The Theory of Determining Locus Delicti Cyber Crime and Its Arrangements in Criminal Law

Edi Sulistio Utomo, Hamidah Abdurrachman, Fajar Ari Sudewo
{sulistio.ed@gmail.com}

Magister of Law, Universitas Pancasakti Tegal, Indonesia

Abstract. The rapid dependence on technology, especially the internet, has led to an increase in cyber crime, which is characterized by its borderless nature. Perpetrators and victims of cyber crime can be located in different places, even different countries, due to the use of sophisticated tools such as cellphones, computers, and laptops. This study aims to determine the locus delicti of cyber crime in Indonesian criminal law and the regulation of court authority over cyber crime using a normative approach, analyzing legal material based on concepts, theories, laws, and expert opinions. The research findings reveal that the locus delicti of cyber crime can be determined using theories such as the theory of material acts, the theory of tools used, or the theory of tools in criminal law. The regulation for determining the court with authority to try cyber crimes is governed by Law no. 8 of 1981 Criminal Procedure Code Article 84 to Article 86. In conclusion, law enforcement officials can use one of the theories of material action, the theory of tools used, or the theory of tools in determining the locus delicti of cyber crime, and the authority for adjudicating cyber crime should refer to Article 84, Article 85, and Article 86 in the Criminal Procedure Code.

Keywords: Locus Delicti, Court Authority, Cyber Crime

1 Introduction

Cyber crime has its own complexity when a court hearing requires a clear locus delictie[1]. This locus delictie is important because in addition to the law requiring the indictment to state a clear locus delictie, it is also important to determine the applicability of the law, jurisdiction or relative competence[2]. In fact, in cyber crime cases, locus delictie determination is not as simple as in traditional crime cases.[3]

To determine locus delictie is not as easy as it seems, especially regarding cyber crimes which are cyber crimes that are not as easy as turning the palm of the hand to track and search for traces of these crimes[4]. In various cases of cyber crime there is almost always a difference between the location (locus) of the perpetrator and the location of the consequences. In fact, it is not uncommon for the actions of someone who is in a certain country to cause losses in another country or several other countries.

Cybercrime acts in some cases are generally carried out by insiders or those who have previously worked for an agency that has computer, telecommunication and information equipment in the form of hardware, software or brainware and a high sense of curiosity[5]. Some examples of cybercrime cases that have occurred in Indonesia include :

1. In 2020, 91 million user data and more than 7 million merchant data on Tokopedia were leaked by a hacker named ShinyHunters. As a result of the actions of ShinyHunters, personal data of Tokopedia users (encrypted email, name, address, date of birth, gender, telephone number and encrypted password) were leaked to the public. In fact, this information is sold online for around Rp. 70 million. Of course, this incident has the potential to bring harm to Tokopedia users. This is because hackers can take advantage of

user profiles for scamming (online fraud) and phishing (taking over accounts or systems).

2. The website of the Attorney General of the Republic of Indonesia will be defaced in 2021 so that its appearance will change. On the site there is a message of protest and a red stamp of hacked. Not only that, hackers also broke into the Attorney General's database and sold 3,086,224 personnel data to RAID Forums for Rp. 400 thousand.
3. In the middle of 2022 there was a hacking of the websites of the State Institutions of the Republic of Indonesia which was carried out by Hacker Bjorka. Through the Telegram group, Bjorka claimed to have hacked President Joko Widodo's correspondence, including letters from the State Intelligence Agency. Bjorka's claim was shared by a Twitter account "DarkTracer: DarkWeb Criminal Intelligence". In addition, the hack carried out by Bjorka has also resulted in the leakage of nearly 1.3 billion personal data which were then sold for commercial purposes.

The formulation of criminal acts in the Criminal Code is still conventional and has not been directly linked to the development of cyber crime[6]. In addition, it contains various weaknesses and limitations in dealing with technological developments and highly varied hit-tech crimes (high-tech crimes)[7]. This is what we want to see, that the Criminal Code has not been fully able to capture these crimes, but instead raises the potential for these crimes to be released from the clutches of the law. Thus, legal instruments are needed that are able to support it.

Even though conventional criminal law as applicable in Indonesia can be used by judges as a legal basis for trying cybercrime perpetrators, in practice there are very many limitations, both in terms of the elements of the crime and criminal responsibility[8]. Anticipating the problem of cyber crime is not only through the Law on Information and Electronic Transactions such as hacking, cracking, defacing, carding, fraud, spamming, cyberpornography, and online gambling, but also regarding the determination of locus delictie in Indonesian criminal law and the regulation of court authority over crimes. cyber crime.

