ISSN 2613-9995 (Cetak)
ISSN 2614-0179 (Online)
AJUDIKASI
Jurnal Ilmu Hukum
ajudikasi.unsera@gmail.com
e-jurnal.lppmunsera.org/index.php/ajudikasi

CHARACTERISTICS OF CYBER CRIME AND DYNAMICS OF THE IMPLEMENTATION *LOCUS DELICTI* THEORY BY LAW ENFORCEMENT OFFICIALS IN INDONESIA

[1]Muhammad Permana Shidiq, [2]Sigid Suseno, [3]Enni Soerjati Priowirjanto
Faculty of Law, Padjadjaran University, Indonesia
Email : permanashidiq12@gmail.com

| ***Article History*** :
| *Submission* : 17 Sep 2024
| *Last Revisions* : 04 Nov 2024
| *Accepted* : 12 Des 2024
| *Copyedits Approved* : 31 Des 2024

Abstract

The implementation of the locus delicti theory in cybercrime faces various complexities. This is due to the unique characteristics of cybercrime, where the use of computers as a crime tool often results in the perpetrator, victim, and impact of the crime being in different locations. This condition has caused debate among law enforcement officials regarding determining the right location where the crime occurred. This research aims to see the implementation of the locus delicti theory in cybercrime by law enforcement officials in Indonesia. The research method applies a normative juridical and descriptive nature of analysis. This research uses a theoretical approach, legal principles, a legal rule approach, and a case approach collected through literature studies, data collection techniques, and interviews. After all the data is collected, it is analysed qualitatively to produce several conclusions. The locus delicti theory has a necessary position in law enforcement efforts. However, in practice, this theory is not always applied in every case of cyber crimes; it only becomes a reference when the provisions in Article 84 Paragraph (2) of the Criminal Code cannot be applied optimally. Therefore, regulatory reform and a more flexible approach are needed to apply the locus delicti theory in the future.

Keywords: *Locus Delicti Theory; Law Enforcer Apparatus.*

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

A. INTRODUCTION

The development of technology and information has experienced rapid development and positively impacted access to information, social involvement, and economic empowerment. In addition, there is also a risk to the developments that occur. In addition to the positive impact, the development of information technology is a tool that is quite effective in committing crimes. The crime occurs in cyberspace and has different characteristics and an extensive range than criminal acts in general (conventional); the crime is currently known as cybercrime.[1] Cybercrime is a relatively new crime that makes computers the most incidental aspect of the implementation of its crimes.[2] Currently, cybercrimes that occur attack individuals (individuals) and companies (corporations) and also target the state, including confidential data to state finances. In the context of the state, cyber security is a serious and important issue because it concerns the security of citizens' data. Based on the National Cyber Security Index (NCSI) in 2023, Indonesia occupies the 49th position in cybersecurity among 176 countries. Indonesia occupies the fifth position in the ASEAN region after Malaysia, Singapore, Thailand, and the Philippines. The cyber attacks experienced are domestic and have transnational and international dimensions. In 2023, there will be a total of 279.84 million cyberattacks originating from within the country and abroad.[3]

Positive law in the era of technology information today must reach several aspects, including those related to the use and development of the rule of law on the internet, legal conflicts and jurisdictions, and law enforcement from cybercrimes.[4] However, not all of these aspects can be reached by the positive law in Indonesia because it is difficult to compensate for the crime applied through information technology, primarily related to the internet network. The locus delicti aspect is one of the aspects that is still debated among law enforcement officials in its application because the global aspect of cybercrime and the use of sophisticated tools or technology in implementing crime cause a situation like a borderless world where all people can apply interaction without time and place restrictions with the internet network, this situation can cause perpetrators, victims and places of various criminal acts.[5]

Various cases of cyber crimes that researchers found, including the Denny Siregar case about defamation[6], the case of Dr Yulianus Paongan about morality[7], and the Yoga Fadilla

---

[1] Rian Dwi Hapsari and Kuncoro Galih Pambayun, "Ancaman *CYBERCRIME* di Indonesia", *Jurnal Konstituen*, 5, no.1 (2023) : 1-17, https://doi.org/10.33701/jk.v5i1.3208

[2] Ervina Chintia et al., ""Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya", *Jurnal Information Engineering and Educational Technology*, 2, no. 1 (2018): 65-69, https://journal.unesa.ac.id/index.php/jieet/article/download/3398/pdf/11740

[3]Muhammad Nur Firman, *Data on the Number of Cyber Attacks in Indonesia 2023* https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/ [accessed on 03/09/2024].

[4]Arthur Simada et al., "Penentuan *Locus Delictie* dalam Tindak Pidana *Cyber Crime* (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)", *Journal Locus* of Academic Litelature Review, 3, no. (2024) : 349-361, https://doi.org/10.56128/ljoalr.v3i4.314

[5] Rahmawati, "Penentuan Tempus dan Locus Delicti dalam Cyber Crime", *Jurnal Sol Justicia*, 3, no. 1 (2020) : 94-104, https://www.neliti.com/id/publications/408567/penentuan-tempus-dan-locus-delicti-dalan-cyber-crime

[6]Andri Saubani, *Locus Delicti Kasus Denny Siregar yang berubah-ubah* https://news.republika.co.id/berita/qpuxdj409/locus-delicti-kasus-denny-siregar-yang-berubahubah, [accessed on 01/07/2024].

