The Indonesian Journal of International Clinical Legal Education
Vol. 7 Issue 1 (2025) 131-166
DOI: https://doi.org/10.15294/ijicle.v7i1.21109
Available online since: March 31, 2025

The Indonesian Journal of International Clinical Legal Education
https://journal.unnes.ac.id/sju/index.php/iccle/index

Dark Web Crime: Criminal Law Challenges in the Era of Cybercrime

Ana Tasia Pase ✉
Faculty of Law, Universitas Dehasen Bengkulu, Bengkulu, Indonesia

Zico Junius Fernando
Faculty of Law, Universitas Bengkulu, Bengkulu, Indonesia

✉ Corresponding email: paseanatasia.safii@yahoo.com

Abstract

The rapid advancement of digital technology has led to increasingly complex cybercrimes, particularly those occurring on the Dark Web. This hidden part of the internet, accessible only through specialized software such as Tor and I2P, has become a hub for various illegal activities, including drug trafficking, financial fraud, data breaches, human exploitation, and cyberattacks. The primary challenge in combating Dark Web crimes lies in the high level of anonymity afforded by encryption, decentralized digital currencies like Bitcoin and Monero, and jurisdictional limitations in law enforcement efforts. This study employs a normative legal research method with a conceptual and comparative approach to analyze global legal frameworks, enforcement strategies, and jurisdictional complexities in prosecuting Dark Web crimes. The findings

indicate that existing criminal laws struggle to address the dynamic nature of cybercrime, necessitating continuous legal reform, stronger international cooperation, and advanced forensic technologies. Additionally, balancing cybersecurity enforcement with digital privacy rights remains a contentious issue in global legal discourse. This study recommends the harmonization of cyber laws, stricter regulations on cryptocurrency transactions, and improved international legal collaboration to effectively combat Dark Web crimes.

Keywords

Dark Web; Cybercrime; Criminal Law; Cybersecurity; Cyber Law Reform.

I. Introduction

The rapid advancement of digital technology has brought significant changes across various aspects of life, including the evolution of crime patterns that have become increasingly sophisticated and difficult to combat. One of the major concerns in the cyber world is the existence of the Dark Web, a hidden part of the internet that cannot be accessed through regular search engines and requires specialized technology such as Tor (The Onion Router) or I2P (Invisible Internet Project) for access.[1] The Dark Web is often associated with various illegal activities, including drug trafficking, child exploitation, identity theft, hacking, and other cybercrimes. This criminal ecosystem presents a significant

[1] Vijaykumar Bidv and Aishwarya Suryakant Waghmare, "Beyond the Onion Routing: Unmasking Illicit Activities on the Dark Web," *International Journal of Innovative Science and Research Technology (IJISRT)*, June 10, 2024, 2419–40, https://doi.org/10.38124/IJISRT/IJISRT24MAY1698.

challenge for the criminal justice system in terms of investigation, evidence collection, and law enforcement.

One of the key characteristics of the Dark Web that makes it difficult to regulate is its high level of anonymity. Criminal actors can conceal their identities and conduct transactions anonymously using cryptocurrencies such as Bitcoin and Monero, which are difficult for law enforcement authorities to trace. One of the most notable cases of Dark Web-related crime is Silk Road, an online black market that facilitated widespread drug trading before being dismantled by the FBI in 2013.[2] This case demonstrated how the anonymity of the Dark Web enables illegal trade to operate on a global scale without oversight from legal authorities. Although Silk Road's founder, Ross Ulbricht, was sentenced to life in prison, the phenomenon of black markets on the Dark Web did not end there. Various other platforms quickly emerged, often with more advanced security measures to evade law enforcement detection.

Following the closure of Silk Road, AlphaBay emerged as the largest black market on the Dark Web. Established in 2014, AlphaBay became a primary hub for transactions involving drugs, stolen data, illegal weapons, and hacking services. It was estimated to have over 400,000 users and handled cryptocurrency transactions worth hundreds of millions of U.S. dollars. In July 2017, the FBI, in collaboration with Europol and other law enforcement agencies, successfully shut down AlphaBay. The site's founder, Alexandre Cazes, was arrested in Thailand but was found dead in his prison cell before the extradition process to the United States could take place. Despite the dismantling of AlphaBay, other black markets quickly took its place, highlighting the

---

2 James Martin, "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket,'" *Criminology & Criminal Justice* 14, no. 3 (October 7, 2013): 351–67, https://doi.org/10.1177/1748895813505234.

ongoing challenge of shutting down criminal networks operating on the Dark Web.[3]

Alongside the operation against AlphaBay, law enforcement also successfully dismantled Hansa Market, another major Dark Web marketplace. However, the approach taken in dismantling Hansa Market was unique. Instead of immediately shutting down the site, Dutch authorities secretly took control of its servers and operated them for several weeks. This strategy allowed law enforcement to monitor and identify thousands of users who migrated from AlphaBay to Hansa Market after the former's shutdown. The intelligence gathered during this operation enabled authorities to conduct hundreds of arrests across multiple countries, proving that digital infiltration can be an effective method for combating crime on the Dark Web.[4]

In 2019, Wall Street Market, one of the largest remaining black markets, was finally shut down in a joint operation involving the FBI, Europol, and German law enforcement. This marketplace facilitated the sale of illegal goods, including drugs, hacking tools, and stolen data. However, before the site could be completely taken down by authorities, its administrators attempted an exit scam stealing users' funds stored in the site's escrow system before disappearing. This case demonstrated that not only do law enforcement agencies pose a threat to Dark Web marketplaces, but internal fraud and deception among cybercriminals themselves also contribute to their downfall.[5]

---

3 Filippo Andrei and Giuseppe Alessandro Veltri, "Status Spill-Over in Cryptomarket for Illegal Goods," *Social Science Computer Review*, September 21, 2024, 08944393241286339, https://doi.org/10.1177/08944393241286339.

4 Yara Abdel Samad, "Case Study: Dark Web Markets," in *Dark Web Investigation*, ed. Babak Akhgar et al. (Cham: Springer International Publishing, 2021), 237–47, https://doi.org/10.1007/978-3-030-55343-2_11.

5 C Bradley and G Stringhini, "A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets," in *2019 IEEE*

Beyond drug trafficking and the sale of illegal goods, the Dark Web is also used for crimes involving human exploitation, as seen in the case of Welcome to Video. This platform was one of the largest Dark Web sites facilitating the trade of child sexual exploitation materials. In 2019, authorities from the United States, the United Kingdom, South Korea, and Germany collaborated to dismantle this network. The operation uncovered over 8 terabytes of illegal content and led to the arrest of more than 300 individuals worldwide. The site's founder, Jong Woo Son, a South Korean national, was arrested and sentenced to prison.[6] The success of this operation underscored the importance of international cooperation in combating crimes involving human exploitation on the Dark Web.

