender, nationality, place of residence, religion and occupation of the suspect and a careful, clear and complete description of the crime charged with mentioning the time and place of the crime being committed, an indictment that does not meet the provisions as intended in paragraph (2) letter b is null and void."

The purpose of sentencing, among others, is to provide protection to the community, to maintain solidarity in society, to prevent and tackle the perpetrators so that they become good people and the same crime does not occur again, and to resolve conflicts that occur so as to create a sense of peace in society. Types of crimes regulated in the Criminal Code (KUHP) contained in Article 10, which consists of: a. Principal punishment, death penalty, imprisonment, confinement, fines, criminal closure b. Additional penalties, revocation of certain rights, Seizure of certain goods, Announcement of judge's decision. Determination of criminal law as a means to tackle crime must really pay attention to all factors supporting the function of criminal law policies in accordance with the realities of people's lives. A rational approach is needed to be able to determine each

criminal law policy so that its conception can be determined consciously and maturely in using criminal sanctions to provide protection for the social interests of the community which need to be protected. Criminal sanctions must be adapted to the needs that have benefits for the community and the values of its manifestation. Criminal sanctions must also be able to foster self-awareness of perpetrators of defamation and humiliation so as to create a deterrent effect (Mask et al., 2019; Dewi & Dwiyantri, 2018).

One alternative to resolve cases of defamation or humiliation is in a civil manner, namely through fines and proportional compensation in the form of material and immaterial. Compensation is intended to provide compensation for losses that have occurred to the victim. Compensation is charged to the perpetrator of defamation or insult. The party who feels aggrieved by the existence of a civil offense has the right to file a counterclaim and resolve it with an apology or payment of compensation in the form of money. This can protect the rights of citizens who want to express their opinions, criticize, or complain to claim the losses they suffer if the defamation is related to the purchase or service of goods or services of poor quality.

Compensation in the form of material is compensation that is calculated in the form of money, carried out if it is truly proven that a loss has occurred intentionally by the perpetrator causing a loss. Meanwhile, compensation in the form of immaterial is compensation that cannot be calculated with money, namely in the form of confessions, apologies, and oaths. Defending can only be done on the grounds of public interest and in a state of necessity to defend oneself. The main purpose of providing compensation for defamation is to provide reparation for direct losses that occur to the legal subject concerned. In terms of compensation, it is stipulated in Article 1365 of the Civil Code (KUHP), namely: "Every act that violates the law and causes harm to others, obliges the person who caused the loss because of his mistake to compensate for the loss". Article 1372 of the Criminal Code: "Civil lawsuits regarding insults are submitted to obtain compensation and restoration of honor and good name. In judging each other, judges must pay attention to whether the insults are rude or not, as well as the rank, position and ability of both parties, and the circumstances.

In terms of proving the truth of the accusation of defamation or insult, it is stipulated in Article 312 paragraphs (1) and (2) of the Criminal Code and is only allowed in the following cases: carried out in the public interest, or because they are forced to defend themselves, if an official is accused of something in carrying out his duties. The burden of proof according to Article 1865 of the Criminal Code: "Everyone who claims to have a right, or designates an event to confirm his right or to refute a right of another person, is obliged to prove the existence of the right or the event stated." Meanwhile, the evidence stipulated in Article 1866 of the Criminal Code includes: written evidence, witness evidence, suspicions, confessions, oaths. Perpetrators of transnational crimes often move from place to place, often using sophisticated high-mobility facilities and infrastructure. Locus delictus or the place where the crime occurred can be applied simultaneously.

There are two objects of action which are also objects of criminal action, namely "Electronic information" and "Electronic Documents". The two phrases are separated by words and/or contain the meaning that in an event there is only one object, and possibly both objects. Meanwhile, phrases that have a charge that violates decency are elements of accompanying circumstances attached to the object of the crime. In this situation lies the unlawful nature of the actions prohibited in the criminal act of Article 27 paragraph (1). In paragraph (2) have gambling. Paragraph (3) contains insults and/or defamation. Paragraph (4) contains extortion and/or threats. Regarding these two objects, the Electronic Information and Transaction Law has authentically interpreted in Article 1 Electronic Information is one or a set of electronic data, including but not limited to writing, sound, pictures, maps, designs, photographs, electronic data interchange, letters Electronic mail (electronic mail), telegram, telex, telecopy or the like, processed letters, signs, numbers, access codes, symbols, or perforations that have meaning or can be understood by people who are able to understand them. If these limits are summarized, it can be seen that 3 elements of the understanding of electronic information are: Electronic information is a collection of electronic data, Electronic information has the form of writing, sound, images, and Electronic information has meaning or can be understood. Electronic information is stored electronically in storage media, for example on a flash drive. This storage object is real, can be seen and ignited. However, the electronic data of the contents of the flash disk in the form of writing, images and sound or all three are not real, cannot be seen/heard. It only becomes real and can be seen and/or heard if through electronic devices with electronic systems it is displayed or accessed by people who have the ability to do so not only be displayed electronically on electronic objects, for example on a monitor screen. But also by

electronic means it can be displayed in the form of writing and/or pictures on printed objects, which can be evidence of writing/letters.