[7] Putusan Pengadilan Nomor 354/Pid.Sus/2020/PN.JKT.SEL.

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

case about online fraud,[8] each have problems and complexities related to the place of the crime (locus delicti). In the case of Denny Siregar, there were several cases of transfer of case files related to alleged criminal acts of defamation. The complainant, who lives in Tasikmalaya, reported Denny Siregar's actions on his Facebook post in the form of a photo of a student with an insulting and/or defamatory narrative. The complainant reported the action to the Tasikmalaya Police. However, after the report, the Tasikmalaya Police delegated the report to the West Java Police because the location of the crime that occurred (locus delicti) was outside the jurisdiction of the Tasikmalaya Police. After all, the crime was committed in Bogor. After the transfer to the West Java Police, there was a development with the summoning of Denny Siregar, who was still limited to being a reported witness. After the summons, there was no follow-up or notification to the complainant until the case was suddenly transferred back to the National Police Headquarters. There was no clarity until the report was made.[9]

Furthermore, in the case of Dr Yulianus Paonganan, S.Si, M.Si, who had entered the process in court, the defendant's legal advisor filed an exception which at the same time resulted in the indictment read out by the public prosecutor (obscure libel) null and void, this became interesting because in his point of exclusion, it touched on the issue of the place where the criminal act occurred (locus delicti) and other material, formal requirements. This indictment does not pay attention to the rules contained in Article 143 Paragraph (2) of the Criminal Procedure Code regarding material and formal requirements, so it results in the court with authority to give the court and the examination of this problem should be the Central Jakarta District Court and not the South Jakarta District Court, because if you look at the facts that are revealed that the hashtag of the content uploaded/posted by the defendant in social media (which contains morality) made in Central Jakarta during the trip as explained in BAP.[10] This means that there is a fundamental error related to the application of the principle/theory of locus delicti by law enforcement officials as a benchmark to find out the existence of criminal acts (locus delicti) and the relative competence of the court with the authority to examine and conduct the court.

Finally, in the case of Yoga Fadilla, which was carried out and planned with Muhammad Ghafur on Jl. Cokro Kisaran Barat, Asahan North Sumatra, has committed online fraud crimes against Malang (East Java) victims, Bekasi (West Java), and Hong Kong. Thus, each of the regions/regions involved or affected should be able to be a benchmark to find out the place of the criminal act that will determine where the court with authority to examine and adjudicate the case should be. However, the fact is that the South Jakarta Court is the one that adjudicates and examines the problem based on detention carried out against the perpetrator who set aside the perpetrator's residence, where the crime was committed (locus delicti) and where the witnesses are.[11]

The problems from the cases that have been described previously show the complexity related to the place where the crime occurred, which is a challenge in itself, especially for law enforcement officials in the implementation of locus delicti both theoretically and practically, which will affect the law enforcement process of cyber crimes, considering the

[8] Putusan Pengadilan Nomor 951/Pid.Sus/2020/PN. JKT. SEL.
[9] Andri Saubani, *loc., cit.*
[10] Putusan Pengadilan Nomor 354/Pid.Sus/2016/PN. JKT. SEL.
[11] Putusan Pengadilan Nomor 951/Pid.Sus/2020/PN. JKT. SEL.

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

principles or elements of locus delicti This is very important because it is directly related to:[12]

1) The enactment of national criminal law, which will also affect the application of the principles of jurisdiction of a crime;
2) Extradition, if the perpetrator is abroad;
3) Competent courts (relative competence);
4) The element of offence in a criminal act, whether it has been fulfilled or has not been fulfilled;
5) Whether or not the formal and material requirements in the indictment are met.

Thus, locus delicti has the necessary position in law enforcement efforts. However, cyber crimes can occur, with some acts occurring in one country and others in other countries. Similarly, the consequences are not only experienced in one area of the country. However, they can be experienced in several areas of the country, which will result in difficulties in confirming theories that can be used to determine the locus delicti of a cybercrime. With these characteristics, in the future, it will affect the locus delicti theory, which will also affect law enforcement, so the problem of locus delicti must be considered and observed in order to be able to keep pace with the technological and information developments that have occurred both theoretically and practically by law enforcement officials. Therefore, this study will discuss the characteristics of cybercrime and the dynamics of law enforcement officials applying the locus deliciti theory in Indonesia.

B. RESEARCH METHODS

The research method applied to the research is a normative juridical approach with a descriptive analysis nature. This research approach uses a theory-theory approach, legal principles, legal approach, and case approach. Secondary data include primary, tertiary, and secondary legal materials, including legal rules, writings, or official journals, collected through interviews and literature studies; after the data is collected, it will be analysed qualitatively to produce several conclusions.

