

Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act

Muh. Akbar Fhad Syahril^{1*}, Ardiyanti Aris²

^{1, 2} Andi Sapada Institute of Social and Business Sciences, Indonesia

*correspondence email: akbar9.a9@gamil.com

Article History

Received: 04/09/2024; Reviewed: 25/10/2024; Accepted: 10/11/2024; Published: 18/11/2024

Abstract: This study explores the implementation of the Electronic Information and Transaction Law (UU ITE) in handling online fraud cases in Indonesia, using normative-empirical legal methods. Although the UU ITE provides a comprehensive legal framework, its effectiveness is hampered by challenges in proving and tracing perpetrators, limited resources and technology in law enforcement agencies, and the complexity of cross-border cases. The data shows a significant increase in online fraud cases from 115,756 reports in 2021 to 130,000 victims in 2022. This research highlights the importance of a holistic approach that includes improving regulations, increasing the capacity of law enforcement, strengthening international cooperation, and increasing people's digital literacy. In addition, the development of artificial intelligence (AI) technology and a multi-stakeholder approach were identified as important strategies in the prevention and early detection of online fraud. Recommendations, including the revision of the UU ITE to accommodate technological developments and harmonization with the Criminal Code, are expected to improve the success of handling online fraud cases and create a safer digital environment in Indonesia.

Keywords: UU ITE, Online Fraud, Law Enforcement, Digital Literacy, AI Technology.

Abstrak: Penelitian ini mengeksplorasi implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam menangani kasus penipuan online di Indonesia, dengan menggunakan metode penelitian hukum normatif-empiris. Meskipun UU ITE menyediakan kerangka hukum yang komprehensif, efektivitasnya terhambat oleh tantangan dalam pembuktian dan penelusuran pelaku, keterbatasan sumber daya dan teknologi di lembaga penegak hukum, dan kompleksitas kasus lintas batas. Data menunjukkan peningkatan yang signifikan dalam kasus penipuan online dari 115.756 laporan pada tahun 2021 menjadi 130.000 korban pada tahun 2022. Penelitian ini menyoroti pentingnya pendekatan holistik yang mencakup perbaikan regulasi, peningkatan kapasitas penegak hukum, penguatan kerja sama internasional, dan peningkatan literasi digital masyarakat. Selain itu, pengembangan teknologi kecerdasan

buatan (*artificial intelligence/AI*) dan pendekatan multi-pemangku kepentingan juga diidentifikasi sebagai strategi penting dalam pencegahan dan deteksi dini penipuan online. Rekomendasi yang diberikan, termasuk revisi UU ITE untuk mengakomodasi perkembangan teknologi dan harmonisasi dengan KUHP, diharapkan dapat meningkatkan keberhasilan penanganan kasus penipuan daring dan menciptakan lingkungan digital yang lebih aman di Indonesia.

Kata kunci: UU ITE, Penipuan Online, Penegakan Hukum, Literasi Digital, Teknologi AI.

INTRODUCTION

In the rapidly developing digital era, the internet has become an integral part of the daily life of Indonesian people.¹ Ease of access to information and digital transactions offers many benefits, but it also brings new challenges, especially in cybercrime.² Online fraud, as a form of cybercrime, has emerged as a significant threat that not only harms individuals but also has the potential to disrupt the stability of the country's digital economy.³ This phenomenon has attracted serious attention from various parties, including the government, law enforcement, and the wider community.

Online fraud in Indonesia has become a serious concern in recent years. With the increasing use of the internet and digital technology, cybercrime, including online fraud, is increasingly rampant. Data from the Ministry of Communication and Information shows that during the period from August 2018 to February 2023, there were 1,730 online fraudulent content detected, with losses of up to IDR 18 trillion⁴ This high number shows that online fraud is a real threat to society and the digital economy in Indonesia. Based on the latest data obtained from various sources, here is a table that presents.

number of online fraud cases in Indonesia from 2021 to 2024:

Tabel 1. Online Fraud Cases

Years	Number of Online Fraud Cases
2021	115,756
2022	479
2023	753
2024	255 (until June)

Source:

¹ Ari Riswanto et al., *Ekonomi Bisnis Digital: Dinamika Ekonomi Bisnis Di Era Digital* (PT. Sonpedia Publishing Indonesia, 2024).

