GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH
**DOI:** https://doi.org/10.38035/gijlss.v3i2


# Uncertainty of Locus Delicti and Tempus Delicti as an Obstacle to Law Enforcement against Cybercrime

**Dwi Nugroho Marsudianto[1], Evita Isretno Israhadi[2]**
[1]Universitas Borobudur, Jakarta, Indonesia, dwi_shinchan@yahoo.com
[2]Universitas Borobudur, Jakarta, Indonesia, evita_isretno@borobudur.ac.id

Corresponding Author: dwi_shinchan@yahoo.com[1]

**Abstract:** Uncertainty in determining the locus delicti (place of the crime) and tempus delicti (time of the crime) is a major challenge in law enforcement against cross-border and anonymous cybercrime. The nature of cybercrime that utilizes technology, such as encryption, VPN, and servers spread across various jurisdictions makes it difficult to determine the exact location and time of the crime, thus hampering the investigation, evidence, and effective law enforcement. Inaccuracy in determining these two aspects can confuse the application of jurisdiction and slow the handling of cases in the judicial realm. Therefore, regulatory reforms are needed that are more adaptive to technological developments to ensure that the legal system can respond to the dynamics of cybercrime more efficiently. Updating laws that align with international standards, strengthening the capacity of law enforcement in digital forensic investigations, and cross-country cooperation are strategic steps in overcoming this obstacle. With a more flexible and technology-based approach, it is expected that the legal system can adapt quickly to the complexity of cybercrime so that law enforcement can run more effectively and accurately, to provide better legal certainty for all parties involved.

**Keywords:** Cyber Crime, Locus delicti, Tempus Delicti

## INTRODUCTION

Locus delicti (place of the crime) and tempus delicti (time of the crime) are two important elements in every criminal case, including cybercrime (Prasatya & Rahmat, 2024). Locus delicti refers to the location where the crime occurred or can be determined from its effects or consequences (Darmawan & Kadir, 2021), while tempus delicti refers to the time the crime occurred which can affect the application of legal sanctions (Simbolon & Gunarto, 2018). These two elements are important because they determine which court has the authority to try the case and affect the validity of the charges and evidence in the trial process, especially when the crime is committed involving technology that is not bound by geographical or time constraints.

Locus and tempus delicti play a crucial role in determining the competence of the court, the validity of the charges, and the process of investigating and examining cases in the criminal justice system (Rasiwan, 2023). Locus delicti determines the court that has jurisdiction over

the case, while tempus delicti helps identify whether an act occurred within a relevant time period for the application of applicable law. In Articles 84 and 143 of the Criminal Procedure Code, the determination of the place and time of the crime refers to the authority of the district court which has the right to try the case, as well as the obligation of the prosecutor to include in detail the time and place in the indictment to ensure legal certainty and clarity of the trial process (Terisno, 2019).

Cybercrime has unique characteristics that distinguish it from conventional crimes (Nabila, 2024). One of the main characteristics is its cross-border nature, where the perpetrator and victim can be in different countries, but remain connected in cyberspace (Barkatullah, 2019). Cybercrime utilizes sophisticated technology such as hacking software, computer viruses, and botnets to carry out its actions, as well as the very rapid dissemination of information via the internet (Ferdiansyah, 2018). This crime can be committed in multiple locations simultaneously, making determining the locus delicti (place of occurrence) very complex, because the physical location of the perpetrator and victim often cannot be determined.

Determining the locus delicti and tempus delicti in cybercrime cases is very difficult due to the digital and anonymous nature of this crime. For example, data used to commit cybercrime can be stored on servers located abroad, making determining the place of occurrence of the crime complicated. The use of sophisticated technology such as encryption and software that can hide the perpetrator's digital footprints hinders efforts to identify the location and time of the incident (Budiyanto, 2025). Time uncertainty also arises because perpetrators can often access the victim's system at various times, or even carry out programmatic attacks that are not immediately visible.