C. RESULTS AND DISCUSSION

1. Characteristics of Cyber Crime

Cyber crimes, although experienced in cyberspace and virtual, can still be categorised as actual legal actions and acts.[13] According to the Criminal Code, cybercrime is any form of a criminal act that applies assistance or electronic means. All general crimes (conventional), as long as they use tools such as technology, information, and the internet to commit their crimes, can be included in the group of cyber crimes, which means broad.[14] Cybercrime is a crime that uses the development of computer technology, especially the internet. This appeared at the birth of the information technology revolution. As explained by Ronni R. Nitibaskara, "Social interaction that minimises physical presence is another criterion of the information technology revolution". Through similar interactions,

[12] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* (Bandung: PT. Refika Aditama, 2012), p. 11.

[13] Faiz Emery Muhammad, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web", *Jurnal USM Law Review,* 6, no. 1 (2023): 226-241, http://dx.doi.org/10.26623/julr.v6i1.6649

[14] Muhammad Anthony Aldriano and Mas Agus Priyambodo, "Cybercrime Dalam Sudut Pandang Hukum Pidana", *Jurnal Kewarganegaraan,* 6, no. 1 (2022) : 2169-2175, https://journal.upy.ac.id/index.php/pkn/article/download/2947/pdf/7209

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

deviations in social relations in the form of crime can provide adjustments through new criteria.[15]

Prof. Widodo defines cybercrime as any act committed by individuals, groups of people, or legal entities that apply computers as a means of committing crimes or can be the goal of crime. All crimes in question are actions that defy the rule of law, either providing material or formal legal resistance.[16] The use of computers as an incidental aspect in committing crimes makes cyber crimes have different criteria than ordinary or conventional crimes; these characteristics include:[17]

a. The activities implemented are illegal or without rights and unethical activities that take place in cyberspace, so it cannot be determined which country has jurisdiction over its activities;
b. This action is implemented using internet-connected tools and devices;
c. Activities carried out cause material and immaterial losses (value, time, money, services, goods, dignity, self-esteem, confidentiality of information) that are greater than general criminal acts (conventional);
d. This perpetrator is someone who has skills and provides mastery of the application of the internet with applications;
e. His actions have involved several countries or are transnational.

In addition to its characteristics, several essential factors can result in cybercrime, including unrestricted internet access, misuse of computers, ease of committing crimes and small risks, the existence of a considerable desire for more, bigotry in technology, security systems that have not been controlled by the community and are still weak or law enforcement officials against activities that occur in cyberspace.[18] The impact of these factors has created various forms of cybercrime. Based on The International Handbook on Computer Crime, forms of cybercrime have several classifications, including:[19]

1) Computer-related economic crimes :
   a. Computer sabotage;
   b. Computer espionage and software piracy;
   c. Fraud by computer manipulation;
   d. Unauthorized access to DP systems and Hacking;
   e. Theft of services;
   f. The computer as a tool for traditional business offences.
2) Computer-related infringements of privacy :
   a. Illegal collection and storage of correct data;
   b. Use of incorrect data;
   c. Infrigments of formalities of privacy laws.
   d. Illegal disclosure and misuse of data;
3) Further Abuses :

[15] Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung: PT Refika Aditama, 2005), p. 25.

[16] Widodo Widodo, *Aspek Hukum Kejahatan Mayantara,* (Yogyakarta: Aswindo, 2011), p. 7.

[17]Budi Suhariyanto, Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan dan Celah Hukumnya,* (Jakarta: PT Raja Grafindo Persada, 2013), p. 13.

[18] Achmad Syaiful Hidayat Anwar, "Pengaruh Itensi, Pengalaman Menggunakan Internet, Kondisi Pemfasilitasan, Dan Undang-Undang Informasi & Transaksi Elektronik No. 11/2008 Terhadap *Cyber Crime"*, *Jurnal Reviu Akuntansi Keuangan,* 1, no. 1 (2011) : 63-71, https://ejournal.umm.ac.id/index.php/jrak/article/view/501/525

[19] Sue Titus Reid, *Crime and Criminology*, (*New York*, CBS College Publishing, 1985), p. 56.

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

a. The extension to offences against personal integrity.
b. Offences against state and Political interests;

Meanwhile, in Indonesia, the forms and legal rules regarding cyber crimes are contained in the ITE Law, including:[20]

1) Criminal acts related to illegal activities :
   - Dissemination or distribution, transmission can be accessed illegal content :
     a. Criminal Acts of Morality (Article 27 Paragraph (1) of the ITE Law);
     b. Gambling Crime (Article 27 Paragraph (2) of the ITE Law);
     c. Crime of Defamation Article 27A of the ITE Law);
     d. Crime of Intimidation and/or Extortion (Article 27B Paragraph (1) and Paragraph (2) of the ITE Law);
     e. Fraud (Article 28 Paragraph (1) of the ITE Law);
     f. Criminal acts that cause hatred based on SARA (Article 28 paragraph (2) of the ITE Law);
     g. The Crime of False Notification Causing Riots in the Community (Article 28 Paragraph (3) of the ITE Law);
     h. Criminal Acts of Sending Information Containing Threats of Violence or Scare Given to Individuals (Article 29 of the ITE Law)
   - Through any effort to illegal access (Article 30 of the ITE Law);
   - Illegal interception or interception of electronic documents, information, and electronic systems (Article 31 of the ITE Law).
2) Criminal acts related to interference :
   a. Interference with electronic documents or information (Article 32 of the ITE Law);
   b. Disruption of the electronic system (Article 33 of the ITE Law);
      - Additional Crimes/Accessoir (Article 36 of the ITE Law);
      - Criminal acts of forging documents or electronic information (Article 35 of the ITE Law);
      - Weight on criminal threats (Article 52 of the ITE Law).