2 Method

The type of research used in this research is library research[9]. Library research is research conducted through data collection or scientific writing with the aim of research objects or library data collection or studies carried out to solve a problem which basically relies on critical and in-depth analysis of relevant library materials[10]. Before conducting a literature review, researchers must know in advance with certainty from which sources scientific information will be obtained[11].

This normative legal research uses a statutory approach (statute approach) and a conceptual approach (conceptual approach)[12]. The statutory approach is carried out by examining all laws and regulations that are related to the legal issues raised[13]. The statutory approach is carried out within the framework of legal research for practical purposes as well as legal research for academic interests[14]. The statutory approach conducts a review of statutory regulations related to the central theme of the research. The source of data from this normative research is using secondary data[15]. Secondary data, namely data obtained from official documents, books related to the object of research, research results in the form of reports, theses, theses, dissertations, and laws and regulations. Secondary data is used as the main reference that is already available in the form of writing in books, scientific journals, and other written sources.

3 Discussion

3.1 Determination of Locus Delicti

The development of information technology has had a considerable impact on human life, the positive impact is to facilitate all activities of human life, while the negative impact is the increasing number of new crimes by utilizing this technological development[16]. This is in line with a theory which states that crime is a product of society itself. The more developed human civilization, the more forms of crime that appear. The presence of computers as the spearhead of the information technology revolution opens up the potential for advancement of various related technologies. The convergence of computer technology with information technology and communication technology gave rise to a new phenomenon, namely the internet.

The internet opens up horizons of information, knowledge and facts from all over the world. The free and global nature of the internet seems to be without boundaries, giving birth to new crimes. Cyber crime utilizes information technology networks globally. The global aspect creates conditions as if the world has no borders (borderless). Problems arise in determining the locus delicti of this cyber crime, due to the cross-border nature of the internet. This situation can result in perpetrators, victims and places of crime (locus delicti) occurring in different areas. Determination of locus delicti in general used by the science of criminal law today is still relevant when applied in determining the locus delicti of cyber crime considering the nature of cyber crime that crosses regional and national boundaries[17].

The existence of legal instruments to eradicate cyber crime is carried out as one of the efforts in reforming the national criminal law, which is in accordance with the sociological theory of law, that social change results in legal changes, because the law is always left behind from technological developments[18]. So that with the renewal of the national criminal law it is hoped that the law can accommodate developments in information technology or at least guarantee legal certainty in the use of information technology, especially the internet. Determining the locus delicti of cyber crime is not as easy as it seems, for this there are many factors that influence one of which is not easy to track to find the locus delicti of cybercrime, due to the limited tools to track these crimes. If we pay attention to the current laws and regulations, we have not found any laws that specifically regulate how to determine the location of a crime (locus delicti), thus it is difficult for law enforcement officials to determine which criminal law applies to a person. who commits a crime in his country or outside his country of origin to solve the problem or case. To determine locus delicti is not regulated in the Criminal Code, but is left to the knowledge and practice of criminal justice. So the determination of locus delicti cyber crime basically still uses existing criminal theories, namely as follows[19] :

a. Theory of material action, that is, where the crime is determined by the physical actor who is committed by the maker in realizing the crime.
b. The theory of instruments (tools) Namely in this theory the place where the offense occurred is the place where the tool used by the maker works.
c. Consequence theory, namely this theory whose size is based on the place where the effect occurs.

There are many opinions from several experts regarding locus delicti, including the following: according to Professor Van Hattum, the government is of the opinion that what must be seen as locus delicti is that an actor has committed a crime, and not the place where the crime has resulted. Professor Van Bemmelen is of the opinion that what must be seen as locus delicti is basically a place where an actor has committed his actions materially. Moeljatno explained that the experts in determining which was the place where the crime occurred had different opinions, giving rise to two streams, namely :

1. The flow that determines "in one place", namely the place where the defendant committed the act.

2. The flow that determines "in several places", that is, maybe the place of action and maybe the place of the result.

Moeljatno in his book explains that the first stream was pioneered by Pompe and Langemeyer who said that the place of crime is not determined by the place of the result of the act, but is determined based on where the defendant committed the act. Regarding this view, it is extended to the place where the tool used by the defendant acts, if the defendant uses the tool. The second stream is followed by Simon, Van Hammel, Joker and Bemelen which states that the place of the act may be chosen between the place where the act started by the accused until the act is finished with the consequences arising. In addition, Moeljatno stated that actions consist of behavior and consequences, so you may choose the place of action/behavior or choose the place of the consequences.