Rapid technological developments, such as the use of VPN (Virtual Private Network), data encryption, and distributed network systems (for example, the use of blockchain) further exacerbate the challenges in determining the location and time of the incident in cybercrime (Dahlan, 2024). This technology allows perpetrators to hide their tracks and avoid detection by law enforcement. For example, by using a VPN, perpetrators can hide their real IP address and redirect their activities to a server located in another country, making it very difficult to determine the locus delicti. Cyberattacks carried out through distributed networks or using encryption can make investigations more complicated because the data needed to determine the time or location of the incident is often hidden or inaccessible.

Uncertainty in determining the locus delicti (place of incident) and tempus delicti (time of incident) in cybercrime can have a major impact on the competence of the court. Without a clear determination of where and when the crime occurred, the court may have difficulty to determe the jurisdiction or authority to try the case (Simada, 2024). This can lead to conflicts of competence between different courts or even cause delays in the legal process, which ultimately hinders access to justice for victims of cybercrime.

Uncertainty in determining the time and place of the occurrence of cybercrime can affect the entire law enforcement process, from investigation to court decision. In terms of investigation, inaccuracy or difficulty in determining the location and time of the incident can cause delays in collecting relevant evidence, thus hindering the investigation process. An indictment that does not clearly state the time and place, as regulated in Article 143 of the Criminal Procedure Code, could potentially invalidate the case of the charges (Suryanagara, 2016). As a result, the court may have difficulty in making fair and appropriate decisions, which leads to the inability of law enforcement to provide a deterrent effect on cybercrime perpetrators.

The research is important to address the complexity of determining the place (locus delicti) and time (tempus delicti) in cybercrime cases, which often involve sophisticated technology and are cross-border. The inconsistency between the characteristics of cybercrime

and existing legal regulations poses a major challenge in law enforcement, especially court competence and the effectiveness of the investigation process. In this context, the first problem formulation highlights the difficulty in determining the place and time of the crime in cybercrime cases, which can affect the court authority. The second problem formulation discusses how uncertainty in determining the place and time can interfere with the effectiveness of law enforcement, both in terms of investigation, indictment, and court decisions, which ultimately impact justice and the effectiveness of the law. This research aims to fill the existing legal gap and contribute to the development of policies that are more appropriate and responsive to technological developments

## METHOD

The research method used in this study is normative research with a statutory approach, which focuses on the study of laws and regulations governing the determination of place (locus delicti) and time (tempus delicti) in cybercrime cases. This approach aims to analyze the relevance and application of existing legal provisions, as stated in the Criminal Procedure Code (KUHAP) and related laws, to understand how the law can respond to the complexity arising from digital and cross-border crimes. With this approach, this study will explore gaps or inconsistencies in existing regulations, as well as provide recommendations for improving and developing regulations that are more in line with developments in information technology.

## RESULT AND DISCUSSION

### Complexity of Determining Place and Time of Occurrence of Cyber Crime Cases

Cybercrime is a form of crime committed by utilizing information and communication technology, especially the internet, to carry out illegal acts, such as hacking, data theft, or online fraud (Guardian, 2020). This crime has a different nature from conventional crimes because it can occur globally, involves sophisticated technology, and often involves the anonymous identity or location of the perpetrator (Richard, Andri, & Sapan, 2025). One of the main challenges in law enforcement against cybercrime is the difficulty in determining the place (locus delicti) and time (tempus delicti) of the crime. In the context of cybercrime, this is important to determine the jurisdiction of the court, the authority of the investigator, and the validity of the charges that can be brought against the perpetrator, considering that this crime can involve various countries with different legal systems.

Locus delicti (place of the crime) and tempus delicti (time of the crime) are two very important elements in the criminal law system, including in cases of cybercrime (Prasatya & Rahmat, 2024). Locus delicti refers to the place or location where the crime occurred, while tempus delicti refers to the time at which the crime was committed. In cybercrime, determining these two elements becomes more complicated due to the cross-border nature of cybercrime, where a crime can occur simultaneously in various places through cyberspace. In addition, technologies such as encryption and the use of VPN networks make determining the location and time of the incident even more difficult, because the digital traces left by the perpetrator can be spread across various servers located abroad or even hidden in a distributed system.