In response to the growing number of black markets operating on the Dark Web, Operation DisrupTor was launched in 2020 as one of the largest international operations targeting digital criminal networks. The operation involved law enforcement agencies from the United States, the European Union, Canada, and several other countries, successfully leading to the arrest of 179 suspects, the seizure of over $6.5 million in cash and cryptocurrencies, and the confiscation of thousands of illegal weapons and narcotics. This operation demonstrated that while the Dark Web continues to expand, law enforcement agencies are also becoming increasingly sophisticated in their strategies to track and dismantle criminal activities within these concealed cyber spaces.[7]

European Symposium on Security and Privacy Workshops (EuroS&PW), 2019, 453–63, https://doi.org/10.1109/EuroSPW.2019.00057.

6 Merrit Kennedy, "More Than 300 Arrested In Child Porn Site Bust : NPR," https://www.npr.org, 2019, https://www.npr.org/2019/10/16/770628069/one-of-the-worst-forms-of-evil-more-than-330-arrested-in-child-porn-site-bust.

7 Mostafa Soliman, "Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework," *SSRN Electronic Journal*, April 14, 2023, 1–7, https://doi.org/10.2139/SSRN.4418508.

However, these cases illustrate that even though numerous black markets on the Dark Web have been successfully shut down, new platforms inevitably emerge to replace them. Each time a black market is dismantled, criminals adapt by implementing more advanced security systems, making law enforcement efforts increasingly complex. This presents a significant challenge for law enforcement agencies, requiring them to continually develop more advanced investigative technologies, strengthen international cooperation, and balance law enforcement efforts with the protection of legitimate internet users' privacy rights.

Beyond anonymity, jurisdictional issues pose another significant challenge in tackling cybercrime on the Dark Web. Many cybercrimes are perpetrated by transnational offenders, making it difficult for any single country to pursue legal action without international collaboration. For instance, in the case of the REvil Ransomware Gang, a Russian-based hacker group that targeted global corporations such as JBS Foods and Kaseya, U.S. authorities faced challenges in extraditing key perpetrators due to differences in legal frameworks and policies between nations.[8] This scenario underscores that without strong intergovernmental coordination, efforts to combat Dark Web crimes will continue to face significant obstacles.

Additionally, evidence collection in the digital realm remains a major hurdle within the criminal justice system. Crimes on the Dark Web often leverage high-level encryption technologies, making it extremely difficult for law enforcement agencies to access electronic evidence. In the case of Playpen, a child pornography website operating on the Dark Web, the FBI employed digital infiltration techniques to uncover user identities.[9] However, this approach sparked legal

---

8 Nicole Sganga et al, "Russia Arrests 14 Alleged Members of REvil Ransomware Gang," https://www.cbsnews.com, 2022, https://www.cbsnews.com/news/ransomware-russia-arrests-revil/.

9 Ian Warren, Monique Mann, and Adam Molnar, "Lawful Illegality: Authorizing Extraterritorial Police Surveillance," *Surveillance & Society*

controversy, as some courts ruled that the methods used violated privacy rights and the principles of due process of law. This case highlights the ongoing debate surrounding the use of digital evidence in legal proceedings and the challenges posed by differing judicial interpretations across various jurisdictions.

As cybercrime on the Dark Web continues to evolve, the legal challenges extend beyond technological barriers they also require legal norms to adapt to the changing landscape. The ongoing debate on balancing security and privacy rights, regulating cryptocurrencies, and achieving global harmonization of cyber laws remains at the forefront of discussions on law enforcement efforts against Dark Web crimes.

II. Method

This research employs a normative legal method, focusing on the study of applicable legal norms and relevant concepts in addressing crimes on the Dark Web. The research adopts a conceptual and comparative approach. The conceptual approach is used to understand how criminal law concepts can be applied in the context of cybercrime occurring on the Dark Web, including aspects of jurisdiction, evidence, and the role of international law. Meanwhile, the comparative approach involves analyzing various legal models implemented in different countries to combat crimes on the Dark Web, aiming to identify best practices that can be applied within Indonesia's criminal law framework. This study is descriptive-prescriptive in nature.[10] The descriptive approach

18, no. 3 (August 19, 2020): 357–69, https://doi.org/10.24908/ss.v18i3.12795.

10 Zico Junius Fernando, Kiki Kristanto, and Ariesta Wibisono Anditya, "Knitting Democracy, Separating Restraints: Legal Reform and a Critical Analysis of Article 256 of the New Criminal Code and Its Impact on Freedom of Speech," *Journal of Law and Legal Reform* 5, no. 2 (April 30, 2024): 555–86, https://doi.org/10.15294/JLLR.VOL5I2.1670.

systematically outlines the characteristics of crimes on the Dark Web, including modus operandi, challenges in law enforcement, and case studies from various countries. On the other hand, the prescriptive approach formulates policy recommendations and legal solutions to strengthen criminal law enforcement against crimes on the Dark Web, both through the enhancement of national regulations and international legal cooperation. Data for this research is collected through a literature review encompassing various legal sources, such as legislation, academic literature, court rulings, and reports from international law enforcement agencies. Additionally, international legal documents related to cybercrime and intergovernmental cooperation agreements are also primary references in this study. Data analysis is conducted using content analysis[11], where the collected data is examined in depth to identify patterns, legal principles, and challenges in the implementation of laws against crimes on the Dark Web. This approach enables the study to reveal regulatory gaps, assess the effectiveness of existing laws, and evaluate the relevance of criminal law policies in addressing the continuously evolving technological challenges.

[11] Panca Sarjana Putra et al., "Judicial Transformation: Integration of AI Judges in Innovating Indonesia's Criminal Justice System," *Kosmik Hukum* 23, no. 3 (August 15, 2023): 233–43, https://doi.org/10.30595/KOSMIKHUKUM.V23I3.18711.

III. Legal Framework for Combating Crime on the Dark Web: A Comparative Study of National and International Regulations

The existence of the Dark Web as a concealed digital space presents significant challenges for law enforcement, particularly in determining the applicable jurisdiction for criminal law. The Dark Web enables perpetrators to operate without geographical limitations, leading to debates on the application of legal jurisdiction for violations occurring within this space. The principles of criminal law jurisdiction traditionally based on territoriality, nationality, passive personality, and universality often prove insufficient in addressing cybercrimes that transcend national borders. Consequently, many countries have begun expanding their jurisdictional reach to address cybercrimes that impact national interests, even if they are committed outside their legal territories.

