DE LEGA LATA
Jurnal Ilmu Hukum
Volume 10 Nomor 2, July-December 2025
E-ISSN: 2477-7889 I ISSN: 2477-653X I Akreditasi: SINTA 3, SK No: 28/E/KPT/2019
http://jurnal.umsu.ac.id/index.php/delegalata

Dark Web in Narcotics Crime: A Critical Study of Central Jakarta District Court Decision No. 12/Pid.Sus/2023

Dewi[1], Albert Fajar Yuga Yusdi Putra[2], Lee Yong Hwa[3], Meivina Jayanti[4], Muhammad Elvio[5]
[1,2,3,4,5] Universitas Pelita Harapan, Indonesia
Email : 01053240069@student.uph.edu (Corresponding Author)

Accepted: 09-06-2025. Revised: 11-06-2025 Approved: 12-06-2025 Published: 13-06-2025
DOI: 10.30596/dll.v10i2.24979

How to cite:
Dewi, et, al. (2025). "Dark Web in Narcotics Crime: A Critical Study of Central Jakarta District Court Decision No. 12/Pid.Sus/2023", De Lega Lata: Jurnal Ilmu Hukum, Volume 10 (2): p. 203-210

Abstract

The distribution of narcotics through the dark web is a new criminal offense in the Indonesian judicial system. This paper attempts to examine how the court views the use of the dark web as evidence related to criminal cases through an examination of the Central Jakarta District Court Decision No. 12/Pid.Sus/2023. This paper employs a normative legal approach methodology, analyzing each court decision document. The research findings indicate that while electronic evidence demonstrating connections to activities on the dark web has been submitted, there remain significant challenges in proving the connection between such evidence and the elements of the crime. These findings underscore the need for further regulatory improvements alongside enhanced capacity of law enforcement agencies in addressing crimes facilitated by increasingly sophisticated technology today.

Keywords: Dark Web, Drug Trafficking, Crime, Court Rulings, Electronic Evidence.

INTRODUCTION

The development of information technology today has created disruption in many aspects of human life, including in the modus operandi of criminal acts. And one technological innovation that poses a major challenge to law enforcement is the existence of the Dark Web, which is a hidden part of the internet that cannot be reached through conventional search engines such as Google or Bing (Marie-Helen Maras, 2016). The Dark Web can only be accessed using specialized software such as Tor (The Onion Router) which provides a layer of anonymity to its users (Michael Chertoff and Tobby Simon, 2015).

In practice, the Dark Web has developed into a digital space that is often used as a space for various illegal transactions and one of the most common activities found on the Dark Web is the illicit drug trade, which is carried out anonymously and protected by sophisticated encryption systems. These transactions usually use cryptocurrencies such as Bitcoin, which makes the process of tracing the identity of the perpetrator and the distribution channels more complex and difficult to identify (James Martin, 2014). In Indonesia, the use of the Dark Web in drug offenses is still a relatively new phenomenon, but that does not mean it is insignificant. And one of the cases that shows the close relationship between Dark Web technology and narcotics crime is the Central Jakarta District Court Decision No. 12/Pid.Sus/2023. And in that case, the defendant was proven to have used the Dark Web to obtain ecstasy narcotics, where payment was made through cryptocurrency (Decision No. 12/Pid.Sus/2023, 2023). This case is very interesting to study in depth because it illustrates how national criminal law responds to crimes with non-conventional technology-based methods.

The problem that arises is whether the national legal system, especially Law No. 35/2009 on Narcotics and Law No. 11/2008 on Electronic Information and Transactions (ITE), is adequate in dealing with this form of crime and whether law enforcement officials, including judges, have understood the dynamics of the technology used in these crimes and are able to apply it in a comprehensive legal consideration?

A critical study of the court's decision in this case is very important because it does not only involve understanding the normative aspects of criminal law and cyber law, but also to assess the ability of legal institutions to adapt to the complexity of information technology that continues to develop.

METHOD RESEARCH

This research uses a normative juridical approach, which is a method that relies on a literature study of legislation, legal doctrine, and relevant court decisions (Soerjono Soekanto dan Sri Mamudji, 2001). And in this case, the Central Jakarta District Court Decision No. 12/Pid.Sus/2023 will be used as the main material for analysis through a case study approach and can be used to examine the applicable positive legal norms, and can understand how these provisions are applied, especially in judicial practice, especially technology-based narcotics crimes.