The process of determining locus in cyber crime is actually the same as determining locus delicti in ordinary crimes in general, but the thing that distinguishes cyber crime is that the media used in committing the crime are electronic media such as laptops, computers, cellphones. , and so forth there are many more sophisticated electronic media at this time. And therefore cyber crime is classified as a special crime. The issue of where the crime occurred (locus delicti) is not only important in the perspective of formal criminal law, but also in the perspective of criminal law in general. In general, certainty regarding the place of occurrence of a crime (locus delicti) is also important regarding the following matters :

1. Relating to the relative competence of the courts, namely determining which country's courts have the authority to try criminal acts that occur in a certain place. The certainty of the place of crime (locus delicti) is important and needs to be taken into account because each court has a different jurisdiction from one another. Courts can only handle or adjudicate cases that are only within the reach of the district/municipality administrative area, courts can handle cases filed. Thus, by knowing the place where the crime occurred (locus delicti), it is also known which court has the authority to try the crime that occurred within its administrative area (relative authority).
2. Relating to the scope of application of Indonesian criminal rules as stipulated in Article 2 to Article 9 of the Criminal Code. In the provisions of Article 2 of the Criminal Code it states, "That the Indonesian criminal rules apply to everyone (for Indonesian citizens or foreigners) who commit criminal acts in Indonesia". So by knowing the place where the crime occurred (locus delicti), for example it occurred abroad, the criminal rules do not apply to everyone except those regulated in the law. For example, it only applies to Indonesian citizens who take certain actions. As stipulated in Article 5 (1) to 2 of the Criminal Code which states: Criminal rules in Indonesian legislation apply to Indonesian citizens outside Indonesia who commit: 2nd one of the acts committed by a criminal regulation in Indonesian legislation seen as a crime while according to the laws of the country where the act was committed, it is punishable by crime.
3. Relating to exceptions as referred to in Article 9 of the Criminal Code. Based on the provisions of Article 9 of the Criminal Code, it has been determined that the application of the provisions of Articles 2 – 5, 7 and 8 is limited by exceptions that have been recognized in international law. With the limitation of the provisions of Article 9 of the Criminal Code, it can be interpreted that if an international crime occurs in a territorial area, then the territorial principle as stipulated in Article 2 of the Criminal Code does not apply absolutely. This is because even though the criminal acts that occurred were in the territory of Indonesia, they were not tried based on Indonesian criminal regulations, but regulations of other countries. This is because according to international criminal regulations every country has the same authority against international crimes that occur wherever the locus

delicti of these international crimes.

4. With regard to the conditions, that an act can be considered a criminal act if it is committed in a public place, for example a criminal act that tarnishes the values of decency in a public place as stipulated in Article 281 of the Criminal Code. Matters related to this condition are said to be an act of crime if it is not in accordance with the place where it is carried out, as exemplified above if it is done in a closed place it is not a crime but if it is done in a public place even though it is carried out by an official partner legally, the act is still considered an act criminal act because it is considered to injure the value of decency.
5. One of the absolute conditions for the validity of an indictment.

3.2 Regulating The Authority Of The Court Against Cyber Crime

Power in adjudicating there are two things, which are commonly referred to as competence, namely the first is relative competence, namely the jurisdiction of a State Court to try a criminal case, in other words which State Court has the authority to try a criminal incident, while the second is absolute competence, namely the authority court to try cases based on other levels of court. In determining a trial, the public prosecutor looks at the domicile of the perpetrator, and the number of witnesses available to facilitate the trial process later. Arrangements for the District Court that has the right to adjudicate are regulated in the Criminal Procedure Code (KUHAP), but tempus and locus delicti arrangements are not regulated in the Criminal Procedure Code or other laws, because the Criminal Procedure Code only regulates the following: Article 84 of the Criminal Procedure Code :

1. The District Court has the authority to try all cases regarding criminal acts committed within its jurisdiction.
2. The District Court in whose jurisdiction the accused resides, last resides, where he is found or detained, only has the authority to try the defendant's case, if the residence of most of the witnesses summoned is closer to the location of the District Court than the location of the District Court in whose territory the crime was committed.
3. If a defendant commits several criminal acts within the jurisdiction of the District Court, each District Court has the authority to try said criminal case.
4. Against several criminal cases which are related to each other and carried out by a person in the jurisdiction of various District Courts, the respective District Courts are tried with the provision that the possibility of combining these cases is opened.