One crucial aspect of law enforcement against crimes on the Dark Web is the regulation of cryptocurrency transactions, which serve as a primary tool for criminals to conceal their identities and conduct illicit transactions. Cryptocurrencies such as Bitcoin, Monero, and others are frequently used in illegal activities, including drug trafficking, child sexual exploitation, money laundering, and the trade of personal data.[12] The regulation of cryptocurrency varies significantly across different countries. Nations such as the United States and the European Union have taken substantial steps to regulate cryptocurrency usage to prevent its misuse in illegal activities on the Dark Web. They have implemented Know Your Customer (KYC) and Anti-Money Laundering (AML)

---

12 Sean Foley, Jonathan R. Karlsen, and Tālis J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?," *SSRN Electronic Journal*, December 14, 2018, https://doi.org/10.2139/SSRN.3102645.

regulations, requiring cryptocurrency exchange platforms to verify user identities, report suspicious transactions, and ensure that digital assets are not used for money laundering, terrorist financing, or other illegal transactions.[13]

In the United States, for instance, agencies such as the Financial Crimes Enforcement Network (FinCEN) mandate that virtual currency service providers register as Money Service Businesses (MSBs) and implement monitoring policies for suspicious user transactions. Additionally, regulations under the Bank Secrecy Act (BSA) require cryptocurrency companies to share information with financial authorities to prevent the use of digital assets in transnational crimes.[14] Similarly, in the European Union, the implementation of the Fifth Anti-Money Laundering Directive (5AMLD) has extended AML regulations to the cryptocurrency industry, obliging digital asset service providers to comply with stricter reporting and monitoring standards.[15]

However, challenges arise when these regulations are not uniformly enforced worldwide. Many developing countries and offshore jurisdictions still lack clear or stringent regulations regarding cryptocurrency transactions, creating safe havens for cybercriminals to hide or launder their illicit gains. Some countries have even become hotspots for Dark Web black markets, where cryptocurrencies are freely

---

13 Benedictus Renny See et al., "Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes," *Journal of Law, Policy and Globalization* 81 (2019): 101–8, https://doi.org/10.7176/JLPG.

14 Lawrence J. Trautman, "Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace," *SSRN Electronic Journal*, May 30, 2018, 1–92, https://doi.org/10.2139/SSRN.3182867.

15 Lars Haffke, Mathias Fromberger, and Patrick Zimmermann, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them," *SSRN Electronic Journal*, February 3, 2019, 1–23, https://doi.org/10.2139/SSRN.3328064.

used without strict oversight from financial authorities. Nations with weak regulations often have minimal financial reporting mechanisms, low levels of coordination with international bodies, and limited law enforcement capacity to tackle illegal digital financial activities.

Additionally, the lack of international coordination in cryptocurrency regulation remains a major obstacle in combating Dark Web crimes. While international efforts such as the Financial Action Task Force (FATF) have established global guidelines on AML and KYC for the cryptocurrency industry, implementation varies significantly between countries. These discrepancies often hinder international cooperation in investigating illicit cryptocurrency-based transactions, as law enforcement in one country may struggle to obtain data from jurisdictions with more lenient regulations. As a result, Dark Web criminals can easily transfer their digital assets to countries with weaker regulations, evade detection, and continue engaging in illicit transactions without significant barriers.

To address jurisdictional challenges and regulatory discrepancies in cryptocurrency governance, international cooperation through cyber law agreements is essential for law enforcement against crimes on the Dark Web. One of the most influential international legal instruments is the Budapest Convention on Cybercrime, designed to facilitate cross-border cooperation in investigating and prosecuting cybercrimes. This convention enables member states to collaborate on information exchange, extradition of criminals, and strengthening digital investigation mechanisms. However, the implementation of this convention still faces challenges, particularly because not all countries have ratified it. Some nations, such as Russia and China, have refused to join due to concerns over Western dominance in decision-making. Therefore, beyond the Budapest Convention, many countries are developing bilateral agreements or regional cooperation frameworks to enhance law enforcement mechanisms against cybercrimes on the Dark Web.

Differences in regulation and law enforcement approaches to crimes on the Dark Web are evident when comparing policies implemented by various countries. The United States, for instance, adopts an aggressive approach through agencies such as the FBI and DEA, which frequently conduct infiltration operations and network monitoring to dismantle illicit marketplaces on the Dark Web. The European Union, through Europol and Interpol, prioritizes multilateral cooperation by sharing intelligence, training law enforcement officers, and strengthening oversight of illegal financial transactions. Meanwhile, in several developing countries, the primary challenges in addressing crimes on the Dark Web stem from a lack of technological infrastructure and weak regulations, which hinder the effectiveness of investigations and enforcement. Therefore, the most effective approach to combating crimes on the Dark Web is a combination of strong national regulations and closer international cooperation, ensuring that transnational cybercrimes can be tackled more effectively and in a coordinated manner.

In the context of regulating crimes on the Dark Web, several legal theories provide an academic foundation for developing a legal system that is responsive to advancements in digital technology. Legal positivism, natural law, utilitarianism, and cyber legal realism serve as the basis for understanding how the law should adapt to cybercrime phenomena.

In the tradition of legal positivism, law is seen as a set of rules established by a legitimate authority and must be enforced regardless of morality or substantive justice. This perspective, pioneered by John Austin and later developed by Hans Kelsen in his *Pure Theory of Law (Reine Rechtslehre)*, asserts that regulations against cybercrimes should be clear, structured, and enforceable. However, the limitation of this approach in addressing Dark Web crimes lies in the fact that legal certainty often lags behind technological developments. For example, many countries still lack explicit regulations governing the misuse of

encryption, cryptocurrency-based illicit trade, and the mechanisms for seizing digital assets used in criminal transactions. As a result, legal positivism demands systematic legal reforms so that law enforcement authorities have the necessary legal instruments to handle cases occurring on the Dark Web effectively. In contrast to legal positivism, natural law theory, as developed by Thomas Aquinas, John Locke, and Hugo Grotius, argues that law must align with moral principles and universal justice. In the context of Dark Web crimes, natural law emphasizes that regulations should prioritize the protection of victims' rights, especially in cases of human trafficking, child sexual exploitation, and the distribution of illegal content that harms individuals and society.

This approach underscores the necessity for legal frameworks that not only focus on punishing offenders but also emphasize victim recovery (restorative justice). Therefore, international regulations such as the Budapest Convention on Cybercrime do not merely focus on prosecuting cybercriminals but also stress the importance of cooperation in safeguarding victims of digital crimes.[16] Utilitarianism, as proposed by Jeremy Bentham and John Stuart Mill, focuses on the creation of laws that maximize benefits for the greatest number of people. In the context of Dark Web crimes, effective regulations should aim to prevent crimes, reduce risks for victims, and enhance the efficiency of law enforcement.

An example of a utilitarian approach to Dark Web regulation is the enforcement of cryptocurrency transaction policies. Several countries have introduced Know Your Customer (KYC) and Anti-Money Laundering (AML) policies to ensure that cryptocurrency transactions remain under the supervision of financial authorities. These

---

16 Filippo Spiezia, "International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime," *ERA Forum* 23, no. 1 (2022): 101–8, https://doi.org/10.1007/s12027-022-00707-8.

regulations are designed to minimize the misuse of digital currencies in illicit Dark Web transactions, ensuring that the overall societal benefits of such laws outweigh potential privacy concerns. Legal realism, as developed by Oliver Wendell Holmes and Karl Llewellyn, argues that law should not be static but must evolve alongside social and technological developments. In the context of Dark Web crimes, legal realism requires that regulations be adaptive, evidence-based, and capable of responding to emerging threats arising from digital advancements. This approach acknowledges that crimes on the Dark Web continuously evolve and cannot be completely eradicated through rigid regulations alone. Therefore, a responsive law approach, as developed by Philip Selznick, is necessary. This concept emphasizes that regulations should be flexible and capable of adjusting to rapid technological changes, allowing legal frameworks to remain effective in addressing new and complex cybercrime challenges.