#### **4 Conclusion**

- a) The legal basis for determining data confiscation in cyber crime is the promulgation of Law no. 11 of 2008 concerning Information and Electronic Transactions. This Law is not a Special Crimes Act, because this Law does not only contain criminal law, but contains regulations regarding the management of information and electronic transactions at the national level, with the aim that information technology development can be carried out optimally, evenly, and spreads to all levels of society in order to educate the nation's life and the Criminal Code.
- b) The mechanism for confiscation of data in cyber crime begins with electronic data containing flash disks in the form of writing, images and sound or all three cannot be seen/heard. It only becomes real and can be seen and/or heard if through an electronic device with an electronic system it is displayed or accessed by a person who has that ability.

#### *Acknowledgments*



The researcher would like to thank the partners who have helped and supported this research so that the results of this research can later provide benefits to the community.



## References

- Ahmed, M., Mashkoo, F., & Nasar, A. (2020). Development, characterization, and utilization of magnetized orange peel waste as a novel adsorbent for the confiscation of crystal violet dye from aqueous solution. *Groundwater for Sustainable Development*, 10, 100322. <https://doi.org/10.1016/j.gsd.2019.100322>
- Ben-Itzhak, Y. (2009). Organised cybercrime and payment cards. *Card Technology Today*, 21(2), 10-11. [https://doi.org/10.1016/S0965-2590\(09\)70057-X](https://doi.org/10.1016/S0965-2590(09)70057-X)
- Chamberlain, G. (1984). Panel data. *Handbook of econometrics*, 2, 1247-1318. [https://doi.org/10.1016/S1573-4412\(84\)02014-6](https://doi.org/10.1016/S1573-4412(84)02014-6)
- Chazawi, A. (2015). Tindak Pidana Informasi & Transaksi Elektronik.
- Chelh, I., Gatellier, P., & Santé-Lhoutellier, V. (2006). A simplified procedure for myofibril hydrophobicity determination. *Meat science*, 74(4), 681-683. <https://doi.org/10.1016/j.meatsci.2006.05.019>
- Dewi, P. P., & Dwiyantri, K. T. (2018). Professional commitment, self-efficacy and ethical decision auditor. *International Research Journal of Management, IT and Social Sciences*, 5(6), 93-104. <https://doi.org/10.21744/irjmis.v5n6.379>
- Dwiyatmi, S. H. (2006). Pengantar Hukum Indonesia.
- Feinstein, A. R., & Horwitz, R. I. (1997). Problems in the "evidence" of "evidence-based medicine". *The American journal of medicine*, 103(6), 529-535. [https://doi.org/10.1016/S0002-9343\(97\)00244-1](https://doi.org/10.1016/S0002-9343(97)00244-1)
- Hamzah, A. (2008). Asas-asas hukum pidana edisi revisi.
- Indonesia, P. R., & Indonesia, P. R. (1981). Undang Undang No. 8 Tahun 1981 Tentang: Kitab Undang Undang Hukum Acara Pidana. *Sinar Grafika. jakarta*.
- Kapoor, R., & Nemat-Nasser, S. (1998). Determination of temperature rise during high strain rate deformation. *Mechanics of materials*, 27(1), 1-12. [https://doi.org/10.1016/S0167-6636\(97\)00036-7](https://doi.org/10.1016/S0167-6636(97)00036-7)
- Lee, J., Lapira, E., Bagheri, B., & Kao, H. A. (2013). Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing letters*, 1(1), 38-41. <https://doi.org/10.1016/j.mfglet.2013.09.005>
- Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, 2013(6), 9-13. [https://doi.org/10.1016/S1361-3723\(13\)70053-8](https://doi.org/10.1016/S1361-3723(13)70053-8)
- Mask, E., Brown, S., Lucky, W., & Peter, L. (2019). The importance of energy efficient in wireless sensor networks. *International Research Journal of Management, IT and Social Sciences*, 6(6), 207-219. <https://doi.org/10.21744/irjmis.v6n6.801>
- Sekretariat Negara, R. I. (2008). Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Sunarso, S. (2009). Hukum informasi dan transaksi elektronik: studi kasus: prita Mulyasari.
- Sutherland, W. J., Pullin, A. S., Dolman, P. M., & Knight, T. M. (2004). The need for evidence-based conservation. *Trends in ecology & evolution*, 19(6), 305-308. <https://doi.org/10.1016/j.tree.2004.03.018>
- Werb, D., Wood, E., Small, W., Strathdee, S., Li, K., Montaner, J., & Kerr, T. (2008). Effects of police confiscation of illicit drugs and syringes among injection drug users in Vancouver. *International Journal of Drug Policy*, 19(4), 332-338. <https://doi.org/10.1016/j.drugpo.2007.08.004>
- Widodo, H. P. D. B. T. (2013). Informasi Cybercrime Law, Telaah Teoritik dan Bedah Kasus. *Yogyakarta: Aswaja Pressindo*.

## Biography of Authors

	<p>Ni Made Liana Dewi Lecturer at the law study program, Faculty of Law, Dwijendra University, Denpasar. <i>Email: <a href="mailto:wahanadewi80@gmail.com">wahanadewi80@gmail.com</a></i></p>
	<p>I Made Wahyu Chandra Satriana Lecturer at the Faculty of Law, Dwijendra University, Denpasar, as a lawyer and legal aid consultant as well as a team of legal experts from the LBH Bali WCC Non-Governmental Organization. <i>Email: <a href="mailto:wahana.chandra@gmail.com">wahana.chandra@gmail.com</a></i></p>