The main object of analysis is the Central Jakarta District Court Decision No. 12/Pid.Sus/2023, which will be used as a case study to evaluate the application of criminal law and cyber law in Indonesia in dealing with crimes that utilize the Dark Web and cryptocurrency. And this case study is analyzed using a descriptive-analytical approach, which aims to systematically describe legal facts and evaluate the judge's legal considerations in the context of proof and punishment.

Secondary data sources are obtained from laws and regulations, court decisions, academic journals, and academic literature relevant to the research theme and analysis is carried out by linking applicable norms with actual judicial practices to assess the effectiveness of positive law in responding to increasingly complex forms of technology-based crime.

DISCUSSION

1. Chronology and Legal Facts in the Case and Analysis of Judges' Considerations

The narcotics criminal case registered as Number 12/Pid.Sus/2023/PN.Jkt.Pst serves as a clear illustration of the integration of advanced technology in organized crime, highlighting a shift in the modus operandi of narcotics offenses toward digital and transnational domains. According to the public prosecutor's indictment, the defendant, AR, was proven to have acquired ecstasy through the Dark Web a concealed segment of the internet accessible only via encrypted networks such as Tor, which are specifically designed to anonymize users' identities. The server hosting the illicit platform was located overseas, and the transaction was facilitated using cryptocurrency specifically Bitcoin which was transferred to a digital wallet account based abroad. This transaction unequivocally qualifies as illegal and necessitates immediate action. However, addressing such crimes demands cross-border cooperation, advanced detection technologies, and firm legal enforcement. While this presents considerable challenges, it is essential to act swiftly to minimize societal harm and protect future generations.

According to the prosecutor's indictment, the transactions are conducted anonymously through peer-to-peer systems and digital crypto wallets that cannot be directly traced to the identity of the owner. This activity makes it difficult to track the flow of money and identify the perpetrators involved in the network. In this case, cryptocurrency becomes a payment intermediary that allows for fast, cheap and relatively unmonitored cross-border trade.

The initial investigation was conducted by the Directorate of Drug Crimes at the Criminal Investigation Unit of the National Police after receiving information from Interpol regarding suspicious package delivery activity from the Netherlands to Indonesia. After several weeks of surveillance, the package containing the narcotics finally arrived at the destination address used by the defendant as a fictitious identity and field reconnaissance led to the arrest of AR when he picked up the package at a predetermined location via an expedition service.

He also admitted that he never directly knew the seller and all communication was done through encrypted messaging services and payment was also made through an unidentified account into a wallet using bitcoin on a crypto peer-to-peer network, and the identity of the seller was never known. This fact shows that AR is an active user of cyber technology in carrying out the narcotics crime he has committed.

Prosecutors finally charged AR with Article 114 paragraph (2) in conjunction with Article 132 paragraph (1) of Law Number 35 of 2009 concerning Narcotics which regulates the attempt or conspiracy to distribute class I narcotics in large quantities and because it was proven to have committed an attempt or conspiracy to distribute class I narcotics in large quantities, during the trial, evidence in the form of ecstasy totalling more than 1,000 items with a transaction history of crypto wallets, and screenshots of Dark Web sites from electronic devices confiscated from the defendant.

The panel of judges in their verdict stated that AR's actions were legally proven and constituted a narcotics crime, so AR was sentenced to imprisonment for 15 (fifteen) years and a fine of Rp2,000,000,000 (two billion rupiah) in lieu of 1 (one) year of confinement3. This decision is interesting to be studied further because it considers electronic evidence which has not been fully regulated in Indonesian criminal procedure law in detail and specifically.

In case No. 12/Pid.Sus/2023, the Panel of Judges of the Central Jakarta District Court handed down a verdict against the defendant with the initials AR who was proven to have committed a narcotics crime by ordering ecstasy through the Dark Web and making payments using cryptocurrency. In handing down their verdict, the Panel of Judges considered several legal aspects that showed a progressive interpretation of the technology-based crime mode.

First, the judges stated that the defendant's modus operandi of utilizing the Dark Web and cryptocurrency did not erase the essence of the drug crime itself but rather showed a new level of sophistication in its implementation. Therefore, the judge still referred to the provisions of Article 112 paragraph (1) and Article 114 paragraph (1) ofthe Narcotics Law as the legal basis for punishment, even though the tools and methods of the crime were digital.