IV. Challenges in Investigating and Proving Crimes on the Dark Web: Encryption, Anonymity, and Legal Barriers

The investigation of crimes on the Dark Web faces significant challenges, primarily due to the inherent anonymity of its ecosystem. The Dark Web is designed as a digital environment that offers a high level of anonymity for its users, mainly through the use of layered encryption technologies. One of the primary tools enabling this level of anonymity is Tor (The Onion Router), a distributed network designed to conceal users' identities and locations by routing internet traffic through a series of randomly encrypted servers located in different

countries.[17] Each time a user accesses a site on the Dark Web, their data requests pass through three or more relay nodes, which encrypt and redirect the communication, making it difficult to trace by internet service providers (ISPs) or law enforcement authorities. Each node in the Tor network only knows the IP address of the previous and next node but does not have knowledge of the complete communication route. This mechanism creates a layered anonymity system (similar to the structure of an onion), making it nearly impossible for third parties to identify the original source or final destination of the communication.

Unlike the conventional internet, where user IP addresses and communication metadata can be recorded and monitored by internet service providers or legal authorities, the Dark Web actively prevents such tracking techniques through various obfuscation strategies. These techniques work by masking sender and receiver information, randomizing communication routes, and using encrypted protocols that cannot be accessed by standard search engines. For example, most websites on the Dark Web use addresses with the ".onion" extension, which can only be accessed through browsers that support Tor. Additionally, users on the Dark Web often implement extra measures such as VPNs (Virtual Private Networks), peer-to-peer (P2P) networks, or proxy servers to further enhance their anonymity.[18]

The security and anonymity provided by Tor and the Dark Web were initially developed for positive purposes, such as protecting freedom of speech in countries with strict censorship, allowing

---

17 Raghu Raman et al., "Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals," *Heliyon* 9, no. 11 (November 1, 2023): 1–8, https://doi.org/10.1016/J.HELIYON.2023.E22269.

18 Arber S. Beshiri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," *Journal of Computer and Communications* 7, no. 3 (March 4, 2019): 30–43, https://doi.org/10.4236/JCC.2019.73004.

journalists or human rights activists to communicate without fear of surveillance, and supporting users in regions with restricted internet access. However, these features have also been exploited by criminals to evade detection and conduct various illegal activities without being identified. The Dark Web's ability to conceal user identities poses a significant challenge for law enforcement agencies in tracing and apprehending cybercriminals. Although several investigative techniques have been developed, such as network infiltration, digital entrapment (honeypots), and exploiting vulnerabilities in the Tor system, criminals on the Dark Web continuously adapt by strengthening their security protocols.[19] Some criminal groups even use end-to-end encryption (E2EE), multi-hop VPNs, and secure drop points to ensure their transactions remain undetected. This creates difficulties for law enforcement in identifying perpetrators and building legally admissible evidence-based cases.

In addition to anonymity, the use of high-level encryption presents a major challenge in investigating crimes that occur on the Dark Web. Criminals utilize encryption technology not only to protect their communications from law enforcement detection but also to secure the storage and distribution of illegal data. Various types of sensitive information and illicit goods, such as stolen credit card databases, forged identification documents, child sexual exploitation materials, and hacking tools, are often stored in encrypted formats, making them nearly impossible to access without a decryption key. These encryption keys are typically known only to the parties involved in illegal transactions, further complicating efforts to track and prove criminal activities. In some cases, criminals even implement multi-layer encryption or double encryption, combining multiple encryption

---

[19] Matthew Robert Shillito, "Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law," *Information & Communications Technology Law* 28, no. 2 (May 4, 2019): 186–207, https://doi.org/10.1080/13600834.2019.1623449.

algorithms simultaneously, making data decryption increasingly difficult and time-consuming.

Although digital forensic technology has advanced significantly with methods such as cryptanalysis and reverse engineering, law enforcement agencies still face limitations in decrypting information secured with modern encryption systems. Encryption algorithms like AES-256 and RSA-4096, frequently used in criminal activities on the Dark Web, are designed to provide extremely high levels of security. Even with powerful computing resources, the decryption process can take years or may not be feasible within a realistic timeframe. Consequently, in many investigations, law enforcement agencies are forced to rely on techniques such as lawful hacking, where they infiltrate suspects' systems through software exploitation or controlled cyberattacks to gain access to encrypted data. Additionally, methods such as infiltrating criminal networks, social engineering, and monitoring digital transaction activities are used as alternative strategies to access encrypted data without having to decrypt it directly. However, these methods also pose their own challenges, particularly in terms of legality, ethical concerns in investigations, and resource limitations in conducting effective and sustainable cyber operations.

Another challenge in investigating crimes on the Dark Web is the difficulty in collecting, validating, and using digital evidence in court, primarily due to its electronic nature, which makes it easy to manipulate and difficult to verify for authenticity.[20] Evidence in cybercrime cases does not have the physical characteristics of traditional evidence that can be examined using conventional forensic methods. Instead, digital evidence can be easily deleted, altered, or disguised without leaving a tangible trace, especially if perpetrators use encryption technology,

---

[20] Syed Atir Raza, Aqsa Anwar, and Abdul Hannan Khan, "Current Issues and Challenges with Scientific Validation of Digital Evidence," *Review of Computer Engineering Studies* 9, no. 3 (September 30, 2022): 111–15, https://doi.org/10.18280/RCES.090304.

VPNs, or anti-forensic methods designed to evade detection by law enforcement authorities.[21] Additionally, Dark Web marketplaces and criminal forums often have automated systems that delete transaction data and conversations within a certain period, limiting investigators' opportunities to collect necessary information before the evidence disappears permanently.

Legal systems in different countries also have significant variations in the recognition and admissibility of digital evidence, further complicating law enforcement efforts at the international level. In some jurisdictions, courts apply very strict standards for accepting electronic evidence, where aspects such as data authenticity, evidence integrity, and legally valid acquisition methods are key requirements for evidence to be used in trials. If evidence is obtained through unlawful means, such as illegal hacking, unauthorized surveillance, or infiltration methods that violate privacy rights, the evidence may be deemed inadmissible in court. For example, in the United States, the Exclusionary Rule in criminal procedure law prohibits the use of evidence obtained in violation of a defendant's constitutional rights, including breaches of the Fourth Amendment, which protects against unlawful searches and seizures. Meanwhile, in the European Union, the General Data Protection Regulation (GDPR) provides strict protections for individual privacy, meaning that any surveillance or electronic data seizure must go through rigorous legal processes to avoid violating human rights.[22]

---

21 I A Mohammad et al., "Anti-Forensic Challenges in Digital Forensics Investigations: An Overview of Techniques and Tools," in *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 2024, 1–6, https://doi.org/10.1109/ICSPIS63676.2024.10812632.