In the Indonesian legal framework, determining locus and tempus delicti is very important to determine the competence of the court in trying a case (Purnawinata, 2021). Article 84 of the Criminal Procedure Code explains that the district court has the authority to try criminal cases that occur in the jurisdiction of the place of the incident, as well as where the defendant lives or is found (Terisno, Imposition of Two Criminal Case Decisions in the Same Object of Case: (Study of Decision Number 2135 K / Pid. Sus / 2016)., 2019). This also applies to crimes committed across borders, as stated in Article 86 of the Criminal Procedure Code which states that crimes committed abroad can be tried by the Central Jakarta District Court if they meet the provisions of Indonesian law. In addition, Article 143 of the Criminal Procedure

Code requires the indictment to include the time and place of the crime, which is also a reference in ensuring the validity of the indictment and the court's authority to process the case (Kartiko, 2024). Clarity in determining the time and place is very important to ensure a fair legal process and in accordance with applicable legal procedures.

Determining the place of occurrence of cybercrime (locus delicti) is quite a challenge because the nature of this crime is cross-border and not bound by a specific physical location. Cybercrime can be committed from various places simultaneously, both in cyberspace and the physical world. For example, a cybercriminal can attack a computer system or network located in Indonesia, but the attack is carried out from a server located abroad (Sari, 2023). This condition makes determining the place of occurrence of the crime more complicated because the location of the attack often cannot be clearly identified or can even be spread across many places around the world.

Cases of cyber-attacks involving the use of servers abroad or the distribution of data on the global network also exacerbate the complexity of determining the locus delicti. In this case, although the impact of the attack can be felt in Indonesia, the physical place that can be linked to the crime may be in another country. For example, the case of a Distributed Denial of Service (DDoS) attack that attacks a website in Indonesia can be controlled from servers spread across several countries, making it difficult to determine the exact location of the incident. This adds to the difficulty for law enforcement in identifying the location of the incident which is the basis for the court's authority.

The use of increasingly advanced technology, such as Virtual Private Networks (VPN) and other digital identity-hiding techniques, allows cybercriminals to hide their real location. The use of VPNs or proxy servers to direct data traffic to different locations allows perpetrators to launch attacks from locations that cannot be easily tracked. This situation makes it difficult for courts and authorities to determine the exact location to begin the process of investigation and prosecution because the digital traces left behind do not clearly indicate where the crime occurred. As a result, law enforcement in cybercrime has become more complex and requires international cooperation and flexible legal mechanisms.

Determining the time of occurrence of cybercrime (tempus delicti) is a major challenge because of the nature of this crime which can occur simultaneously in various places and times, and often involves technology that can hide or change the time trail of the incident. Cybercrime, such as DDoS attacks or the spread of malware, can occur in seconds or minutes, and often the digital traces left by the perpetrators do not record a clear or accurate time. In addition, data involved in cybercrime is often stored on servers spread across various countries, which can confuse in determining when the crime occurred.

The use of encryption technology and VPNs by cybercriminals further worsens the determination of the time of the incident. Encryption can hide the time of transmission of data or certain events relevant to the crime committed, while VPNs allow perpetrators to change their location and time trail of origin. Thus, even though a digital time recording system may exist, the technology can be manipulated or hidden, making it difficult for law enforcement to determine the exact time associated with a crime. This can hinder the investigation process and can complicate charges and the presentation of evidence in court.

The difference in time zones between the countries where the perpetrator and victim are located is also a factor that complicates determining the tempus delicti. Cybercrime often involves perpetrators operating in countries with different time zones, which can confuse determining the exact time of the incident. For example, when an attack occurs at 11 pm local time in Indonesia, but the perpetrator is in a country with an earlier time zone, the time of the attack can be recorded significantly differently. This affects the accuracy of recording the relevant time, and may confuse the ongoing legal process, both in terms of investigation and in determining the authority of the court trying the case.

