Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung
Volume 4 No. 4, December 2025

Analysis of Determining Locus Delicti in the Cybercrime Investigation Process

Aksarudin Adam
Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: aksarudinkukar@gmail.com

Abstract: *The purpose of this study is to determine and analyze the locus delicti determination scheme in cybercrime investigations. In this paper, the author uses a normative juridical method with descriptive analysis as the research specification. Cybercrimes are committed in cyberspace, with the internet as an intermediary for committing cybercrimes. Cybercriminals can carry out cybercrime activities both from close range from the target of the crime or from a great distance, they can commit cybercrimes against the target victim of cybercrime. In cybercrime investigations, the crime scene can be in various jurisdictions, both international and national, thus creating problems in determining the competent court. This is further complicated by the existence of the Electronic Information and Transactions Law (UU ITE), which regulates the jurisdiction of cybercrimes with different principles, such as the territorial principle, the national principle, and the universal principle. Because there is always a difference between the location (locus) of the perpetrator and the location of the consequences.*

Keywords: *Cybercrime; Delicti; Investigation; Locus.*

1. Introduction

Every citizen's action is regulated by law, every aspect has their respective rules, provisions and regulations. The law determines what is must be done, what can be done and what is prohibited. One of the fields in law is criminal law, namely regulating the rules of conduct-certain prohibited acts. While criminal acts are acts which is prohibited by a legal regulation which is accompanied by a threat (sanction).

Technological developments bring change with the emergence of technology electronic information in the form of a computer system. One of the works in the field of technology information in computer systems that brought major changes in the 20th century one of them is the internet (*International Network*). With the internet, society can access various information, communicate, shop, and even do indirect financial

transactions through electronic media. With various convenience and positive benefits provided by technological developments Apart from this information, there are also negative impacts from technological advances. information, namely the emergence of crime in cyberspace or cybercrime (*cybercrime*). Cybercrime is a criminal activity related to with the virtual world (*cyberspace*) and computers based on sophistication the development of internet technology as the main media for carrying out crime.

The supremacy of law in Indonesia cannot be separated from technological developments nowadays. Technological progress can be considered a double-edged sword that can provide benefits or cause problems in everyday life.

This causes criminal activities in cyberspace to become increasingly varied and widespread. This crime occurs in cyberspace (*virtual*) so that it has characteristics that different from traditional crime. Cybercrime (*cybercrime*) is wrong one dark side of technological progress that has a very negative impact broad for all areas of modern life today permission, while material crimes are actions that result in losses for others. The existence of cybercrime has become a threat to stability, so that the government finds it difficult to keep up with the criminal techniques carried out by computer technology, especially in internet and intranet networks. However Thus, cybercrimes have their own complexities when court hearings require the presence of*locus delicti* clear. *Locus Delicti* This is important because besides the law requiring the indictment to mention *locus delicti* clear, *locus delicti* also important to determine the applicability law, jurisdiction or relative competence. While in cases *cybercrime*, determination *locus delicti* not as simple as in traditional crime cases or other crimes.

In cybercrime investigations, the crime scene can be at various jurisdictions, both international and national, thus giving rise to problems in determining the competent court. This is further complicated with the existence of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) which regulates the jurisdiction of cybercrimes with different principles, such as the territorial principle, the national principle, and universal principle. Because there are always differences between locations (*locus*) perpetrator with the location of the resulting consequences. In fact, it is not uncommon for a perpetrator's actions who are in a particular country, give rise to the consequences of their actions in other countries.

In connection with this topic, to research further and pour it into legal research with the research objective of knowing and analyze the scheme for determining the locus delicti in cybercrime investigations.

2. Research Methods

The approach used in this research is normative juridical or written legal approach (legislation/*statute approach).* Approach normative juridical is an approach that is carried out based on primary legal materials by examining theories, concepts, legal principles and regulations legislation related to this research. This approach also known as the library approach, namely by studying books, laws and regulations and other documents related to

this research.

3. Results and Discussion

3.1. Definition Locus Delicti

Locus Delicti, *Locus* (English) which means location or place, in terms of namely the application of criminal law seen from the perspective of the location where the act occurred criminal or simply *locus delicti* is the place where the crime occurred. *Locus Delicti*, or what is often called the crime scene, is the location where the crime occurred and is used to determine the jurisdiction of the court. authorized to examine the case.6*Locus delicti* need to know for:

1) Determine whether Indonesian criminal law applies to the act the crime or not.

2) Determine which prosecutor and court should handle the case the case (relative competence).

There are many opinions from several experts regarding *locus delicti* namely between others as follows: according to Van Hattum, the government is of the opinion.

3.2. Cybercrime

According to Widodo, that *cybercrime* interpreted as a person's activity, a group of people, legal entities that use computers as a facility committing crimes, and as targets.9In another definition, crime cyberspace is a term that refers to criminal activity using computers or computer networks become tools, targets or places where crimes occur.