Second, the judge considered that the evidence in the form of digital forensic results submitted by the public prosecutor had met the requirements as legal evidence, based on Article 5 paragraph (1) of the ITE Law. Evidence such as Bitcoin transaction history from the defendant's wallet address, encrypted communication recordings through a special application, as well as the results of digital tracking of narcotics marketplaces on the Dark Web, were considered to have provided sufficient confidence in the defendant's involvement in the transaction (Undang Undang No. 11 Tahun 2008 Tentang ITE, 2008).

Third, the judge's reasoning also reflected an intellectual and functional approach to the law, where the judge did not only focus on the formal form of evidence, but also on the substance and integrity of the evidence, including the validity of the method of tracing the defendant's identity through the virtual network mapping (Tor) used (Satjipto Rahardjo, 2010).

However, in this decision, there is no explicit statement from the judge regarding the urgency of law reform related to the Dark Web and cryptocurrency. The verdict tends to use a conventional legal framework to interpret actions that are based on high technology. This reflects the limitations of positive law in anticipating the evolution of increasingly complex digital crimes (Haposan Hutabarat, 2022).

Finally, the judge still found the defendant guilty and sentenced him to 8 years of imprisonment and a fine as stipulated in the criminal provisions of the Narcotics Law. This decision shows the court's efforts to apply the law dynamically amidst the limitations of the regulation of information technology and digital transactions.

2. The Development of Cybercrime in Drug Trafficking and Crypto in Drug Crime

Today's advances in digital technology have fundamentally changed the landscape of crime and have revolutionized the form and modus operandi of crime around the world, including in terms of illicit drug trafficking. Narcotics crime is no longer limited to direct physical transactions, but has transformed and is categorized as cybercrime, namely criminal acts committed by utilizing technological systems as the main medium for committing crimes using digital (David S Wall, 2007).

Cyber-based drug trafficking is carried out by utilizing a variety of digital devices including encrypted messaging applications with only an internet connection and digital wallets. In addition, VPN (Virtual Private Network) technology, proxy servers, and the use of false identities or pseudonyms make it more difficult for law enforcement officials to identify the real perpetrators because they use blockchain technology, anonymous wallet addresses, encrypted communication channels such as Telegram or Signal and transactions through cryptocurrencies such as Bitcoin and Monero, as well as access to digital darknet marketplaces such as Hydra Market or AlphaBay. Transactions made through these platforms are difficult to trace (Europol, 2022).

Criminals do not need to physically interact with buyers or couriers, but with just an internet network and privacy-enabled software such as VPNs (Virtual Private Networks), proxy servers, and digital pseudonyms, they can carry out their operations covertly. In many cases, the delivery of goods is also carried out using third-party expedition services, which makes tracking even more difficult because it does not involve the real identity of the perpetrator (UNODC, 2023).

According to the UNODC (United Nations Office on Drugs and Crime) *World Drug Report*, drug trafficking through the Dark Web has become part of a decentralized transnational crime infrastructure. It allows drug networks to operate globally without jurisdictional boundaries and with less legal risk. The online black market enables the distribution of drugs from one country to another at a low cost and with a wide.

In Indonesia, the main challenges in dealing with this phenomenon are limited human resources, technological tools, and lack of adaptive regulations. Although some law enforcement units have started to develop digital forensic units and cooperation with international institutions, their effectiveness is still limited and not optimal for the legal framework in ensnaring cross-border digital criminals. From a law enforcement perspective, cyber-narcotics demands new capabilities in digital forensics, blockchain tracking, and the use of cyber-intelligence, but in Indonesia, limited human resource capacity, software, and regulations are still relatively behind the dynamics of advanced and evolving crimes. This shows that drug crime has now become a transnational and complex problem that can no longer be handled only with conventional approaches but must be balanced with the development of sophisticated digital tools and support in dealing with drug crimes in the age of digitalization like today.

Thus, narcotics crime has undergone a transformation from a local problem to a global threat that is digitally hidden, and highly organized. In this case, handling requires a multidisciplinary approach that includes law, technology, and cooperation between countries in forming a comprehensive and integrated response (David Bryans, 2021).