22 Alexander Wodi, "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review," *SSRN Electronic Journal*, 2023, 1–22, https://doi.org/10.2139/SSRN.4601142.

Beyond legal standards, another challenge in using digital evidence in court is the requirement to prove the validity and continuity of the chain of custody. Electronic evidence must be transparently traceable from the moment it is collected by investigators until it is presented in court, without any indication of modification or tampering by unauthorized parties. In some cases, the defense may argue that the digital evidence submitted in court has been manipulated, edited, or even illegally planted by certain parties, potentially undermining the prosecution's case. As a result, law enforcement agencies worldwide are now developing more advanced digital forensic methods, including the use of hashing technology, digital timestamps, and blockchain-based forensic tools to ensure that each piece of digital evidence maintains strong authenticity and cannot be falsified.

However, despite the continuous advancements in digital forensic technology, challenges in the collection and use of digital evidence remain a major obstacle in investigating crimes on the Dark Web. Without a globally unified legal standard and stronger international coordination, law enforcement agencies will continue to struggle in bringing Dark Web criminals to justice with strong and legally admissible evidence.

The debate over the ethics and legality of cyber investigation methods has become more prominent as the use of hacking techniques and cyber surveillance by law enforcement increases. Some law enforcement agencies have employed techniques such as government malware, zero-day exploits, and remote access trojans (RATs) to covertly access suspects' devices and collect evidence.[23] However, the use of these methods raises significant legal and ethical dilemmas, as they may violate individual privacy rights and legal principles that protect civil

---

[23] Hardik Vyas, "Fully Undetectable Remote Access Trojan: Windows," *International Journal for Research in Applied Science and Engineering Technology* 7, no. 5 (2019): 1886–90, https://doi.org/10.22214/ijraset.2019.5316.

liberties. On the one hand, these methods are effective in dismantling criminal networks on the Dark Web, but on the other hand, there is a risk of abuse by governments or intelligence agencies for unauthorized purposes. Some countries have restricted the use of lawful hacking by requiring strict court orders before conducting digital interventions, while others have developed more flexible regulations to accommodate the needs of cyber investigations.

As criminals on the Dark Web continue to adopt increasingly sophisticated technology, law enforcement agencies must develop investigative strategies that strike a balance between effective law enforcement and human rights protection. International collaboration in intelligence sharing, capacity building in digital forensics, and legal reforms on digital evidence collection and use are crucial steps in addressing the challenges of Dark Web investigations. Without a comprehensive approach, Dark Web crimes will continue to evolve, exploiting legal loopholes and technological advancements to evade detection and law enforcement.

V. Law Enforcement Strategies Against Dark Web Crimes: Regulatory Reform and Strengthening International Cooperation

Enforcing the law against crimes on the Dark Web requires a more adaptive and collaborative strategy due to the complexity and technological challenges involved. One of the main steps in strengthening efforts to combat crime on the Dark Web is enhancing cybercrime regulations that criminalize illegal activities occurring within the Dark Web and improving law enforcement mechanisms to be more responsive to digital technology developments. Several countries have updated their laws to cover advanced technology-based crimes,

including the misuse of encryption, the spread of malware, and the trade of illegal goods and services through the Dark Web. However, legal gaps still exist, allowing criminals to exploit jurisdictions with more lenient regulations to evade detection and prosecution.[24]

Beyond strengthening national regulations, the harmonization of international laws is a crucial element in addressing Dark Web crimes, which often transcend national borders. Cybercrimes do not recognize geographical limitations, and differing legal approaches among countries frequently hinder the effectiveness of global law enforcement efforts. Some nations enforce stricter regulations on cybercrime, while others still have legal gaps that criminals can exploit to avoid prosecution. Differences in crime definitions, investigative mechanisms, and extradition procedures often impede law enforcement agencies' ability to take action against Dark Web criminals, particularly when they operate from countries that lack legal cooperation agreements with the jurisdictions where the crimes occur.

To address these challenges, international agreements such as the Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, play a vital role in establishing global standards for cybercrime regulation.[25] This convention is the first international legal framework specifically designed to regulate various aspects of cybercrime law enforcement, including mechanisms for international cooperation in digital investigations, electronic evidence seizure, and extradition procedures for cybercriminals. Furthermore, the convention encourages its member states to adopt domestic regulations aligned with

---

24 Faisal Shaikh, "The Dark Web: Challenges and Countermeasures in Combating Cybercrime," *International Journal for Research in Applied Science and Engineering Technology* 12, no. 3 (2024): 636–43, https://doi.org/10.22214/ijraset.2024.58892.

25 Enver Buçaj and Kenan Idrizaj, "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention," *Multidisciplinary Reviews* 8, no. 1 (January 1, 2025): 2025024–2025024, https://doi.org/10.31893/MULTIREV.2025024.

international standards to combat various forms of crime on the Dark Web, such as illegal trade, cyberattacks, child exploitation, and cryptocurrency-based money laundering.

However, despite the Budapest Convention being a global standard for cyber law enforcement, its implementation still faces significant challenges, particularly because not all countries have ratified it. Some nations, such as Russia and China, refuse to join the convention due to concerns over Western dominance in cyber law enforcement and the potential misuse of data exchanges and extradition requests. These countries prefer to develop their own cyber regulations or establish bilateral and regional agreements that they consider more aligned with their national interests. Consequently, gaps in international legal cooperation remain, allowing Dark Web criminals to take refuge in jurisdictions without extradition treaties or strict cyber regulations, enabling them to operate illegal activities without fear of arrest.

In response to these challenges, international organizations such as INTERPOL and Europol have taken a more active role in strengthening global coordination in combating Dark Web crimes. They have established specialized task forces focused on cybercrime investigations and intelligence sharing with countries lacking the technological capacity to tackle cybercrime independently. For instance, Europol's European Cybercrime Centre (EC3) has conducted major operations, such as Operation DisrupTor, which resulted in the arrest of hundreds of individuals across multiple countries involved in drug trafficking and illegal goods trade on the Dark Web. Additionally, INTERPOL has developed the Cyber Fusion Centre, serving as a platform for various countries to share information, develop new investigative techniques, and train law enforcement officials to combat increasingly complex cyber threats.