2. Locus Delict's Theory in the Context of Cybercrime

Locus delicti is a series of words that are derived from "locus", meaning "location" or "place", and "dictum", meaning "criminal acts, legal resistance". Thus, locus delicti can be interpreted as where the crime occurred. Satochid Kartanegara stated that theories/teachings about the place of criminal acts (locus delicti) are part of "Algemene leerstukken" (general teachings), and their regulation is not regulated in laws and regulations but develops through principles, doctrines and jurisprudence in criminal

[20] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi danTransaksi Elektronik, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Undang-Undang Republik Indonesia, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

law.[21] Locus delicti is, in principle, closely related to material criminal law and formal criminal law because its position significantly affects several things, including:[22]

1) Relating to the scope of the enforcement of the national criminal law in the provisions of Articles 2 to 9 of the Criminal Code (territorial principle of Article 2 of the Criminal Code, subjective and objective territorial principle of Article 3 of the Criminal Code, principle of passive nationality Article 4 of the Criminal Code, active nationality of Article 5 of the Criminal Code);
2) Relating to extradition, which is the process of returning individuals accused and suspected of committing crimes;[23]
3) Regarding the relative competence of the judiciary, the authority to adjudicate and examine existing problems. This is important because every court can examine and adjudicate cases in the administrative area of the district/city. By being able to ensure locus delicti, it will make it easier to file a case for a court that has the authority to adjudicate and examine;
4) Regarding the element of offence in the criminal act, whether it has been fulfilled or has not been fulfilled;
5) Related to the conditions for the validity of an indictment. The indictment has material and formal requirements, which require a careful and clear explanation related to the criminal act and the place where the criminal act was committed (locus delicti).

Therefore, the position of locus delicti cannot be underestimated because it is very influential in every stage of the process that exists in material criminal law and formal criminal law. Currently, being able to know and ascertain the place of the crime can be based on several theories, which include:[24]

1) The theory of material acts (de leer van de lichamelijke daad/gedraging) is adapted to the material acts of a criminal act. This means that this theory emphasises that the place where the criminal act occurs is the area where the material act is carried out;
2) The theory of the tool's working (de leer van het instrument) is adjusted to the use or use of the tool to commit a criminal act. This means that this theory emphasises that when the tool functions or begins to be used, the place where the criminal act (locus delicti) occurs can be seen when the tool reacts;
3) The theory of the occurrence of consequences (de leer van het gevolg/de leer van constitutive gevolg) is based on the consequences of a criminal act. That is, this theory emphasises that when a criminal act occurs, the place where the criminal act occurs (locus delicti) is the result of the criminal act;

[21] Sofian Sastrawidjaja, *Hukum Pidana (Asas Hukum Pidana Sampai Dengan Alasan Peniadaan Pemidanaan),* (Bandung: Armico, 1996), p. 143.

[22] Pifzen Finot, "Strategi Penentuan Locus Delicti Tindak Pidana Penerbangan Poho Tanpa Izin di Kawasan Cagar Alam Maninjau Pada Tingkat Penyidikan", *Jurnal UNES Swara Justisia,* 5, no. 1 (2021) : 43-51, https://doi.org/10.31933/ujsj.v5i1.197

[23] Deli Waryenti, Ekstradisi dan Beberapa Permasalahannya, *Fiat Justicia Jurnal Ilmu Hukum",* 5, no. 2 (2012) : 1-18, https://jurnal.fh.unila.ac.id/index.php/fiat/article/view/64/65

[24] Rani Purwaningsih and Rhmat Dwi Putranto, "Tinjauan Yuridis Terhadap Penetapan Locus Delicti dalam Kejahatan Dunia Maya *(Cyber Crime)* Berkaitan Dengan Upaya Pembaharuan Hukum Pidana di Indonesia", *Jurnal Mimbar Keadilan,* 16, no. 1 (2023) : 130-138, https://jurnal.untag-sby.ac.id/index.php/mimbarkeadilan/article/view/8021/5438

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

4) The theory on various places of criminal acts (de leer van de meervoudge plaats/ubiquieteitsleer), the theory is adjusted to the places where the criminal act occurs, whether it is a material act, a tool until the consequences occur can be a benchmark for the place where the criminal act occurs (locus delicti), this theory is a combination of the three previous theories.