The development of technology, especially in terms of the use of devices that can hide digital traces, has increased the complexity of determining the place and time of cybercrime. Technologies such as VPNs (Virtual Private Networks) and other anonymizing techniques allow perpetrators to hide their physical location and identity, making it extremely difficult to identify where the crime occurred. In addition, increasingly sophisticated data encryption and cloud storage also exacerbate this challenge, as data stored on servers distributed around the world can obscure the time and location of the incident. This makes it difficult for authorities to conduct accurate investigations, as well as to determine the appropriate jurisdiction and authority of the court to try the case.

**Effectiveness of Law Enforcement Regarding the Place and Time of the Crime in Cybercrime**

The effectiveness of law enforcement in cybercrime is very important because this crime involves technology that can penetrate geographical and time boundaries, making it difficult to identify and overcome. Determining the place (locus delicti) and time (tempus delicti) in cybercrime cases is crucial because both determine the competence of the court and the jurisdiction that has the authority to try the case. Without a clear determination of the place and time, the legal process can be hampered, because it cannot be ascertained which court has the authority, and how evidence can be carried out effectively. Therefore, it is important to develop a legal mechanism that can handle this complexity and ensure effective law enforcement in the context of cybercrime.

The legal system faces major challenges in determining the place and time of the crime because of the cross-border nature of this crime and the involvement of various technological elements. Cybercrime can be committed from various locations that are not limited by physical territory and can use various tools and networks spread across various countries. It causes difficulties in determining the locus delicti (where the crime occurred) because cyber attacks can be carried out from servers abroad, or data distributed through internet networks distributed in various locations. This uncertainty hampers the legal process, especially in terms of determining the competent court and the appropriate jurisdiction to try the case.

The impact of difficulties in determining location and time greatly affects the smoothness of the legal process, including investigations, charges, and evidence in court. Determining the exact time is also hampered by the technology used by the perpetrator, such as the use of VPNs, encryption, or distributed networks that can hide digital traces. This makes it more difficult to identify the time of the incident, especially when time zone differences or anonymity techniques are used to disguise when and where the crime was committed. Thus, the role of technology in complicating the identification of the place and time of the incident is very significant and requires a flexible and adaptive legal approach so that law enforcement remains effective.

Determination of locus delicti and tempus delicti plays a very crucial role in determining the competence of the court and jurisdiction in law enforcement (Winarni, 2016), especially in cybercrime. Locus delicti or the place where the crime occurred determines where the crime can be tried, which is directly related to the court's authority to handle the case (Purwaningsih, 2023). For example, in cybercrimes involving parties from various countries, determining a clear place of occurrence helps identify the competent court, whether it is a court in the perpetrator's country of origin or the country where the server was attacked. Likewise with tempus delicti or time of occurrence, it is important to know when the crime was committed and to ensure that the court that decides the case is within the time limit specified by applicable law.

Accurate determination of location and time also directly affects the validity of the indictment and the smooth implementation of the investigation. Without proper determination,

the indictment prepared by the prosecutor can be null and void, because it does not clearly state the place and time, as regulated in Article 143 of the Criminal Procedure Code. In addition, investigators will also have difficulty tracking evidence that can support the judicial process if the place and time of the incident cannot be ascertained. In the context of cybercrime, this is further complicated by the use of technology that can disguise digital traces and make law enforcement more difficult.

Uncertainty in determining the time and place of a crime in cybercrime can have a direct impact on the effectiveness of investigations and evidence collection. Without clarity regarding the location and time of the incident, investigators will have difficulty tracking digital traces and identifying relevant witnesses. In addition, the evidence collected may be scattered across various servers located abroad, making the investigation process more complex and requiring international cooperation. This also increases the potential for evidence to be lost or damaged before it can be properly identified or analyzed, which in turn hinders the ability to prove the perpetrator's guilt.