Article 85, KUHAP: "In the event that regional conditions do not allow a District Court to adjudicate a case, then on the recommendation of the head of the District Court or the Head of the District Prosecutor's Office concerned, the Supreme Court proposes to the Minister of Justice to determine or appoint a District Court other than the one referred to in Article 84 to try the case in question". Article 86, KUHAP: "If a person commits a crime abroad that can be tried according to the laws of the Republic of Indonesia, then the Central Jakarta District Court has the authority to try him." locus delicti and court authority are easy to identify and track, but cyber crime is the opposite.

The difference in the investigation process between cybercrime and conventional crime is handled by investigators by conducting investigations at the Computer Forensic Laboratory. The working mechanism of a digital forensics include :

- Acquiring and Imaging Process. After the investigator receives digital evidence, the Acquiring and Imaging process must be carried out, namely copying (cloning/duplicating) precisely and with 1: 1 precision. It is from the results of the copy that a digital forensic expert can carry out an analysis because the analysis cannot be carried out from the original digital evidence because it is feared that it will change the evidence.

- Performing Analysis After carrying out the Acquiring and Imaging processes, you can proceed to analyze the contents of the data, especially those that have been deleted, hidden, encrypted, and traces of log files left behind.

The results of the analysis of digital evidence will later be transferred by investigators along with the case files to the prosecutor's office to be brought to court. The investigator's case files that have been declared complete by the prosecutor's office, the investigator submits or delegates the case file, the accused, and their handling responsibilities to the prosecutor's office which will be handled by the prosecutor by the public prosecutor to check for completeness and to carefully re-analyze the case, and to make a pre-prosecution file to be delegated to the court and prepare the indictment for the trial process later. The Criminal Procedure Code itself does not regulate how to mention locus delicti in an indictment, but materially in Article 143 paragraph 2 of the Criminal Procedure Code only mentions in the indictment the time and place of the crime committed. Determining locus delicti in cybercrime is very important for a prosecutor public prosecutor because this will later affect the legitimacy of the indictment. Therefore the determination of locus delicti uses the existing theory as follows:

1. The theory of the place where the crime was committed.
2. Theory where the effect is caused.
3. The theory of the tools used in committing the crime.

The Prosecutor's Office in placing locus delicti for cybercrime is not easy because the prosecutor must re-analyze the files submitted by the investigator to the prosecutor's office even though in the investigation process there is a prosecutor who takes part in the investigation process but needs to check and analyze again because this will later affect the placement of the jurisdiction of a court to try the case, also to determine whether or not an indictment made by the public prosecutor is valid or not. The examination at the Attorney General's Office is complete, the criminal act file is submitted to the District Court which has the right to try criminal acts related to cybercrime, after which the clerk determines the date and day of the trial along with the appointment of judges approved by the Chairperson of the District Court.

The appointed judge needs to review the matter so that later he will understand the case and be able to give a fair decision. In terms of cybercrime crime it is not easy to analyze the case easily due to the use of today's sophisticated technological tools which make it traceable even though there are expert witnesses who provide information and help but this does not necessarily make it easier as well in trials to determine locus Delicti is also one of the judge's considerations in making decisions in a criminal act.

After the police file is handed over to the public prosecutor and the public prosecutor issues P-21, the public prosecutor determines which court will try the crime based on the domicile of the defendant, the place where the case was committed and the number of witnesses and evidence involved in the crime. perpetrated by the accused". From the explanation above, it is clear that the determination of the tempus and locus delicti of cyber crime at the prosecution level needs to be re-analyzed after obtaining the files from the police (investigators) because it is not enough for the police to analyze the tempus and locus of cyber crime because later on the determination The tempus and locus delicti play an important role in drafting an indictment which determines whether or not an indictment made by the public prosecutor is legal.

Considering that the crime was committed using technology that required expert witnesses specifically telematics to assist prosecutors (public prosecutors) in handling cyber crime cases, to assist public prosecutors in solving and proving the crime. Apart from that, the determination of tempus and locus delicti in Article 15 of Law No. 8 of 1981 of the Criminal Procedure Code states that the public prosecutor demands criminal cases that occur within his jurisdiction according to the provisions of the law. From the level of investigation at the police and

pre-prosecution at the prosecutor's office, this will later influence the determination of the authority of the court that has the right to try a criminal act. In regulating the authority of the court itself, it has been regulated in Articles 84-86 of the Criminal Procedure Code (KUHAP) in this article, it is clearly regulated in the regulation of the authority of the court regarding criminal acts.

From the research results, the determination of the tempus and locus delicti of cyber crimes committed by the prosecutor's office is only based on the first theory, namely the theory of material acts (the place where the perpetrator committed the crime), as well as in determining the authority of the court which is determined by the public prosecutor based on provisions certain provisions that are in accordance with Articles 84-86 of the Criminal Procedure Code (Book of Laws. Criminal Law). In Law No. 8 of 1981 concerning the Criminal Procedure Code it does not discuss tempus and locus delicti, but determines the relative competence of the District Court.