Legal experts are divided into 2 (two) schools in viewing and determining the place where the crime occurred (locus delicti); first stream 1) pioneered by Pompe Langemeyer, who stated that the place of the crime was not chosen from the place of the crime, but was chosen based on the place where the perpetrator committed the crime. This school was expanded to the place where the crime occurred based on the means applied by the perpetrators to commit the crime committed applied tools. Second stream 2) spearheaded by Simon, Van Hamel, Jonkers, Bemelen and Moeljatno, who explained that the place where the crime occurred (locus delicti) may be chosen from the place where the perpetrator acts until the action is completed and causes consequences. So, according to this stream, the place where the crime occurred does not have to be based on one of the actions committed by the perpetrator but can be chosen to know from the place where the crime occurred (locus delicti).[25]

Theory locus delicti This can be applied by law enforcement officials to know where the crime is committed (locus delicti) in the context of criminal acts in general (conventional). However, when this theory is applied in the context of cybercrime, law enforcement officials will face difficulties because of the nature and characteristics of cybercrime. It seems as if the world has no limits/no borders (borderless), so its implementation becomes problematic. Therefore, the researcher refers to the 10th UN Congress in Vienna and Austria in 2000, where several theories can be the basis for finding out where the crime occurred (locus delicti) in cyberspace (cyberspace). These theories are recognised or become positive law in the State of the United States in determining jurisdiction in cyberspace (cyberspace), which can be used as a basis for determining the place of cybercrime (locus delicti); these theories include:[26]

1) The theory of the uploader and the downloader this theory is based on downloading and uploading activities. Uploading is an activity carried out by entering electronic information in cyberspace, and downloading (downloader) is an activity of searching for information. This means that the place of the crime (locus delicti) can be seen when there are activities carried out by the perpetrator or victim when uploading (uploader) and downloading (downloading) an electronic information or electronic document that is prohibited from a legal rule;
2) The theory the law of the server, this theory is based on the fact that webpages are physically located webpages or can also be called web pages are a document that contains important and specific information about something, namely where everyone can see and who makes it will be recorded as electronic data. This means where the crime occurred (locus delicti) can be known on a webpage when the perpetrator carries out illegal activities. Later, there will be tracking actions based on the IP Address or server address

[25] Achmad Yasin, Akselerasi Locus Delicti dan Tempus Delicti dalam Nalar Fikih Jinayah", *Jurnal Al-Qanun,* 11, no. 1 (2008) : 232-246, https://jurnalfsh.uinsa.ac.id/index.php/qanun/article/download/146/132/134

[26] Jawade Hafidz, "Kajian Yuridis dalam Antisipasi Kejahatan *Cyber", Jurnal Pembaharuan Hukum,* 1, no. 1 (2014) : 32-40, https://jurnal.unissula.ac.id/index.php/PH/article/download/1466/1134

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

physically located, which is stored and deformed into electronic data to implement cyber crimes;

3) The theory of international space explains that cyberspace is a legal environment separate from conventional law, and all countries have similar sovereignty. This means that all activities in cyberspace are analogous to activities in space, and all activities can be regulated together.

3. Implementation of Locus Delicti Theory on Cyber Crime by Law Enforcement Officials in Indonesia

In practice, the police as investigators will first conduct an investigation; this action is essentially carried out so that they can choose whether or not to apply investigative actions from events suspected of being a criminal act.[27] After it is known and constitutes a criminal act, it is continued to the investigation stage; at this stage, the locus delicti must be known with certainty. The investigation process is carried out in the following stages: issuance of SPDP (Investigation Commencement Warrant), collection of evidence, evidence, summoning and examination of victim-witnesses, reported witnesses, and witnesses who support or are directly related to the reported cyber crime, after the summons and examination, a case will be held to determine the suspect of the reported cyber crime, arrests, detentions, making investigation reports (BAP) and confiscation. In these stages, the investigator must already know the locus delict because the locus delicti itself is an aspect that is sought in disclosing who the suspect is and what criminal acts have been committed.[28]

These stages are carried out with skill and caution by the police as investigators because of the crimes experienced in cyberspace, where everything can happen very quickly. Cyber crime's efficient and fast nature causes difficulties in tracking criminals.[29]Therefore, in each stage, the police, as investigators, will ask for the help of IT experts and ITE experts to ensure the validity of evidence and evidence related to cyber crimes and to identify the perpetrators.

Furthermore, to find out the place of the crime (locus delicti), the investigator does not directly apply the theories of locus delicti that develop through principles, doctrines and jurisprudence in criminal law but pays attention to and applies the provisions contained in Article 84 Paragraph (2) of the Criminal Code:[30] "The district court in the jurisdiction where the defendant last resided or lived, in the place where he was detained or found, has only the authority to adjudicate the defendant's matter if the place of residence of most of the witnesses called is closer to the place of the district court than the place of residence of the district court in the area where the crime occurred".

This provision explains that the court can adjudicate and examine when a criminal act occurs based on where the defendant lives, last resides, or is found. It also pays attention to the presence of most of the witnesses. This emphasises that the locus delicti

[27] M. Husein Harun, *Penyidik dan Penuntut Umum dalam Proses Pidana,* (Jakarta: PT Rineka Cipta, 1991), p. 56.