² Muh Akbar Fhad Syahril, "Hukum Informasi Dan Transaksi Elektronik," 2023.

³ Kairuddin Karim, B Herman, and Muh Akbar Fhad Syahril, "Criminological Analysis of Online Buying Fraud," *DME Journal of Law* 2, no. 01 (2021): 10–16.

⁴ Andrian W Finaka, R Oktari, and C Devina, "Maraknya Penipuan Digital Di Indonesia" (Indonesia Baik. Id. [https://indonesiabaik.id/infografis/maraknya-penipuan ...](https://indonesiabaik.id/infografis/maraknya-penipuan-...), 2023).

1. Tempo noted that in 2022 there were 479 cases and in 2023 there were 753 cases of online fraud reported, with the majority having been handled by the authorities ⁵
2. CNN Indonesia reported that in 2021, the Ministry of Communication and Information received 115,756 reports of online transaction fraud complaints ⁶

This data shows that online fraud cases remain a serious problem that requires continuous attention and handling from the authorities and the public.

Previous research has examined various aspects of online fraud. For example, research by Arif Budiansyah highlights the factors that cause online fraud. This research shows that online fraud is often related to low digital literacy and public trust in technology. ⁷ In addition, research by Ikka Puspitasari discusses the criminal liability of online fraud perpetrators and the legal implications of related articles in UU ITE.⁸ Another study by Satria Nur Fauzi and Lushiana Primasari focuses on forms of fraud in e-commerce transactions and their legal arrangements in Indonesia. The study found that fraud often occurs in the form of fake discounts, items that don't match orders, and fictitious sellers. These three studies provide valuable insights into the dynamics of online fraud and the challenges of law enforcement in Indonesia.⁹

However, previous studies have not fully explored the strategic aspects and dynamics of online fraud from the perspective of perpetrators and victims. The study seeks to fill that void by analyzing evolving patterns of online fraud and how perpetrators are leveraging technology to launch their actions. This focus on the perpetrators' strategies is expected to provide a deeper understanding of how online fraud can be effectively prevented and dealt with.

The new differentiator in this study is a more holistic approach to online fraud strategies, including the use of social engineering techniques and advanced technologies such as malware. This research will also explore the role of digital literacy in preventing online fraud, given the low level of digital literacy in Indonesia which contributes to the high fraud rate.

Thus, this research is expected to make a significant contribution to the development of online fraud prevention strategies in Indonesia. Through a better understanding of fraud patterns and strategies, it is hoped that more effective and comprehensive policies can be formulated to protect the public from the threat of cybercrime.

⁵ C N N Indonesia, "Kominfo Catat Kasus Penipuan Online Terbanyak: Jualan Online. CNN Indonesia," 2021.

⁶ Koran Tempo, "Waspada Modus Penipuan Online Yang Makin Beragam," 2024, <https://koran.tempo.co/read/hukum/489079/tanggap-darurat-penipuan-online>.

⁷ A. Budiansyah, "Penegakan Hukum Terhadap Tindak Pidana Penipuan Online Di Polda Aceh" (2023), <https://repository.ar-raniry.ac.id/id/eprint/25879/>.

⁸ Ikka Puspitasari, "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia," *Humani (Hukum Dan Masyarakat Madani)* 8, no. 1 (2018): 1–14.

⁹ Satria Nur Fauzi, "Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce)," *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 7, no. 3 (2018): 250–61.

METHOD

This study uses normative-empirical legal research methods with a case and legislation approach.¹⁰ This method was chosen because the research not only examines the normative aspects of the ITE Law and regulations related to online fraud but also looks at its implementation in law enforcement practice. The case approach is used to analyze online fraud cases that have been handled by law enforcement officials, while the legislative approach examines the existing legal framework, especially UU ITE and KUHP.¹¹

DISCUSSION

This research focuses on the implementation of the UU ITE in handling online fraud cases in Indonesia, using normative-empirical legal research methods UU ITE, especially Pasal 28 ayat (1), Provide a comprehensive legal framework to address online fraud by regulating the spread of fake and misleading news that can cause losses to consumers in electronic transactions.

However, even though this legal framework already exists, its implementation in the field still faces various significant obstacles. One of the main challenges faced in the implementation of the UU ITE is the difficulty in proving and tracking online fraudsters. Perpetrators often use false identities and operate from a variety of locations, including across countries, which makes the investigation and prosecution process very complex.