Strengthening international cooperation in law enforcement and digital investigations is crucial in eradicating Dark Web crimes, given

their transnational and anonymous nature. Crimes committed on the Dark Web often extend beyond a single national jurisdiction, involving criminal networks operating across multiple countries. In many cases, servers hosting illegal activities are located in one country, while the criminals themselves operate from another, and victims are dispersed worldwide. This network structure presents challenges for investigation and prosecution, as each country has different legal systems, investigative procedures, and regulatory standards for handling cybercrime. Therefore, a more robust mechanism for international coordination among law enforcement authorities is necessary to ensure that investigations into Dark Web crimes can be conducted more effectively.

One of the global cooperation models that has been implemented is Mutual Legal Assistance Treaties (MLATs), a legal mechanism that allows countries to exchange information and electronic evidence for the investigation and prosecution of transnational crimes.[26] Through MLATs, law enforcement agencies in one country can submit formal requests to another country to gain access to electronic data, seize digital assets, or arrest suspects residing within a foreign jurisdiction.[27] However, MLATs still have limitations, particularly in terms of slow bureaucratic procedures, legal differences between countries, and a lack of transparency in sharing sensitive data between authorities. In many cases, the speed of investigation is crucial, especially since digital evidence on the Dark Web can be deleted or encrypted within hours.

---

[26] Andrew Keane Woods, "Mutual Legal Assistance in the Digital Age," in *The Cambridge Handbook of Surveillance Law*, ed. David Gray and Stephen E Henderson, Cambridge Law Handbooks (Cambridge: Cambridge University Press, 2017), 659–76, https://doi.org/DOI: 10.1017/9781316481127.029.

[27] I Nyoman Sindhu Gautama, "Pemberatasan Kejahatan Internasional Berdasarkan Mutual Legal Assistance Treaties (MLATs)," *Jurnal Aktual Justice* 4, no. 1 (June 10, 2019): 54–65, https://doi.org/10.47329/AKTUALJUSTICE.V4I1.474.

Therefore, the lengthy MLAT procedures often hinder the effectiveness of investigations.[28]

As a solution to the limitations of MLATs, several countries and international organizations have established Joint Cybercrime Task Forces, which enable the integration of resources, technology, and law enforcement expertise from multiple countries to handle more complex cybercrimes. One example of successful cooperation is Europol's European Cybercrime Centre (EC3), which has played a crucial role in dismantling illegal trade networks on the Dark Web, including major operations such as Operation DisrupTor and the takedown of AlphaBay and Hansa Market. Additionally, INTERPOL's Cybercrime Directorate has developed various training programs and intelligence-sharing initiatives to assist countries with lower technological capacity in tackling cybercrime. Such collaborations not only enhance the effectiveness of investigations but also allow countries to align legal standards and procedures in handling digital evidence and prosecuting criminals operating on the Dark Web.

With the rapid development of digital technology, the criminal evidence system must be continuously updated to address emerging challenges in law enforcement against Dark Web crimes. Unlike physical evidence, which is relatively easy to identify, classify, and present as admissible proof in court, digital evidence is often volatile, susceptible to manipulation, and difficult to verify for authenticity. Therefore, legal systems in various countries must adapt standard procedures in digital forensics to ensure that electronic evidence is admissible and legally valid in criminal proceedings.

One of the primary challenges in criminal evidence related to Dark Web crimes is the validity and authenticity of digital evidence.

---

[28] Shambhavi Sharma, "Issues with Enforcing Mutual Legal Assistance Treaties (MLATs): Access to Cross-Border Data in Criminal Investigation," *SSRN Electronic Journal*, November 29, 2020, 1–15, https://doi.org/10.2139/SSRN.3815270.

Evidence obtained from cyber investigations must meet the principles of integrity, authenticity, and reliability to be used to build a case against suspects without raising doubts in legal proceedings. In many cases, law enforcement agencies face difficulties in proving that the submitted evidence has not been modified or altered since it was first collected. To address this challenge, many countries have adopted new standards in digital forensics, such as ISO/IEC 27037, which regulates the identification, collection, acquisition, and preservation of digital evidence to ensure its validity and maintain the chain of custody required in court proceedings.[29]

Moreover, technological advancements have enabled the use of more sophisticated digital forensic methods in investigating Dark Web crimes. One emerging technology is blockchain analytics, which allows law enforcement agencies to trace cryptocurrency transactions used in illegal activities. Since transactions on blockchain are decentralized and transparent, investigators can use forensic blockchain algorithms to identify suspicious transaction patterns, track digital wallet addresses linked to criminal activities, and uncover connections between Dark Web criminals. Several law enforcement agencies, such as Europol and the FBI, have partnered with blockchain analysis firms like Chainalysis and Elliptic to support financial crime investigations involving cryptocurrencies.[30]

In addition to blockchain analytics, machine learning and artificial intelligence (AI) technologies are increasingly being used to

---

29 A Ajijola, P Zavarsky, and R Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012," in *World Congress on Internet Security (WorldCIS-2014)*, 2014, 66–73, https://doi.org/10.1109/WorldCIS.2014.7028169.

30 Hiroki Kuzuno and Giannis Tziakouris, "Ad-Hoc Analytical Framework of Bitcoin Investigations for Law Enforcement," *IEICE Transactions on Information and Systems*, no. 11 (November 1, 2018): 2644–57, https://doi.org/10.1587/TRANSINF.2017ICP0007.

detect criminal patterns on the Dark Web. By leveraging algorithms that can analyze communication patterns, transactions, and user activities, investigators can identify indicators of illegal activities more quickly and accurately. These technologies enable systems to scan thousands of forums, marketplaces, and encrypted communications to detect suspicious activities, such as the sale of stolen data, drug trafficking, or other illicit transactions. Consequently, law enforcement agencies can obtain more accurate and data-driven intelligence to support investigations and enforcement against Dark Web crimes.

Regulation of cryptocurrency use is becoming an increasingly important aspect of law enforcement strategies against Dark Web crimes, given that digital currencies have become the primary means of transaction within this ecosystem. Cryptocurrencies such as Bitcoin, Monero, and Ethereum are widely used for drug trafficking, child exploitation, weapons trade, money laundering, and hacking services due to their anonymity, decentralization, and difficulty in being traced by financial authorities and law enforcement. Unlike traditional financial transactions, which are monitored by banks or financial institutions, cryptocurrency transactions operate on blockchain, a system that enables asset exchanges without intermediaries or direct regulatory oversight.

To address this challenge, several countries have implemented stricter regulations on cryptocurrency transactions, particularly by introducing Know Your Customer (KYC) and Anti-Money Laundering (AML) policies, which require digital currency exchanges to identify and report suspicious activities. In the United States, for example, the Financial Crimes Enforcement Network (FinCEN) has mandated that all crypto service providers comply with the same financial regulations as traditional financial institutions, including verifying user identities, reporting suspicious transactions, and preventing money laundering associated with Dark Web crimes. Similarly, the European Union has adopted the Fifth Anti-Money Laundering Directive (5AMLD), which

extends AML and KYC obligations to the cryptocurrency industry to enhance transparency and reduce the risk of digital assets being exploited for criminal activities.