The emergence of cryptocurrencies as financial instruments based on blockchain technology has triggered a profound transformation in the digital economy ecosystem (Nakamoto, 2008). Initially designed to be decentralized, secure, and anonymous, cryptocurrencies such as Bitcoin, Monero, and Zcash were originally developed to democratize the global payment system and protect the privacy of users (Möser, 2013). However, these characteristics were later misused by some users by facilitating cryptocurrencies as the main means of payment in committing criminal acts, especially in the scope of narcotics trafficking, money laundering, and Dark Web-based terrorism financing.

In various digital black markets such as AlphaBay, Silk Road, and Hydra Market, narcotics transactions no longer use cash, but exclusively all transactions rely on cryptocurrencies. This is because crypto allows offenders to make cross-border transactions without going through formal financial channels overseen by official regulators such as official institutions and banks that must verify the identity of the user, and the use of pseudonyms in these digital wallets can create a layer of protection that makes it difficult for law enforcement authorities to trace the user's real identity so that this crypto is a fairly safe means of payment for the offender or user.

Furthermore, several types of crypto, including Monero and Zcash, have been equipped with a fairly perfect technology where all transaction information, sender data, recipients, and the amount of funds cannot be traced. And they use quite sophisticated privacy features to protect the criminal acts committed and this will add complexity to law enforcement efforts to act because these transactions cannot be easily traced, even by highly capable cyber agencies.

And in the AlphaBay case exposed by the FBI and Europol in 2017, it was found that the proceeds of massive narcotics trafficking were stored in Bitcoin, then laundered (money laundering) through mixing services, illicit exchanges, and other digital asset conversions (FBI Press Release, 2017). This strategy aims to disguise the origin of funds to avoid being traced in the legitimate global financial system.

This practice shows that crypto has evolved into a strategic tool in transnational narcotics crime especially facilitated by Dark Web infrastructure.

In Indonesia, although Law No. 8/2010 on “Prevention and Eradication of Money Laundering Crimes” has opened up space for the supervision of digital assets, its implementation still faces various challenges both technically and regulatively (Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang, 2010). This is due to the lack of explicit legal instruments on the use of cryptocurrencies in drug crimes, which is one of the obstacles for law enforcement to take effective action.

3. Conceptual Framework for Analyzing Court Decisions

In analyzing the Central Jakarta District Court Decision No. 12/Pid.Sus/2023, the conceptual approach used is to combine an understanding of the phenomenon of digital-based drug crime through the Dark Web with the application of Indonesian positive law.

This framework refers to three main pillars, namely:

a. Legal characteristics of technology-based transnational crimes
b. Legal protection of society from the negative impact of the development of digital technology
c. The adaptive ability of the criminal justice system in dealing with cybercrime.

1) Cyber Crime and its Transnational Dimension
Crimes involving the use of the Dark Web and cryptocurrencies are classified as a new form of transnational crime that is quite complex, with perpetrators and victims spread across multiple jurisdictions and this will cause difficulties in conventional law enforcement, both in the aspects of tracking the perpetrator, collecting digital evidence, to the execution of interstate law. Therefore, the approach used in analyzing this decision must consider cross-border aspects and keep up with the development of technological changes.
2) Conception of Criminal Responsibility in the Digital Realm
Criminal responsibility in a case like this does not only have to be proven by physical possession of drugs, but also needs to be traced through digital footprints, crypto wallets, and pseudonyms used by the defendant. This refers to evidentiary methods based on digital forensics, including blockchain transaction logs and encrypted communications (Brenner, 2010).
3) Relevance of National Criminal Law Principles
Court decisions must be analyzed within the framework of the principles of legality, fairness, and proportionality. On the one hand, the Indonesian criminal law system still refers to physical and conventional evidence while on the other hand, digital crimes require a more flexible approach, including in interpreting electronic evidence and cryptocurrency transactions as tools of crime (Barda Nawawi Arief, 2012).
4) Responsiveness of the Justice System to Innovative Crimes
This case is an important study of how responsive law enforcement officials and judges are to the growing trend of cybercrime in modern times, especially in the context of drug trafficking. By considering digital evidence and the technology used, judges are required to deeply understand how the Dark Web mechanism works, as well as its legal implications in the national context (David S Wall, 2008).

Through this framework, the analysis of the verdict does not only look at the suitability of formal and material law but must also be assessed from the extent to which the national legal system is able to keep up with the development of digital crimes that continue to change and develop rapidly.