4 Conclusion

Based on the discuss, we now that first, determination of the tempus and locus delicti of cyber crime is very important, besides being related to the application of the principle of legality in criminal law, tempus and locus delicti can also determine other matters such as the relative authority of the court, accountability, expiration and so on and most importantly the existence of tempus and locus This delicti is an absolute condition for the validity of an indictment. So if these two things cannot be determined or do not exist, then the indictment can be canceled by law. In addition to determining tempus and locus delicti, there are four theories that can be used, namely: a. The theory of material action (de leer van de lichamelijke daad) b. . Consequence theory (de leer van het gevolg) c. Instrument theory (de leer van het instrument) d. Combined theory (de leer van de meervoudige pleets) So, in determining where and when an innocent cyber crime occurs. Law enforcers use the four theories mentioned above, but mostly use the theory of material actions and the theory of consequences. So that later the determination of the place and time of the cyber crime can be justified or in other words it can be determined with certainty.

Second, The arrangement of which District Court has the right to try cyber crime and conventional crime is the same, which is regulated in Article 84 of Law Number 8 of 1981 concerning the Criminal Procedure Code, which essentially contains that the District Court has the authority to try all cases regarding criminal acts committed within their jurisdiction, and the District Court in whose jurisdiction the accused resided, the last resident, where he was found and detained, and most of the witnesses' residences. Article 85 of Law Number 8 of 1981 concerning the Criminal Procedure Code, which in essence, in terms of regional conditions do not allow a District Court to hear a case, then on the recommendation of the Head of the District Court or the Head of the Prosecutor's Office and the Supreme Court appoint another District Court to try it. Article 86 of Law Number 8 of 1981 concerning the Criminal Procedure Code, which in essence, if someone commits a crime abroad that can be tried according to Indonesian law, the Central Jakarta District Court has the authority.

References :

[1] Berlian C. Kejahatan Siber Yang Menjadi Kekosongan Hukum". Journal Equitable 2020;5. https://doi.org/https://ejurnal.umri.ac.id/index.php/JEQ/article/view/2532/1403.

[2] Syamsudin M. Operasionalisasi Penelitian Hukum. Jakarta: PT RajaGrasindo Persada; 2007.

[3] Widyopramono. Kejahatan di Bidang Komputer". cetakan pertama. Jakarta: Pustaka Sinar Harapan; 1994.

[4] Riswandi BA. Hukum dan Internet di Indonesia. Yogyakarta: UII Press; 2003.

[5] Sipropoulus J. CyberCrime Fighting, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership 1999.

[6] Soemadiningrat OS. Teori hukum Mengingat, Mengumpulkan dan Membuka Kembali". Bandung: Refika Aditama; 2004.

[7] Budhi I. Jaringan Komputer. Yogyakarta: Graha Ilmu; 2005.

[8] Abdul W. Kejahatan Mayantara (Cyber Crime. Malang: Fakultas Hukum Unisma Dari Internet; 2005.

[9] Sugiyono. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta; 2012.

[10] Mulyadi M. Riset Desain Dalam Metodologi Penelitian. Jurnal Studi Komunikasi Dan Media 2012;16.

[11] Marzuki PM. Penelitian Hukum. Jakarta: Kencana Prenada Media Group; 2005.

[12] Jhonny I. Teori dan Metodologi Penelitian Hukum Normatif. Malang: PT. Bayu Media Publishing; 2010.

[13] M H. Model-Model Pendekatan Dalam Penelitian Hukum dan Fiqh. Pekanbaru: UIN Suska Riau; 2015.

[14] Ali HZ. Metode Penelitian Hukum. Jakarta: Sinar Grafika; 2009.

[15] Yusuf AM. Metode Penelitian Kuantitatif, Kualitatif dan Penelitian Gabungan. Jakarta: Prenadamedia Group; 2014.

[16] Makarim E. Pengantar Hukum Telematika. Jakarta: PT. Raja Grafindo Persada; 2005.

[17] Soerodibroto S. KUHP dan KUHAP". Jakarta: PT RajaGrafindo Persada; 2000.

[18] Harahap MY. Pembahasan Permasalahan dan Penerapan KUHAP. Jakarta: Sinar Grafika; 2012.

[19] Lamintang PAF. KUHAP dengan Pembahasan Secara Yuridis Menurut Yurisprodensi dan Ilmu Pengetahuan Hukum Pidana". Bandung: Sinar Baru; 1984.