However, in strengthening law enforcement efforts, the balance between public security and the protection of individual privacy rights must still be considered. Increased monitoring of online activities, including the use of cyber surveillance techniques and lawful hacking by law enforcement agencies, has sparked debates over the boundaries between privacy rights and security needs. Some countries have implemented more transparent oversight mechanisms, such as requiring court authorization before monitoring specific individuals, to ensure that law enforcement actions do not violate human rights. Additionally, strengthening oversight and accountability mechanisms for law enforcement agencies is crucial to prevent abuse of power in efforts to combat Dark Web crimes.

With the increasing complexity of crimes on the Dark Web, effective law enforcement strategies must integrate regulatory reforms, international cooperation, digital forensic technology, and the protection of individual privacy rights. Without a comprehensive and adaptive approach, efforts to combat Dark Web crimes will continue to face significant challenges, while criminals will develop increasingly sophisticated methods to evade detection and prosecution.

Indonesia can learn from global experiences in tackling Dark Web crimes by strengthening regulations, enhancing international cooperation, and developing digital forensic and investigative capacities. The growing complexity of crimes on the Dark Web demands a more adaptive legal approach, particularly in monitoring cryptocurrency transactions, cyber investigations, and law enforcement against illicit activities based on digital anonymity. Developed countries have implemented stricter policies in monitoring the Dark Web ecosystem, and Indonesia needs to adopt proven best practices in dismantling digital criminal networks.

One crucial aspect that needs to be strengthened is the reform of cybercriminal laws, including the criminalization of illegal activities on the Dark Web and strict supervision of cryptocurrency transactions. Countries such as the United States and the European Union have implemented Know Your Customer (KYC) and Anti-Money Laundering (AML) measures to ensure that cryptocurrency transactions are not used for drug trafficking, child exploitation, or money laundering. Indonesia can adopt similar regulations by tightening oversight of crypto exchange platforms, increasing transparency in digital transactions, and imposing sanctions on service providers that fail to comply with global financial compliance standards.

In addition to regulations, international cooperation is key to addressing cross-border cybercrimes. Dark Web crimes do not recognize geographical boundaries, so Indonesia must strengthen collaboration with INTERPOL, the ASEAN Cyber Security Centre, Europol, and other international law enforcement agencies to exchange intelligence, expedite the extradition of perpetrators, and align cyber investigation policies. Global experiences indicate that international agreements such as the Budapest Convention on Cybercrime can be crucial instruments in enhancing legal coordination between countries. Moreover, Mutual Legal Assistance Treaties (MLATs) must be improved to ensure that Dark Web crime investigations can be more effective and not hindered by jurisdictional differences.

Indonesia must also enhance its digital investigation and cyber forensic capabilities to better track activities on the Dark Web. Countries like the United States, the United Kingdom, and Germany have used blockchain analytics, artificial intelligence (AI), and machine learning to track illegal transactions and identify cybercrime patterns. Indonesia needs to develop a national cyber forensic center with cutting-edge technological support and train law enforcement officers to utilize advanced digital investigative tools. The ability to analyze digital evidence, bypass encryption systems, and infiltrate criminal networks

must be improved so that law enforcement in Indonesia can be more responsive to the threats posed by Dark Web crimes.

Alongside technological capacity improvements, Indonesia must also balance cyber law enforcement with privacy protection. The use of surveillance technologies such as lawful hacking and cyber surveillance must be conducted transparently and with judicial approval to avoid human rights violations. Some countries have adopted regulations ensuring that cyber investigations are not misused for political or authoritarian purposes, and Indonesia should consider implementing similar safeguards to regulate the limits and oversight mechanisms for law enforcement in digital investigations.

In conclusion, Indonesia must adopt a comprehensive and adaptive strategy to tackle Dark Web crimes. Cybercriminal law reforms, strengthened international cooperation, enhanced digital investigation capabilities, and a balance between cybersecurity and privacy rights should be priorities in developing a more resilient legal system against cybercrime threats. Without serious and coordinated efforts, Dark Web crimes will continue to evolve, exploiting legal loopholes and technological advancements to evade detection and prosecution.

VI. Conclusion

This study highlights the legal challenges in tackling crimes on the Dark Web, which continue to grow alongside digital advancements. The Dark Web is a hub for illegal activities such as drug trafficking, child exploitation, data theft, and cyberattacks. Its high level of anonymity, strong encryption, and cryptocurrency-based transactions make it difficult for law enforcement to track and prosecute offenders. A major challenge is the anonymity provided by technologies like Tor and I2P, allowing criminals to hide their identities and locations. Strong encryption further complicates investigations, making it difficult to

access digital evidence. Additionally, jurisdictional issues create obstacles, as cybercrimes on the Dark Web cross national borders, while legal systems vary, slowing down international cooperation and prosecution. Cryptocurrency regulations also remain a challenge. Digital currencies like Bitcoin and Monero are widely used for illegal transactions due to their untraceable nature. Some countries have introduced Know Your Customer (KYC) and Anti-Money Laundering (AML) rules, but inconsistent enforcement worldwide leaves loopholes for criminals to exploit. To address these issues, international cooperation is essential. Agreements like the Budapest Convention on Cybercrime and joint operations by Europol and INTERPOL, such as Operation DisrupTor, have helped dismantle criminal networks. Strengthening digital forensics with blockchain analytics, artificial intelligence (AI), and machine learning is also crucial for tracking illegal transactions and identifying cybercriminals. However, law enforcement must balance security with privacy protection. Techniques like lawful hacking and cyber surveillance can aid investigations but also raise ethical concerns. Clear regulations and oversight are needed to ensure these methods respect human rights. Fighting Dark Web crimes requires stronger cyber laws, international cooperation, advanced forensic technology, and a balance between law enforcement and privacy. Without coordinated efforts, Dark Web criminals will continue to exploit legal and technological gaps to evade justice.

VII. References

Abdel Samad, Yara. "Case Study: Dark Web Markets." In *Dark Web Investigation*, edited by Babak Akhgar, Marco Gercke, Stefanos Vrochidis, and Helen Gibson, 237–47. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-55343-2_11.

Ajijola, A, P Zavarsky, and R Ruhl. "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012." In *World Congress on Internet Security (WorldCIS-2014)*, 66–73, 2014. https://doi.org/10.1109/WorldCIS.2014.7028169.

Andrei, Filippo, and Giuseppe Alessandro Veltri. "Status Spill-Over in Cryptomarket for Illegal Goods." *Social Science Computer Review*, September 21, 2024, 08944393241286339. https://doi.org/10.1177/08944393241286339.

Arber S. Beshiri. "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." *Journal of Computer and Communications* 7, no. 3 (March 4, 2019): 30–43. https://doi.org/10.4236/JCC.2019.73004.

Bidv, Vijaykumar, and Aishwarya Suryakant Waghmare. "Beyond the Onion Routing: Unmasking Illicit Activities on the Dark Web." *International Journal of Innovative Science and Research Technology (IJISRT)*, June 10, 2024, 2419–40. https://doi.org/10.38124/IJISRT/IJISRT24MAY1698.

