International Asia Of Law and Money Laundering
Vol. 4 No.4 December 2025
https://doi.org/10.59712/iaml.v4i4.149

P-ISSN 2829-1654
E-ISSN 2829-517X

International Asia Of Law and Money Laundering

Analysis of Fraud in Cybercrime Perspective

Tengku Erwinsyahbana[1*], Guntur Rambey[2]
Fakultas Hukum, Universitas Muhammadiyah Sumatera Utara, Indonesia
: *tengkuerwins@umsu.ac.id*
Coresponding Author*

ARTICLE INFO

Keywords:
Cybercrime,
Digital Technology,
Fraud.

Date received : 13 Oktober 2025
Revision date : 06 Nov 2025
Date received : 26 Des 2025

ABSTRACT

The development of digital technology has transformed the landscape of conventional fraud crimes into more complex and sophisticated cybercrime crimes. This study analyzes the characteristics, modus operandi, legal arrangements, and obstacles to law enforcement against fraud in the perspective of cybercrime in Indonesia. Using a normative juridical approach, this study examines primary and secondary legal materials relevant to digital technology-based fraud crimes. The results showed that cyber fraud has distinctive characteristics such as the nature without geographical boundaries, the anonymity of the perpetrators, and the use of information technology as the main means of crime. The growing Modus operandi includes phishing, social engineering, electronic transaction fraud, digital identity theft, to cryptocurrency investment fraud. Regulation of Indonesian criminal law through Article 378 of the Criminal Code and Law No. 19 of 2016 on information and electronic transactions has provided a juridical foundation, but there is still a gap between the dynamics of technology and regulatory readiness. The main obstacles faced include the limited competence of the apparatus in digital forensics, the lack of valid electronic evidence, and the complexity of handling cross-jurisdictional cases. Optimizing handling requires increasing the capacity of law enforcement officers, harmonizing regulations, strengthening international cooperation, and improving digital literacy in a comprehensive and sustainable manner.

P-ISSN 2829-1654
E-ISSN 2829-517X

INTRODUCTION

The development of digital technology has changed the landscape of conventional crime into a more complex and sophisticated form of crime, especially in the context of fraud which is now metamorphosed into the realm of cybercrime. Massive digital transformation has created a new space for criminals to launch fraud through various information technology-based modus operandi, ranging from phishing, online fraud, to digital data manipulation that harms victims materially and immaterially .

This phenomenon is increasingly worrying given the uneven level of digital literacy in society, thus creating vulnerability gaps that cybercriminals use to trick victims with increasingly sophisticated fraud schemes . The complexity of handling fraud in the perspective of cybercrime requires a deep understanding of the characteristics of cybercrime that is transnational, without geographical boundaries, and leaves a digital footprint that requires special expertise in the process of Investigation and legal proof . The urgency of this study arises from the need to comprehensively analyze how the Indonesian criminal law, especially the information and Electronic Transaction Law, is able to accommodate the development of digital fraud modes as well as the effectiveness of law enforcement in the rapidly evolving digital era .

Based on the background that has been described, this study focuses on three main problems. First, What are the characteristics and modus operandi of criminal acts of fraud in the perspective of cybercrime that develops in Indonesia? Second, How is the regulation of Indonesian criminal law in dealing with digital technology-based fraud? Third, What are the obstacles and challenges in law enforcement against perpetrators of cybercrime fraud and how are efforts to optimize handling?.

This study aims to analyze in depth the characteristics of criminal acts of fraud in the context of cybercrime, reviewing the Indonesian criminal law framework in regulating and dealing with digital fraud crimes, as well as identifying various obstacles in the law enforcement process as well as formulating strategic solutions to improve the effectiveness of handling criminal acts of fraud based on information technology. The theoretical benefit of this study is to contribute to the development of criminal law, especially in the realm of cyber law and enrich academic literature on fraud in the digital age.

In practical terms, this research is expected to be a consideration for law enforcement officers in dealing with cybercrime fraud cases, providing input to policy makers to improve regulations related to cybercrime, as well as increasing public awareness about digital fraud modes and prevention efforts.

METHOD

This study uses a normative juridical approach that examines criminal acts of fraud in the perspective of cybercrime through in-depth analysis of primary and secondary legal materials. The normative approach was chosen because this study focuses on the assessment of legal norms, legal principles, and doctrines related to digital technology-based fraud crimes in the Indonesian criminal law system . Primary legal materials used include the Criminal Code, Law No. 19 of 2016 on amendments to Law No. 11 of 2008 on information and electronic transactions, as well as other relevant laws and regulations governing cybercrime. Secondary legal materials include scientific journals, criminal law textbooks, the results of previous research, and academic literature relevant to the research topic . Data collection techniques are carried out through library studies (library research) by identifying, classifying, and analyzing various legal sources related to research problems. Data analysis using qualitative methods with descriptive-analytical approach, which describes the legal facts and then analyze them critically using theories of criminal law and cyber law. The analysis process is carried out systematically to find answers to established problem formulations using deduction logic and comprehensive interpretation of laws.