[28] Winda Rahmadani et al., "Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Online", *Sumbang 12 Jurnal,* Volume 1, Nomor 2 (2023) : 90-97, https://jurnal.umsb.ac.id/index.php/smb12lj/article/view/4044

[29] Rozi Yudha Febriansyah, ""Delik-Delik Diluar KUHP (Tindak Pidana CyberCrime dan Cara Penanggulangan), *JHP (Jurnal Hasil Penelitian),* 6, no. 2 (2021) : 51-57, https://jurnal.untag-sby.ac.id/index.php/jhp17/article/view/6216/4612

[30] Pasal 84 Ayat (2) KUHAP.

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

theory can be set aside or excluded if the provisions of Article 84 Paragraph (2) of the Criminal Procedure Code are applied. Investigators consider that the provisions contained in Article 84 Paragraph (2) of the Criminal Code are easier to apply when a cybercrime occurs because it is based on evidence and evidence that will show where the cybercrime committed is, as well as being able to find out the court that has the authority to examine and adjudicate the case.[31] The theories of locus delicti will be used by investigators when applying the provisions contained in Article 84 Paragraph (2) of the Criminal Procedure Code encounters obstacles, then the theory of locus delicti will be used by investigators to help solve problems regarding the place where the criminal act occurred (locus delicti).

The steps taken by investigators in applying the provisions contained in Article 84 Paragraph (2) of the Criminal Procedure Code to determine the locus delicti of the cybercrime that occurred, including:[32]

1) Follow up on reports from victims of suspected cyber crimes (investigations);
2) Searching for the IP Address or mobile phone number of the perpetrator to find the place where the unlawful act was committed;
3) If it is found that the tool used to commit cyber crimes is a public facility or belongs to another person, such as Internet Café, another person's or friend's computer, disposable cellphone or cellphone that does not belong to him, an examination will be carried out on the relevant parties to be able to find out the connection of the actions taken by the perpetrator whether it involves other people or not;
4) Collect evidence and witnesses related to cyber crimes as stipulated in Article 184 of the Criminal Procedure Code and Article 5 Paragraph (2) of the ITE Law;
5) If the witnesses related to this cybercrime turn out to be in different places or outside the jurisdiction of the police where the victim reports, then the investigator will try to present witnesses or experts whose scope is the same as the victim who reported to the police in that jurisdiction, this is done as an effort to make it easier for the police of the jurisdiction where the reported person is to conduct searches and files;
6) Coordinate and cooperate with the police in other areas if there are witnesses or perpetrators of cyber crimes that are reported outside the jurisdiction of the reporting victim;
7) The investigator conducts the file, and after it is completed, it will be submitted to the prosecutor as the public prosecutor.

Thus, investigators' application of the locus delicti theory in the police is not based on existing theories. However, it can be used or not used as needed by the police as investigators in the investigation process and the investigation of cyber crimes.

Furthermore, the application of the locus delicti theory in the prosecutor's office is carried out with prior coordination with the police; the prosecutor's office, as the public prosecutor, will formulate the locus delicti in the indictment based on the results

[31] Interview with Mr. AKP Reno Apri Dwijayanto, S.Kom., S.H. as the chief investigator of Sub-Directorate 1 of the West Java Police (West Java Police Cyber Committee).

[32] Interview with Mr. AKP Reno Apri Dwijayanto, S.Kom., S.H. as the chief investigator of Sub-Directorate 1 of the West Java Police (West Java Police Cyber Committee).

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

of the investigation and investigation in the BAP by the police[33], the prosecutor's office can check whether the case file is complete or not if it is found to be incomplete, it will be given back to the investigator so that it can be completed. The act of returning the file is known as the P-19 code, and the file's return is given a maximum of 14 (fourteen) days after the public prosecutor assesses that this file is incomplete. The public prosecutor assessing the case file is still incomplete when there are shortcomings in the formal and material requirements. These requirements include full name, place of birth, age, gender, nationality, place of residence, religion, and occupation (formal requirements), a clear, meticulous, and complete description related to the criminal act charged through the mention of the time and place of the criminal act (material requirements).[34] After the file is completed and declared complete, the public prosecutor will immediately apply the prosecution and give the P-21 code to the investigator. In conducting prosecutions, the public prosecutor must:[35]

1) Checking the case file that the investigator will give whether it is strong enough and whether there is enough evidence that the defendant has committed a criminal act;
2) If there is insufficient evidence, and it does not include criminal acts or public affairs, then the termination of prosecution shall be applied;
3) After a clear and definite explanation of the criminal act committed by the defendant, the public prosecutor makes an indictment according to this case.