Bradley, C, and G Stringhini. "A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets." In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 453–63, 2019. https://doi.org/10.1109/EuroSPW.2019.00057.

Buçaj, Enver, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention." *Multidisciplinary Reviews* 8, no. 1 (January 1, 2025): 2025024–2025024. https://doi.org/10.31893/MULTIREV.2025024.

Fernando, Zico Junius, Kiki Kristanto, and Ariesta Wibisono Anditya.

"Knitting Democracy, Separating Restraints: Legal Reform and a Critical Analysis of Article 256 of the New Criminal Code and Its Impact on Freedom of Speech." *Journal of Law and Legal Reform* 5, no. 2 (April 30, 2024): 555–86. https://doi.org/10.15294/JLLR.VOL5I2.1670.

Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņš. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" *SSRN Electronic Journal*, December 14, 2018. https://doi.org/10.2139/SSRN.3102645.

Gautama, I Nyoman Sindhu. "Pemberatasan Kejahatan Internasional Berdasarkan Mutual Legal Assistance Treaties (MLATs)." *Jurnal Aktual Justice* 4, no. 1 (June 10, 2019): 54–65. https://doi.org/10.47329/AKTUALJUSTICE.V4I1.474.

Haffke, Lars, Mathias Fromberger, and Patrick Zimmermann. "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them." *SSRN Electronic Journal*, February 3, 2019, 1–23. https://doi.org/10.2139/SSRN.3328064.

Kuzuno, Hiroki, and Giannis Tziakouris. "Ad-Hoc Analytical Framework of Bitcoin Investigations for Law Enforcement." *IEICE Transactions on Information and Systems*, no. 11 (November 1, 2018): 2644–57. https://doi.org/10.1587/TRANSINF.2017ICP0007.

Martin, James. "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket.'" *Criminology & Criminal Justice* 14, no. 3 (October 7, 2013): 351–67. https://doi.org/10.1177/1748895813505234.

Merrit Kennedy. "More Than 300 Arrested In Child Porn Site Bust : NPR." https://www.npr.org, 2019.

https://www.npr.org/2019/10/16/770628069/one-of-the-worst-forms-of-evil-more-than-330-arrested-in-child-porn-site-bust.

Mohammad, I A, A O Nasar, M Alkhawaldeh, E -U. -H. Qazi, and T Zia. "Anti-Forensic Challenges in Digital Forensics Investigations: An Overview of Techniques and Tools." In *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 1–6, 2024. https://doi.org/10.1109/ICSPIS63676.2024.10812632.

Nicole Sganga et al. "Russia Arrests 14 Alleged Members of REvil Ransomware Gang." https://www.cbsnews.com, 2022. https://www.cbsnews.com/news/ransomware-russia-arrests-revil/.

Putra, Panca Sarjana, Zico Junius Fernando, Bhanu Prakash Nunna, and Rizaldy Anggriawan. "Judicial Transformation: Integration of AI Judges in Innovating Indonesia's Criminal Justice System." *Kosmik Hukum* 23, no. 3 (August 15, 2023): 233–43. https://doi.org/10.30595/KOSMIKHUKUM.V23I3.18711.

Raman, Raghu, Vinith Kumar Nair, Prema Nedungadi, Indrakshi Ray, and Krishnashree Achuthan. "Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals." *Heliyon* 9, no. 11 (November 1, 2023): 1–8. https://doi.org/10.1016/J.HELIYON.2023.E22269.

Raza, Syed Atir, Aqsa Anwar, and Abdul Hannan Khan. "Current Issues and Challenges with Scientific Validation of Digital Evidence." *Review of Computer Engineering Studies* 9, no. 3 (September 30, 2022): 111–15. https://doi.org/10.18280/RCES.090304.

See, Benedictus Renny, Ahmadi Miru Ahmadi Miru, Muhadar, and Hasbir Paserangi. "Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes." *Journal of Law, Policy and Globalization* 81

(2019): 101–8. https://doi.org/10.7176/JLPG.

Shaikh, Faisal. "The Dark Web: Challenges and Countermeasures in Combating Cybercrime." *International Journal for Research in Applied Science and Engineering Technology* 12, no. 3 (2024): 636–43. https://doi.org/10.22214/ijraset.2024.58892.

Sharma, Shambhavi. "Issues with Enforcing Mutual Legal Assistance Treaties (MLATs): Access to Cross-Border Data in Criminal Investigation." *SSRN Electronic Journal*, November 29, 2020, 1–15. https://doi.org/10.2139/SSRN.3815270.

Shillito, Matthew Robert. "Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law." *Information & Communications Technology Law* 28, no. 2 (May 4, 2019): 186–207. https://doi.org/10.1080/13600834.2019.1623449.

Soliman, Mostafa. "Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework." *SSRN Electronic Journal*, April 14, 2023, 1–7. https://doi.org/10.2139/SSRN.4418508.

Spiezia, Filippo. "International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime." *ERA Forum* 23, no. 1 (2022): 101–8. https://doi.org/10.1007/s12027-022-00707-8.

Trautman, Lawrence J. "Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace." *SSRN Electronic Journal*, May 30, 2018, 1–92. https://doi.org/10.2139/SSRN.3182867.

Vyas, Hardik. "Fully Undetectable Remote Access Trojan: Windows." *International Journal for Research in Applied Science and Engineering Technology* 7, no. 5 (2019): 1886–90. https://doi.org/10.22214/ijraset.2019.5316.

Warren, Ian, Monique Mann, and Adam Molnar. "Lawful Illegality: Authorizing Extraterritorial Police Surveillance." *Surveillance & Society* 18, no. 3 (August 19, 2020): 357–69. https://doi.org/10.24908/ss.v18i3.12795.

Wodi, Alexander. "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review." *SSRN Electronic Journal*, 2023, 1–22. https://doi.org/10.2139/SSRN.4601142.

Woods, Andrew Keane. "Mutual Legal Assistance in the Digital Age." In *The Cambridge Handbook of Surveillance Law*, edited by David Gray and Stephen E Henderson, 659–76. Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316481127.029.

***

Acknowledgment

With the deepest sense of gratitude and humility, we extend our sincere appreciation to all individuals and institutions who have generously contributed their time, expertise, and unwavering support throughout the entire process of preparing this article. Your invaluable assistance, insightful feedback, and encouragement have played a crucial role in shaping and refining this work, and for that, we are truly grateful.

Funding Information

None

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

We, the authors, hereby declare that this work is original and has not been published in any form or medium, nor is it under consideration for publication in any other journal. We also affirm that all sources cited in this work adhere to the fundamental standards of scientific citation, ensuring proper acknowledgment of the original authors and contributions. We are committed to upholding the highest standards of ethical conduct in the preparation, submission, and dissemination of this research.