Included in cybercrime are, among other things, auction fraud. online, check fraud, credit card fraud, *confidence fraud*, identity fraud, child pornography, etc. Even though cybercrime or cybercrime generally refers to criminal activity with computers or networks computer as the main element, this term is also used for activities traditional crimes where computers or computer networks are used to commit facilitate or enable the crime to occur.

Computer crime encompasses a wide range of potential illegal activities. Generally, this crime is divided into two categories, namely (1) Crimes that result in computer networks and *device* directly become the target; and (2) Crime facilitated by a computer network or *device*, and the main target is the network independent computer or *device*. Raharjo believes that crime is social phenomena that have existed in the world since the beginning of human life. More advanced (modern) crime is a form of crime that has changed from original form due to communication technology.10The face of evil has also been softened in this way, conventional crimes in the real world emerge into the virtual world in a virtual way.

3.3. Scheme for Determining Locus Delicti in Cybercrime Investigations

The cybercrime investigation process is a critical step that carried out by law enforcement officers to uncover and follow up cybercrime. Success in dealing with cybercrime involves use of specialized methodologies and close collaboration with stakeholders related. According to Michael R. Overly, emphasizing the importance of the investigation process and investigation *cybercrime* proactive. He highlighted that organizations need to have a trained team and effective procedures to respond to attacks cyber.

The process of investigating cybercrimes involves reporting the victim to investigators, who then forward the case to the public prosecutor to be brought to trial. court. If the investigator is from the PPNS, the results of the investigation are submitted through Indonesian National Police investigators. This process applies to cybercrimes in the broad sense or narrow.13Apart from the ITE Law, the legal basis for handling cybercrimes in

Indonesia also includes implementing regulations for the ITE Law, the Criminal Procedure Code, and various regulations technical matters in each investigative agency. This arrangement ensures the smooth running of the investigation legal process while maintaining public interest and the integrity of the system electronic.

The mechanism for investigating cybercrimes is regulated in the ITE Law and several other laws. implementing regulations. The police have a primary role in investigations, starting from from receiving reports, collecting digital evidence, to identification and arrest of the perpetrator. However, cybercrimes (*cybercrime*) each has its own complexities when the investigation process takes place requires the existence of *locus delicti* clear. *Locus Delicti* this is important because besides the law requires that the indictment state *locus delicti* clear, *locus delicti* it is also important to determine the applicability of law, jurisdiction or relative competence. However, in cases *cybercrime*, determination *locus delicti* not as simple as in traditional crime cases or crimes that other.

In the investigation process, determine *locus delicti* on cybercrime, the process is basically similar to determining *locus delicti* on crime conventional. The difference lies in the media used in the crime cyber, namely electronic media such as laptops, computers, cell phones, and various other sophisticated electronic devices. Therefore, cybercrime is classified as a special crime. To broaden understanding of this matter, it is necessary It is understood that cybercrime involves the use of advanced technology that allows perpetrators to commit crimes remotely, often without leaving a physical trace. Electronic media used in cybercrime covers a variety of devices and platforms, such as computer networks, the internet, *Locus delicti* there are no provisions for this in national legal products related to handling cybercrimes, namely the ITE Law and the Criminal Procedure Code. In determine *locus delicti* in criminal acts *cybercrime* that is the same or relevant with the theory of determining the place of occurrence in conventional crimes, namely based on the opinions of criminal law experts (doctrine), one of the theories is

put forward by Van Hamel and also based on previous judge's decisions

(jurisprudence), in criminal acts *cybercrime* namely there are several theories that used by investigators *cybercrime* namely:

This theory is the same as the theory of action and the theory of effect, only that adapted to practice in the scope of information technology, this theory used in determining the scene of a crime in a criminal act *cybercrime* and this theory emphasizes that in the cyber world there are 2 (two) main things, namely *uploader* (the party providing information into *cyber space*) And *downloader* (parties accessing information)17, so in determining the place where the crime occurred *cybercrime* can view based on the place of delivery (the perpetrator's place) and can also based on the place of reception (the victim's place).

Based on this theory a country can prohibit it in its territory, an activity *downloading* and *uploading* the materials that is estimated to be contrary to the public interest of the country.