RESULTS AND DISCUSSION

The criminal act of fraud in the perspective of cybercrime has unique characteristics that distinguish it from conventional crime. The most prominent nature of cybercrime is borderless or without geographical boundaries, allowing perpetrators who are outside the jurisdiction of Indonesia to still be able to reach victims in the country through the internet network . Anonymous characteristics become the second crucial aspect, where perpetrators can hide their true identity through the use of fake accounts, virtual private Networks (VPNs), and fictitious digital identities that complicate the identification and arrest process by law enforcement officers. The use of digital technology as the main means of crime makes the perpetrator not need to deal directly with the victim, in contrast to conventional fraud which is generally carried out face to face.

P-ISSN 2829-1654
E-ISSN 2829-517X

The elements of the criminal act of fraud in the digital context still refer to Article 378 of the Criminal Code which requires the existence of intent to benefit oneself or others unlawfully, using a false name or false dignity, deception, or a series of lies to move others to hand over goods. The development of digital technology has given rise to a new complex mode of fraud crime and requires an in-depth evaluation of the relevance of Article 378 of the Criminal Code as the legal basis for action . In the digital space, the element of "gimmick" is realized through the manipulation of electronic information, the creation of false websites, misleading emails, or fictitious online applications designed to trick victims.

The difference between conventional fraud and cybercrime fraud lies in three aspects: the medium of execution, the means of evidence, and the reach. Conventional fraud is carried out face-to-face with evidence in the form of witness statements and physical documents, while cybercrime utilizes electronic transactions with electronic information evidence that is recognized as valid through Article 5 Paragraph (1) of law no. 19 of 2016. The recognition of electronic evidence marks the expansion of the proof system in Indonesian criminal law that accommodates the development of digital technology.

Phishing and social engineering became the dominant mode that utilizes psychological manipulation techniques to obtain victims ' sensitive data such as OTP codes, pins, or passwords through sending fake messages that resemble official institutions. The rapid flow of technology has a significant impact on the growth of phishing crimes that no longer rest on one pattern, but are present in a variety of motives and increasingly sophisticated methods . Social engineering techniques target the psychological aspects of the victim by creating an urgent situation so that the victim unknowingly gives up his personal information.

Electronic transaction fraud or online fraud is rife in marketplace and e-commerce platforms, where the perpetrator offers fictitious goods, asks for a transfer of funds, but the goods are never sent. The regulation of the Indonesian criminal law against online buying and selling fraud crimes is contained in Article 28 paragraph (1) of the ITE Law with sanctions under Article 45A paragraph (1) in the form of a maximum imprisonment of 6 years and/or a fine of Rp1, 000, 000, 000.00 (Pramesti & Rosnawati, 2023). Digital identity theft (identity theft) is done by taking the victim's personal data without permission, then used for illegal transactions.

This mode violates Article 26 paragraph (1) of the ITE Law which states that the use of personal data information must be with the consent of the person concerned. Online and cryptocurrency investment scams thrive on digital ponzi schemes that offer high returns with no apparent basis of legality, attracting victims through social media promotions and fake testimonials. Scams through social media and marketplace applications include impersonation mode, fake job offers, to romance scam. The phenomenon of online ticket fraud via WhatsApp poses significant financial losses, with National Cyber and Cipher Agency data showing 1,216 cybercrime complaints in 2023.

Material losses include the loss of funds, digital assets, and economically valuable personal data. Research shows the total reported financial losses reached IDR 1.4 trillion, while immaterial losses included psychological trauma, insecurity, and reputational damage . The social impact is in the form of declining public confidence in electronic transactions and digital payment systems which have implications for slowing national digital economic growth. Psychologically, the victim experiences prolonged mental stress, feelings of shame, and even depression due to the loss of financial assets. Implications of the digital economy include decreased public participation in online transactions, reduced investment in the financial technology sector, and increased security costs that digital businesses must incur to protect consumers from fraud threats.