The locus delicti aspect in the prosecutor's office is a material requirement that must be formulated or listed clearly and firmly in the indictment (Article 143 Paragraph (2) of the Criminal Code. The mechanism for applying locus delicti in the prosecutor's office by the public prosecutor to cyber crimes is, in practice, carried out by applying the provisions in Article 84 Paragraph (2) of the Criminal Procedure Code with an agreement on an overview of the criminal act applied, witnesses related to the criminal act. Regarding the investigation's arrest and detention, after an agreement on these points, the public prosecutor can find out About the locus delicti and the court, which has the authority to adjudicate and examine the case. However, when there are differences regarding these points both from the investigator and the public prosecutor, the theory of locus delicate, which develops through principles, doctrines and jurisprudence in criminal law, will be used as a basis or reinforcement regarding the locus delicti, which will determine the court that has the authority to conduct examinations and adjudicate cases.[36]

D. CONCLUSION

The characteristics of cyber crimes are not the same as criminal acts in general or conventional; the use and utilisation of information technology, the internet is an incidental aspect that distinguishes it from other criminal acts; positive law in Indonesia has regulated several acts that are included in cyber crimes both in legal rules with general characteristics

[33] Rio Dirgantara, Ahmad Mahyani, "Landasan Perumusan *Locus Delicti* dalam Surat Dakwaan Pada Kejahatan Siber", *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, 2, no. 1 (2022) : 673-686, https://bureaucracy.gapenas-publisher.org/index.php/home/article/download/160/179/210

[34] Interview with Mr. Christian Dior Parsaoran Sianturi, S.H. (Head of the Pre-Prosecution Subsection of the Bandung City District Attorney's Office).

[35] Zulkarnain, *Praktik Peradilan Pidana*, (Malang: Setara Press, 2013), p. 69.

[36] Interview with Mr. Christian Dior Parsaoran Sianturi, S.H. (Head of the Pre-Prosecution Subsection of the Bandung City District Attorney's Office).

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

and legal rules that have unique characteristics. The results of this study emphasise the "Algemene leerstukken" general teaching about the theory of locus delicti which develops through principles, doctrines and jurisprudence in criminal law. Theoretically, the locus delicti theory that is currently known and used can be divided into 4 (four) theories, namely: the theory of material acts (de leer van de lichamelijke daad/gedraging), the theory of the working of tools (de leer van het instrument), the theory of consequences (de leer van het gevolg/de leer van constitutieve gevolg) and theories in several places of crime (de leer van de meervoudge plaats/ubiquieteitsleer). Law enforcement officials do not always use these four theories to find out where cyber crimes occur (locus delicti). However, they only serve as a reference if the provisions in Article 84 Paragraph (2) of the Criminal Procedure Code experience obstacles in their application. The implementation of the locus delicti theory will be more effective in the future if it can take into account the theories contained in the 10th PPB Congress in Vienna and Austria in 2000, as well as the theory of jurisdiction embraced by the State of the United States, because both theoretical approaches regulate activities in cyberspace so that in its development it can make it easier for law enforcement officials to carry out their functions and duties in enforcing the law against cyber crimes.

REFERENCES

Book

Harun, Husein, *Penyidik dan Penuntut Umum dalam Proses Pidana;* Jakarta : PT Rineka Cipta, 1991.

Nitibaskara, R Ronni dalam Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi;* Bandung: PT Refika Aditama, 2005.

Sastrawidjaja, Sofian, *Hukum Pidana (Asas Hukum Pidana Sampai Dengan Alasan Peniadaan Pemidanaan)*; Bandung : Armico, 1996.

Sue Titus Reid, *Crime and Criminology*; New York: CBS College Publishing, 1985.

Suhariyanto, Budi, *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan dan Celah Hukumnya;* Jakarta*:* PT Raja Grafindo Persada, 2013.

Suseno, Sigid, *Yurisdiksi Tindak Pidana Siber*; Bandung: PT. Refika Aditama, 2012.

Widodo, *Aspek Hukum Kejahatan Mayantara;* Yogyakarta: Aswindo, 2011.

Zulkarnain, *Praktik Peradilan Pidana;* Malang: Setara Press, 2013.

Journal Article

Adriano, Muhammad Anthony and Mas Agus Priyambodo. "Cybercrime Dalam Sudut Pandang Hukum Pidana", *Jurnal Kewarganegaraan,* 6, no. 1 (2022) : 2169-2175. https://journal.upy.ac.id/index.php/pkn/article/download/2947/pdf/7209

Anwar, Achmad Syaiful Hidayat. "Pengaruh Itensi, Pengalaman Menggunakan Internet, Kondisi Pemfasilitasan, Dan Undang-Undang Informasi & Transaksi Elektronik No. 11/2008 Terhadap *Cyber Crime". Jurnal Reviu Akuntansi Keuangan,* 1, no. 1 (2011) : 63-71. https://ejournal.umm.ac.id/index.php/jrak/article/view/501/525

Chintia, Ervina, Rofiqoh Nadia, Humayyun Nabila Ramadhani, Zulfikar Fahmi Haedar, Adam Febriansyah, Nur Aini Rakhmawati. "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya", *Jurnal Information Engineering and Educational Technology*, 2, no. 1 (2018) : 65-69. https://journal.unesa.ac.id/index.php/jieet/article/download/3398/pdf/11740

Deli Waryenti. "Ekstradisi dan Beberapa Permasalahannya", *Fiat Justicia Jurnal Ilmu Hukum,* 5, no. 2 *(*2012) : 1-18. https://jurnal.fh.unila.ac.id/index.php/fiat/article/view/64/65

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

Dirgantara, Rio, Ahmad Mahyani, "Landasan Perumusan *Locus Delicti* dalam Surat Dakwaan Pada Kejahatan Siber", *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, 2, no. 1 (2022) : 673-686. https://bureaucracy.gapenas-publisher.org/index.php/home/article/download/160/179/210