For example, the Republic of Indonesia prohibits everyone within its territory to *downloading* all kinds of gambling activities. This theory can is also categorized into the theory of territorial jurisdiction. Because this theory is located

On *locus delicti* perpetrator *upload* and the perpetrator*download*.18

1) Territorial Jurisdiction

This theory explains that there are five aspects, namely:

a. Location of the occurrence of the act, in this teaching the investigator uses teachings of material actions (*leer van delicha melijkedaad*or*tiori corporeal action*), what is meant by the place of the incident is the place where the perpetrator committed the crime and has completed it as a result of the criminal act.

b. Computer Location, besides that also uses the teachings of location how the tool works (*leer van het instrument*), the scene of the incident is the place where the tool (in this case the computer) used works and has committed a criminal act. As in a simple example of a conventional crime is horse smuggling from The Netherlands to Germany, essentially the place of action is considered finished at the place where the rope is used. By because of that *High Council* (The Supreme Court of the Netherlands) determined, *locus crime* is in the Netherlands.

c. Location of People, in this teaching there are two principles that are used location approach. The first possibility of jurisdiction is determined by heading to the victim's location. The second possibility, jurisdiction determined by pointing to the location of the crime is at.21

d. Location of the effect, then there is also the use of the teaching of the effect of action (*leer van het gevoig*), the scene of the incident is the place where an effect has occurred which results in a criminal act committed by the perpetrator.

e.*Location of Anything*, because the teachings above could be If it is not in accordance with the actions carried out then there are other teachings The teachings used are the teachings of various places of criminal activity. The teachings This is a combination of all the teachings above, so that law enforcement officers are able to determine wherever the crime was committed.

2) Jurisdiction *Ratione Personae* (based on the reasons of the person or person) This criterion is used to determine the jurisdiction of an organ judicial by ensuring who can be asked legal accountability before the judicial organ. Nationality The perpetrator, in determining the jurisdiction of the crime *cybercrime*, approach.

The nationality of the perpetrator can also be done. The Nationality of the Victim can also be done used as an approach in determining the jurisdiction of cybercrime. With this approach, a country can claim jurisdictional authority against crimes involving internet content (*content related offense*), with the argument that some of its citizens have been targeted the crime.

3) *Theory of Law of the Server*

This theory is in terms of determining the location of a crime *cybercrime*, the

investigator treats the server where the page is located *we* physically located that are tracked based on the IP address where they are located recorded or stored as electronic data, then in this case the investigator can determine the location of the crime *cybercrime* based on where the IP address used by the perpetrator came from. In simple terms based on this theory, the place where the server is physically placed, then That's where the law will be enforced. However, this theory will be difficult to use if the uploader is located in a foreign jurisdiction.

4) *Theory of International Space*

According to this theory in determining the place where cybercrime occurs where the cybercrime is outside Indonesian territory, namely criminal act *cybercrime* transnational, then in determining the place incidents must look at the laws that apply across countries *cyber space* on side red as a separate legal environment from conventional law where each country has equal sovereignty, However, in practice, transnational cybercrime is not very common. it is difficult in the law enforcement process if a country has cooperation

in terms of law enforcement, especially in terms of criminal acts *cybercrime*. These theories are used as a reference by investigators in the area Indonesian law, considering that there are no clear regulations regarding *locus delicti*, then it is difficult for law enforcement officers to know the regulations or the article that will be imposed on the suspect, considering that in order to find out the locus the delicti, the investigator in this case requires a legal basis or basis so that there is no confusion in understanding in order to resolve cybercrimes fairly and legal certainty.

Although there are no clear provisions regarding the determination *Locus Delicti* in cybercrime (*cybercrime*) in Indonesia, but expert opinion law can be a reference in determining *Locus Delicti* in the case of cyb*ercrime*. Determination *Locus Delicti* in Criminal Acts of Crime on the Internet (*cybercrime*) according to National Criminal Law in Indonesia is important because rapid technological developments have led to the emergence of cybercrime (*cybercrime*), which is a challenge for law enforcement officers in determine *locus delicti* in cybercrime cases. Determination *locus delicti* important to determine the jurisdiction of the court authorized to handle the case cybercrime.

Theoretically, the determination *locus delicti* cybercrime in the investigation process by using various theories combined with positive law as a formal guideline for investigators in working to provide theoretical representations that the law works in a social perspective, the law does not work in a private space which is empty. There is a reciprocal relationship between the law and

the variables others in society. "Besides the law functioning as a tool for controlling social (*as a tool of social control*) law can also be used as a means

for social engineering (*as a tool of social engineering*) as described by Roscoe Pound".

4. Conclusion

Locus delicti there are no provisions for this in national legal products related to handling cybercrimes, namely the ITE Law and the Criminal Procedure Code. In determine *locus delicti* in criminal acts *cybercrime* that is the same or relevant with the theory of determining the place of occurrence in conventional crimes, namely based on the opinions of criminal law experts (doctrine). In criminal acts *cybercrime* namely, there are several theories used by investigators *cybercrime* namely *theory of the uploader and the downloader*, territorial jurisdiction theory, jurisdiction *ratione personae*, *theory of law of the server*, *theory of international space*. Theory- This theory is used as a reference by investigators in the Indonesian legal area, considering that there are no clear regulations regarding *locus delicti*, then it feels difficult for law enforcement officers to find out the regulations or articles that will be imposed on the suspect, taking into account the need to know the locus delicti

In this case, investigators need a legal basis or basis to prevent this from happening. confusion in understanding in order to resolve cybercrimes fairly and legal certainty. Although there are no clear provisions regarding the determination of *Locus Delicti* in cybercrime (*cybercrime*) in Indonesia, however

The views of legal experts can be used as a reference in determining *Locus Delicti* in Cybercrime.