The provisions of the criminal code on fraud are regulated in Article 378 which regulates the elements of fraud in general, including the intention to benefit oneself, using deception, and moving others to hand over goods. While it can be applied to digital fraud through broad interpretation, there are significant challenges such as the anonymity of perpetrators and across jurisdictions. The ITE Law and its amendments provide for specific regulation of cybercrime. Act No. 11 of 2008 as amended by law No. 19 of 2016 regulates Article 28 paragraph (1) on the spread of false news in electronic transactions, Article 30 on illegal access, and Article 35 on data manipulation. Other complementary regulations include regulations related to consumer protection and technical regulations for the implementation of electronic systems that support the enforcement of cybercrime laws.

The objective element includes the act of disseminating false information, accessing without rights, or manipulating electronic data, while the subjective element includes intentional (dolus) and without rights as stated in the phrase "intentionally and without rights" in Articles 27, 28, 30, and 35 of the ITE Law. Evidence in cases of cybercrime fraud relies on digital evidence in accordance with Article 5

P-ISSN 2829-1654
E-ISSN 2829-517X

Paragraph (1) of the ITE Law which recognizes electronic information and electronic documents as valid evidence (Pramesti & Rosnawati, 2023). The validity of the electronic system must meet the requirements to maintain the integrity and authenticity of the data as stipulated in law no. 11 of 2008. Criminal sanctions are regulated in Chapter XI of the ITE Law, with threats varying depending on the type of offense. Article 45A paragraph (1) threatens a maximum prison sentence of 6 years and/or a fine of Rp1, 000, 000, 000.00 for violation of Article 28 paragraph (1), showing the seriousness of the government's handling of digital fraud crimes.

extraterritorial jurisdiction through Article 2 of the ITE Law which allows the prosecution of perpetrators outside Indonesia . But its shortcomings lie in the potential for multi-interpretation of some norms and the limitations of the technical regulation of cryptocurrency-based crime and artificial intelligence. Legal gaps are still found in aspects of personal data protection and effective cross-border enforcement mechanisms. Supporting regulations such as the development of RKUHP play a role in expanding legal protection, but policy updates are needed to address legal gaps. Comparison with other countries 'regulations such as the United States' Computer Fraud and Abuse Act or the European Union's Budapest Convention on Cybercrime shows that Indonesia still needs to strengthen comprehensive international cooperation instruments to deal with cross-border cybercrime.

The limited competence of law enforcement officers in digital forensics is a major obstacle, where not all investigators have the technical expertise to track digital traces and secure electronic evidence . The difficulty of tracking digital footprints across countries is a significant obstacle even though Article 2 of the ITE Law provides the basis for extraterritorial jurisdiction, as it requires complex bilateral cooperation. The lack of valid digital evidence often occurs due to the victim's misunderstanding in securing electronic evidence or data damage due to the seizure process that is not in accordance with digital forensic procedures. Technical and administrative barriers include limited digital forensic laboratory infrastructure and lengthy bureaucracy in the process of handling cases across regions.

The development of technology is very fast causing regulation is often left behind and the crime mode continues to innovate utilizing the latest technology. The lack of legal awareness of the community makes it easy for victims to be trapped in social engineering mode, with low digital literacy being a crucial factor in the increasing number of victims of online fraud. Coordination between law enforcement agencies is often constrained by overlapping authorities and differences in handling procedures between the police, prosecutors, and Related Agencies. Jurisdiction and international cooperation are structural challenges given that perpetrators are often abroad and require an effective extradition mechanism and mutual legal assistance.

Increasing the capacity of law enforcement officers through intensive digital forensic training and international competency certification is a strategic step. Strengthening the digital investigation System (digital forensic) with the procurement of the latest technological devices and the construction of digital forensic laboratories in every jurisdiction is needed to improve the effectiveness of handling. Harmonization of regulations and policies between the Criminal Code, ITE Law, and related regulations must be carried out to avoid conflicts of norms and ensure legal certainty . Education and digital literacy of the public through public awareness campaigns about online fraud modes and how to prevent them becomes an effective preventive effort, as recommended to minimize online fraud and protect the public from losses. Strengthening international cooperation in handling cybercrime through ratification of international conventions, bilateral extradition agreements, and the establishment of joint task forces with other countries is the key to successful enforcement of cross-border perpetrators.