Uncertainty about the place and time of the cybercrime incident also slows down the judicial process and enforcement of sentences. In the legal system, unclear time and place can result in inaccuracy in determining the jurisdiction of the court authorized to try the case. A court that does not have the authority can cause delays in the legal process, even the cancellation of the case, if no appropriate competence is found. In addition, this uncertainty can be detrimental to the victim who expects fast and effective justice. This protracted process has the potential to reduce public trust in the justice system.

For example, in cases of global cyber attacks such as hacking of large companies or theft of personal data, determining the time and place is often difficult. In cases of hacking, perpetrators can use VPNs or servers located abroad, and hide their digital footprints with encryption. It makes it difficult for investigators to determine when and where the attack took place, which ultimately hinders the investigation and slows down the legal process. The ambiguity of the location and time of the incident can result in a longer time in law enforcement and often leads to failure in the process of punishing cyber criminals.

To overcome the challenges in law enforcement against cybercrime, it is important to make improvements to existing laws and regulations. One step that can be taken is to update and improve existing regulations to be more relevant to developments in information technology. For example, including more specific provisions related to the regulation of jurisdiction and authority of the court in cybercrime cases, as well as providing clarity regarding the mechanism for cross-border law enforcement. In addition, it is also important to ensure that cybercriminal law covers crimes related to new technologies, such as the use of VPNs, encryption, or other concealment techniques commonly used by perpetrators of crimes.

Increasing the capacity of law enforcement agencies is also key to addressing the challenges posed by technology in law enforcement (Dinda, 2024). Law enforcement agencies need to be equipped with adequate knowledge and skills in digital and cyber technology, as well as sophisticated equipment to be able to track evidence and digital traces left by perpetrators. More intensive training for law enforcement officers in cybercrime and collaboration with technology experts or companies can improve their ability to deal with increasingly sophisticated and complex cybercrime developments.

In order to increase the effectiveness of investigations and law enforcement, adjustments to technological developments are also very necessary. One of them is by introducing new technologies that can assist in collecting digital evidence, such as data analysis software that can examine digital traces more efficiently and accurately. The blockchain technology, for example, can be used to increase transparency in the collection of evidence and verify the validity of the data found. In addition, international collaboration in the field of technology is also important to ensure that laws can be adapted to the global nature of cybercrime, which

often involves perpetrators and servers spread across different countries. With these steps, law enforcement in the field of cybercrime can be more effective and responsive to changing times.

## CONCLUSION

The complexity of determining the place (locus delicti) and time (tempus delicti) in cybercrime arises because the nature of the crime often involves locations and times that are difficult to identify due to the technology used, such as encryption, VPNs, and servers spread across various countries. Uncertainty in determining these two aspects can hamper the investigation process and slow down law enforcement. Therefore, it is very important to carry out legal reforms that include adjustments to technological developments and a more adaptive approach to these digital challenges, to ensure the effectiveness of the justice system in handling cybercrime cases more efficiently and accurately.

The effectiveness of law enforcement in cybercrime cases is highly dependent on the accurate determination of the place (locus delicti) and time (tempus delicti) of the crime. Uncertainty in determining these two aspects can hamper the investigation process, slow the collection of evidence, and make it difficult to apply the right jurisdiction, which can ultimately slow down the entire justice process. Therefore, more dynamic and responsive legal adjustments to technological developments are important to create an effective justice system, especially in handling increasingly complex cybercrime cases. Such measures, including legislative reforms and capacity building of law enforcement agencies, are needed to ensure more efficient law enforcement and the ability to address the challenges posed by digital and transnational crimes.

## REFERENCES

Barkatullah, A. H. (2019). *Hukum Transaksi Elektronik di Indonesia: sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia.* Bandung: Nusamedia,.

Budiyanto. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia.* Banten: Sada Kurnia Pustaka.