5. References

Journals:

Aldo Satrio Wibowo dan Benny Sumardiana, (2025), Tantangan Hukum dalam Penentuan Locus dan Tempus Delicti Pada Tindak Pidana Revenge Porn di Indonesia, *JRH: Reformasi Hukum*, 29 (1) April

Aliefka Albiandro, (2022), Analisis Hukum dalam Menentukan Locus Delicti dalam Perkara Tindak Pidana Pemalsuan Akta Otentik, *JOM Fakultas Hukum Universitas Riau*, IX (1) Januari-Juni

Andi Rania Risya Zamayya, dkk. (2025), Kajian Teoritis Implikasi the United Nations Convention Against Cybercrime Terhadap Pengaturan Tindak Pidana Siber Indonesia, *Ikraith-Humaniora*, 9 (2) Juli

Arthur Simada, dkk. (2024), Penentuan Locus Delictie dalam Tindak Pidana Cyber

Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain). Locus Journal of Academic Literature Review, 3 (4) April 15

Bobby R. Tamaka, (2014), Pentingnya Tempat Kejadian Perkara Menurut Hukum Pidana di Indonesia, *Lex et Societatis,* II (5) Juni

J. F. Kemit & K. L. Kleden. (2023), Yurisdiksi Kejahatan Siber: Borderless. *Seminar Nasional-Hukum Dan Pancasila*, 2, Juli

K. Permata, dkk. (2024), Analisis Yuridis dalam Fenomena Revenge Porn di Indonesia dan Upaya Perlindungan Hukum terhadap Korban. *Jurnal Pendidikan Tambusai*, 8 (1)

Lastary Okvania, dkk. (2023), Analisis Putusan Pengadilan Negeri Payakumbuh Nomor 4/Pid.Sus/2022/PN Pyh dengan Putusan Mahkamah Agung Republik Indonesia Tentang Tindakan Pidana Konten Asusila lewat Media WhatsApp, *Unes Law Review*, 5 (4) Juni

Miftakhur Rokhman Habibi dan Isnatul Liviani, (2020), Kejahatan Teknologi Informasi (Cybercrime) dan Penanggulangannya dalam Sistem Hukum Indonesia, *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23 (2) Desember

Muhammad Permana Shidiq, et.al. (2024), Characteristics of Cybercrime and Dynamics of the implementation Locus Delicti Theory by Law Enforcement Officials in Indonesia, *Adjudication: Journal Knowledge Law*, 8 (2) December

Siti Hailatul Umami dan Abshoril Fithry, (2023), Mekanisme Penyidikan dan Penuntutan Tindak Pidana Cybercrime: Tinjauan Hukum Indonesia, *Prosiding Seminar Nasional Penelitian dan Pengabdian Masyarakat 2 Tahun 2023*, Sumenep 5-6 Desember

Sulistiyawan Doni Ardiyanto, Eko Soponyono, and Achmad Sulchan, (2020), Judgment Considerations Policy in Decree of the Court Criminal Statement Based on Criminal Destination, *Jurnal Daulat Hukum*: 3 (1) March

Yuliana Surya Galih, (2019), Yurisdiksi Hukum Pidana dalam Dunia Maya, *Jurnal Ilmiah Galuh Justisi*, 7 (1) Maret

Books:

Adami Chazawi, (2002), *Pelajaran Hukum Pidana,* Raja Grafindo Persada, Jakarta

Agus Raharjo, (2002), *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti

Georgia Institute of Technology, (2015). *Navigating the Digital Age: The Definitive*

Cybersecurity Guide for Directors and Officers, Chicago, Illinois; Caxton Business & Legal, Inc

Husamuddin, et.al. (2024), *Hukum Acara Pidana dan Pidana Cyber, Medan: PT Media Penerbit Indonesia*

M. Yahya Harahap, (1985), *Pembahasan Permasalahan dan Penerapan KUHAP*, Jilid II, PT. Sarana Bakti Semesta

P.A.F Lamintang, (2013), *Dasar-Dasar Hukum Pidana*, Sinar Baru, Bandung

Sahat Maruli, (2020), *Cyber Law,* Cet.1, Cakra, Bandung

Teguh Prasetyo. (2014). *Hukum Pidana Edisi Revisi*. Jakarta. Raja Grafindo Persada