CONCLUSION

The development of digital technology has transformed the landscape of conventional fraud crimes into more complex and sophisticated cybercrime crimes. The characteristics of cyber fraud that are borderless, anonymous, and utilize information technology as the main means of creating serious challenges for law enforcement in Indonesia. Modus operandi such as phishing, social engineering, electronic transaction fraud, digital identity theft, to cryptocurrency investment fraud continues to grow following technological advances. Regulation of Indonesian criminal law through the Criminal Code Article 378 and Law Number 19 of 2016 on information and electronic transactions has provided a juridical foundation in dealing with digital fraud crimes, but there is still a gap between technological developments and regulatory readiness. The main constraints include the limited competence of the apparatus in digital forensics, the lack of valid electronic evidence, and the complexity of handling cross-jurisdictional cases that require effective international cooperation to optimize law

P-ISSN 2829-1654
E-ISSN 2829-517X

enforcement. Optimizing the handling of cybercrime fraud requires a comprehensive and integrated approach from various parties. The government needs to accelerate regulatory harmonization by updating laws and regulations that are adaptive to technological developments, including special regulation of cryptocurrency-based crime and artificial intelligence. Increasing the capacity of law enforcement officers through intensive digital forensic training and the provision of digital forensic laboratory infrastructure in every jurisdiction is an urgent need. Strengthening international cooperation through the ratification of cybercrime conventions and bilateral extradition treaties needs to be prioritized to overcome cross-jurisdictional barriers. Education and improvement of people's digital literacy through public awareness campaigns about online fraud modes must be carried out in a massive and sustainable manner. Coordination between law enforcement agencies needs to be strengthened to avoid overlapping authorities and ensure the effectiveness of handling cyber fraud cases.

REFERENCES

Alvina, and Anggita Hanum Pramesti. "Analisis Terjadinya Tindak Pidana Penipuan Melalui Platform Media Sosial" 07 (2024).

Arifin, Z, E P Handayani, and Penerbit Deepublish. *Cybercrime: Menyelisik Penegakan Hukum Dan Penanggulangannya*. Deepublish, 2023. https://books.google.co.id/books?id=H8gM0AEACAAJ.

Miski, Yusran Radyamal Al. "Eksistensi Tindak Pidana Penipuan (Bedrog) Dalam Pasal 378 Kuhp Di Era Digital" 10, no. 2 (2025): 369–89.

Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web Tindakan Dan Perbuatan Hukum Yang Nyata . Secara Yuridis Dalam Hal Ruang Cyber" 6, no. 1 (2023): 226–41.

Muharawati, and Hardian Kumala. "Analisis Fenomena Anak Sebagai Pelaku Kejahatan Penipuan Online Di Kabupaten Wajo Dari Perspektif Kriminologis" 3, no. 2 (2024): 41–49.

Nurfahda, Amanda Faizah, Annasyanda Jelita Putri, Nayottama Aryasuta Yardi, Fitra Deni, Fakultas Ilmu, and Ilmu Politik. "Analisis Penipuan Online Dalam Bentuk Phising Menurut Perspektif Hukum Indonesia" IV, no. Oktober (2024).

Pahrudin, Pajar, and Kalimantan Timur. "Analisis Penipuan Digital (Cyber Fraud) Tantangan Dan Solusi Dalam Era Transformasi Digital" 7 (2025): 70–80.

Pramesti, Yusri Ardiyah, and Emy Rosnawati. "Tindak Pidana Penipuan Dalam Media Jual Beli Online," no. 4 (2023): 1–15.

Rahmadani, Fayza Hafiz, Hendrian Cahya Sutany, and Mohamad Ragil Aditya. "Cybercrime : Analisis Dan Mitigasi Resiko Penipuan Tilang Online Melalui Aplikasi WhatsApp (WA)" 3, no. 1 (2025).

Riswandi, B A, and A M Gultom. *Cyber Crime, Cyber Law, Dan Cyber Profession*. Rajawali Pers, 2023. https://books.google.co.id/books?id=87oL0QEACAAJ.

Royyan, Muhammad Zainil. "Analisis Kriminologis Terhadap Tindak Pidana Penipuan Melalui Media Online Di Kota Makassar Muhammad" 1, no. 1 (2022): 1–9.

"Sekelumit Mengenai Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan TransaUndang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Ksi Elektronik." *Jurnal Legislasi Indonesia* 5, no. 4 (2018): 42–52. https://doi.org/10.54629/jli.v5i4.305.

Sirait, T M. *Cyber Law Dalam Teori Dan Perkembangannya: Cyber Crime, Privacy Data, e-Commerce*. Deepublish, 2023. https://books.google.co.id/books?id=eGS20AEACAAJ.

"Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik." *Journal of Physics A: Mathematical and Theoretical* 44, no. 8 (2011): 287.

Wahyudin, Jalil, Ruslan Renggong, and Abd Haris Hamid. "Analisis Tindak Pidana Penipuan Secara Online Di Wilayah Kepolisian Daerah Sulawesi Selatan" 6, no. 2 (2024): 273–80. https://doi.org/10.35965/ijlf.v6i2.4474.

Wibisono, Claressia Sirikiet. "Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial (Twitter)" 2, no. 2 (2023).

P-ISSN 2829-1654
E-ISSN 2829-517X