Dahlan, A. (2024). *Literasi digital akademik.* Makassar: TOHAR MEDIA.

Darmawan, S., & Kadir, N. A. (2021). ANALISIS TERHADAP DISPARITAS PUTUSAN HAKIM DALAM TINDAK PIDANA PEMBUNUHAN BERENCANA (Studi kasus Putusan Nomor 1608/Pid. B/2019/PN Jkt. Utr dengan Putusan No. 70/Pid. B/2016/PN. Kla). *JCA of Law* .

Dinda, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* , 69-77.

Ferdiansyah. (2018). Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware. *JUSIFO (Jurnal Sistem Informasi)*, 37-48.

Kartiko, N. D. (2024). Juridical Analysis of Interim Decisions in Cases of Embezzlement in Office: Case Study of Decision Number 664/Pid. B/2013/PN. Jkt. Sel. *Journal of Legal and Cultural Analytics*, 73-88.

Nabila, A. P. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional.". *Indonesian Journal of Law*, 26-37.

Nurdiani, I. P. (2020). Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime. *Jurnal Kriminologi Indonesia* .

Prasatya, A., & Rahmat, D. (2024). PENEGAKAN HUKUM TINDAK PIDANA PENCEMARAN NAMA BAIK MELALUI MEDIA SOSIAL. *MALA IN SE: Jurnal Hukum Pidana, Kriminologi, dan Viktimologi*, 43-54.

Prasatya, A., & Rahmat, D. (2024). PENEGAKAN HUKUM TINDAK PIDANA PENCEMARAN NAMA BAIK MELALUI MEDIA SOSIAL. *MALA IN SE: Jurnal Hukum Pidana, Kriminologi, dan Viktimologi* , 43-54.

Purnawinata, D. T. (2021). Aspek Hukum Pidana Dalam Perjudian Secara Online. *Jurnal Solusi*, 261.

Purwaningsih, R. (2023). Tinjauan Yuridis Terhadap Penetapan Locus Delicti dalam Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana di Indonesia. *Mimbar Keadilan*, 130-138.

Rasiwan, I. (2023). *KEWENANGAN HAKIM DALAM PERSIDANGAN PERKARA PIDANA TENTANG PENAHANAN SAKSI MENJADI TERSANGKA.* Bengkulu: Yayasan Sahabat Alam Rafflesia.

Richard, Andri, & Sapan, H. B. (2025). Peran Transformasi Hukum Pidana dalam Mengatasi Kejahatan Siber Berbasis AI dan Geopolitik. *Jurnal Retentum*, 434-449.

Sari, I. (2023). Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai Cyber Crime Dan Cyber Warfare. *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, 241-260.

Simada, A. (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* , 349-361.

Simbolon, T. M., & Gunarto. (2018). Kebijakan Hukum Pidana Terhadap Tindak Pidana Penghinaan Atau Pencemaran Nama Baik Melalui Internet Di Indonesia Sebagai Cybercrime. *Jurnal Daulat Hukum* .

Suryanagara, A. (2016). Dakwaan Batal Demi Hukum Setelah Pemeriksaan Pokok Perkara Dalam Sidang Pengadilan (Studi Putusan Nomor 19/Pid. Sus/2015/PN. Sim). *USU Law Journal*, 204-220.

Terisno, P. A. (2019). *"Penjatuhan Dua Putusan Perkara Pidana Dalam Suatu Objek Perkara Yang Sama:(Kajian Putusan Nomor 2135 K/Pid. Sus/2016).* Indonesian Journal of Criminal Law, 22-32.

Terisno, P. A. (2019). Penjatuhan Dua Putusan Perkara Pidana Dalam Suatu Objek Perkara Yang Sama:(Kajian Putusan Nomor 2135 K/Pid. Sus/2016). *Indonesian Journal of Criminal Law*, 22-32.

Winarni, R. R. (2016). Efektivitas Penerapan Undang–Undang Ite Dalam Tindak Pidana Cyber Crime. *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat*.