Faiz Emery Muhammad, Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web", *Jurnal USM Law Review,* Volume 6, Nomor 1 (2023) : 226-241. http://dx.doi.org/10.26623/julr.v6i1.6649

Febriansyah, Rozi Yudha, "Delik-Delik Diluar KUHP (Tindak Pidana CyberCrime dan Cara Penanggulangan), *JHP (Jurnal Hasil Penelitian)*, 6, no. 2 (2021) : 51-57. https://jurnal.untag-sby.ac.id/index.php/jhp17/article/view/6216/4612

Finot, Pifzen. "Strategi Penentuan Locus Delicti Tindak Pidana Penerbangan Poho Tanpa Izin di Kawasan Cagar Alam Maninjau Pada Tingkat Penyidikan". *Jurnal UNES Swara Justisia,* 5, no. 1 (2021) : 43-51. https://doi.org/10.31933/ujsj.v5i1.197

Hapsari, Rian Dwi and Kuncoro Galih Pambayun, "Ancaman *CYBERCRIME* di Indonesia", *Jurnal Konstituen*, 5 no. 1 (2023) : 1-17. https://doi.org/10.33701/jk.v5i1.3208

Jawade Hafidz. "Kajian Yuridis dalam Antisipasi Kejahatan *Cyber"*, *Jurnal Pembaharuan Hukum,* 1, no. 1 (2014) : 32-40. https://jurnal.unissula.ac.id/index.php/PH/article/download/1466/1134

Purwaningsih, Ranidan and Dwi Putranto. "Tinjauan Yuridis Terhadap Penetapan Locus Delicti dalam Kejahatan Dunia Maya *(Cyber Crime)* Berkaitan Dengan Upaya Pembaharuan Hukum Pidana di Indonesia Rani Purwaningsih". *Jurnal Mimbar Keadilan,* 16, no. 1 (2023) : 130-138. https://jurnal.untag-sby.ac.id/index.php/mimbarkeadilan/article/view/8021/5438

Rahmadani, Winda, Ali Rahman, Syaiful Munandar. "Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Online". *Sumbang 12 Jurnal,* 1, no. *2* (2023) : 90-97. https://jurnal.umsb.ac.id/index.php/smb12lj/article/view/4044

Rahmawati, "Penentuan Tempus dan Locus Delicti dalam Cyber Crime", *Jurnal Sol Justicia,* 3, no. 1 (2020) : 94-104. https://www.neliti.com/id/publications/408567/penentuan-tempus-dan-locus-delicti-dalan-cyber-crime

Simada, Arthur, Syafruddin Kalo, Mohammad Ekaputra, Jelly Leviza. "Penentuan *Locus Delictie* dalam Tindak Pidana *Cyber Crime* (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)", *Journal Locus* of Academic Litelature Review, 3, no. 4 (2024) : 349-361. https://doi.org/10.56128/ljoalr.v3i4.314

Yasin, Achmad. "Akselerasi Locus Delicti dan Tempus Delicti dalam Nalar Fikih Jinayah", *Jurnal Al-Qanun.* 11, no. 1, (2008) : 232-246. https://jurnalfsh.uinsa.ac.id/index.php/qanun/article/download/146/132/134

Laws and Regulations

Indonesia. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Indonesia. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Indonesia. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Court Decision

ADJUDICATION : Journal Knowledge Law, Volume 8 Number 2, Dec 2024. Pp . 169-182
https://doi.org/10.30656/ajudication.v8i1.8972
P-ISSN 2613-9995 & E-ISSN 2614-0179

Mahkamah Agung Republik Indonesia. Putusan Pengadilan Nomor 951 PN.JKT.SEL/Pid.Sus/2020.

Mahkamah Agung Republik Indonesia. Putusan Pengadilan Nomor 354 PN.JKT.SEL/Pid.Sus/2016.

Thesis, Web Page, and Others

Ayu Pramesti, Tri Jata, "*Tempat Kejadian Perkara, Daerah Hukum Polisi, dan Kewenangan Relatif Pengadilan"* https://www.hukumonline.com/klinik/a/tempat-kejadian-perkara--daerah-hukum-polisi--dan-kewenangan-relatif-pengadilan-lt519a80404efeb/ [diakses pada 05/08/2024].

Firman, Muhammad Nur. "*Data Jumlah Serangan Cyber di Indonesia Tahun 2023"* https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/[diakses pada 03/09/2024].

Saubani, Andri. "Locus Delicti Kasus Denny Siregar yang berubah-ubah*"* https://news.republika.co.id/berita/qpuxdj409/locus-delicti-kasus-denny-siregar-yang-berubahubah, [diakses pada 01/07/2024].

Wawancara bersama Bapak AKP Reno Apri Dwijayanto, S.Kom., S.H. sebagai pimpinan penyidik Sub-Dit 1 Polda Jabar (Panit Siber Polda Jawa Barat).

Wawancara dengan Bapak Christian Dior Parsaoran Sianturi, S.H. (Kepala Subseksi Prapenuntutan Kejaksaan Negeri Kota Bandung).