Conclusion

This study explores how the Dark Web and cryptocurrency have changed the landscape of narcotics crime in Indonesia, using the Central Jakarta District Court Decision No. 12/Pid.Sus/2023 as a case study. The case reveals that drug offenders are now utilizing anonymous networks like Tor and digital currencies like Bitcoin to avoid traditional law enforcement detection. This shift marks a growing trend in how illegal drug transactions are being conducted, not only digitally but also across borders, which complicates the legal process and demands more advanced tools and strategies from law enforcement. The involvement of cryptocurrency further limits traceability and enables offenders to operate outside of formal financial systems. The court's handling of this case shows that the Indonesian legal system is attempting to catch up with these technological developments. While the court acknowledged digital evidence and rendered a verdict, its legal reasoning showed limited engagement with complex cyber elements like hash verification or blockchain analysis. This reveals a gap in legal understanding and the lack of specific laws that cover the use of Dark Web platforms and crypto-based drug trafficking. The absence of these legal provisions indicates that current laws particularly the Narcotics Law and the ITE Law are outdated and not fully capable of addressing such crimes.

In summary, this case underlines the urgent need for Indonesia to modernize its criminal justice system to respond to digital-era drug crimes. The transformation of narcotics crime into a cyber-enabled offense requires not only better tools and infrastructure but also legal reforms. Without a proper legal and institutional response, the state risks falling behind in handling such threats, and future generations may face greater risks from the growing nexus between cybercrime and drug trafficking.

Suggestions

First, Indonesia must revise its laws to better reflect the realities of cyber-based narcotics crimes. The current Narcotics Law and ITE Law do not explicitly regulate digital drug markets, cryptocurrency transactions, or anonymous networks like Tor. By updating these laws, the government can provide clearer legal guidelines for law enforcement and the judiciary. The revised law should include definitions of digital evidence, procedures for crypto asset seizure, and recognition of blockchain records as admissible evidence. Without these provisions, legal ambiguity will continue to hinder prosecution.

Second, law enforcement and the judiciary need stronger capacity in handling digital evidence. Technical tools such as blockchain tracing, metadata verification, and hash authentication are essential in investigating cases like this. Therefore, training programs on digital forensics should be implemented across institutions. Moreover, court procedures must be adapted to accommodate the presentation and validation of electronic evidence. Clear technical standards will help judges and prosecutors assess the reliability of evidence derived from digital sources, and prevent wrongful convictions or dismissals.

Lastly, collaboration—both domestically and internationally—is critical. Indonesia must create a specialized cyber-narcotics crime unit with access to the latest technology and authority to work across jurisdictions. At the international level, partnerships with agencies like INTERPOL and UNODC will improve intelligence sharing and assist in tracking crypto transactions that cross borders. Strategic cooperation will also help Indonesia meet global standards in cybercrime prevention. These steps will position the country to effectively counter drug crimes in the digital age while strengthening its overall legal and institutional framework.

REFERENCES

Barda Nawawi Arief. (2012). *Kapita Selekta Hukum Pidana*. Citra Aditya Bakti.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

David Bryans. (2021). Digital Narcotics and Transnational Enforcement Challenges. *Journal of Global Crime*, *10*(3).

David S Wall. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

David S Wall. (2008). Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers & Technology*, *22*(1).

Decision No. 12/Pid.Sus/2023 (2023).

Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*.

FBI Press Release. (2017). *AlphaBay, the Largest Online 'Dark Market', Shut Down*.

Haposan Hutabarat. (2022). Kejahatan Siber dan Tantangan Pembaruan Hukum Pidana Indonesia. *Jurnal Hukum Pidana Dan Teknologi*, *6*(2).

James Martin. (2014). *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. Palgrave Macmillan.

Marie-Helen Maras. (2016). *Cybercriminology*. Oxford University Press.

Michael Chertoff and Tobby Simon. (2015). *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance.

Möser, M. , B. R. , & B. D. (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *ECrime Researchers Summit*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Satjipto Rahardjo. (2010). *Ilmu Hukum: Paradigma Baru dan Implikasinya*. Genta Publishing.

Soerjono Soekanto dan Sri Mamudji. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers.

Undang Undang No. 11 Tahun 2008 Tentang ITE (2008).

Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang (2010).

UNODC. (2023). *Darknet Cybercrime and Drug Trafficking Trends, United Nations Office on Drugs and Crime*.