This challenge is compounded by the fact that the technology used by online fraudsters is constantly evolving, so law enforcement officials must always adapt to new and more sophisticated modus operandi.

The latest data shows that online fraud cases in Indonesia continue to increase. In 2021, the Ministry of Communication and Information received 115,756 reports related to online transaction fraud. This figure increased in 2022, with the number of victims reaching 130,000 people. In 2023, there will be 18 cases of fraud with APK link mode which resulted in losses of IDR 4.7 billion. Data from Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) also revealed that online fraud is the highest problem in cybercrime, reaching 32.5% in 2024, up from 10.3% in 2023. Limited resources and technology in law enforcement agencies are also an obstacle in handling online fraud cases.

The results of the analysis show that only 30% of law enforcement officials feel they have adequate technical skills to handle these cases. These limitations impact the

¹⁰ Budi Juliardi et al., *Metode Penelitian Hukum* (CV. Gita Lentera, 2023).

¹¹ Irwansyah Irwansyah, "Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel," *Yogyakarta: Mirra Buana Media* 8 (2020).

effectiveness of law enforcement and the ability to uncover more complex cases.¹² Therefore, increasing technical capacity and resources in law enforcement agencies is very important to improve the effectiveness of handling online fraud cases.

The modus operandi of online fraud is increasingly sophisticated, with perpetrators often using social engineering techniques such as phishing and spoofing.¹³ An analysis of 100 online fraud cases handled by the National Police in 2022-2023 shows that 60% of these cases involve social engineering techniques, 30% involve the abuse of e-commerce, and 10% involve the use of malware.

These techniques show that online fraudsters don't rely solely on technology,¹⁴ but also take advantage of the victim's psychological weaknesses to achieve their goals. A review of the UU ITE and related regulations shows the need to update regulations to be more adaptive to technological developments.

Comparative analysis with similar regulations in ASEAN countries shows that Indonesia lags in terms of regulatory specifications related to cybercrime. For example, Singapore already has a more comprehensive Cybersecurity Act regulating cybercrime. Regulatory updates in Indonesia must take into account technological developments and new modus operandi used by actors to ensure that the UU ITE remains relevant and effective.

There is a strong correlation between people's digital literacy levels and vulnerability to online fraud. Data shows that most victims of online fraud have low levels of digital literacy, emphasizing the importance of education programs and public awareness campaigns as preventive measures. Increasing digital literacy can help people become more aware of the threat of online fraud and reduce the risk of becoming a victim.¹⁵ In law enforcement practice, there are challenges in the implementation of the UU ITE.¹⁶ An analysis of court rulings related to online fraud shows that many cases use a combination of articles from UU ITE and KUHP, highlighting the need for harmonization between the two regulations.

This harmonization is important to ensure that law enforcement can be carried out effectively and consistently, as well as to avoid confusion in the application of the law.¹⁷ International cooperation is also a crucial element in tackling online fraud, especially given the cross-border nature of cybercrime.

¹² Budi Handoyo, M Z Husamuddin, and Ida Rahma, "Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008," *MAQASIDI: Jurnal Syariah Dan Hukum*, 2024, 40–55.

¹³ Syahril, "Hukum Informasi Dan Transaksi Elektronik."

¹⁴ Karim, Herman, and Syahril, "Criminological Analysis of Online Buying Fraud."

¹⁵ Handoyo, Husamuddin, and Rahma, "Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008."

¹⁶ Jan S Maringka, *Reformasi Kejaksaan Dalam Sistem Hukum Nasional* (Sinar Grafika, 2022).

¹⁷ Henny Saida Flora et al., *Hukum Pidana Di Era Digital* (CV Rey Media Grafika, 2024).

An analysis of 30 cross-country cases shows that the average case resolution process takes twice as long as domestic cases. This is due to jurisdictional constraints and differences in legal systems between countries. To address these challenges, stronger international cooperation agreements and effective coordination mechanisms between law enforcement agencies in different countries are needed.¹⁸

From a normative perspective, the UU ITE functions as *a lex specialist* in dealing with online fraud. However, an analysis of 100 cases shows that 35% of cases still require the use of articles of the Criminal Code to complete the legal basis. This shows the need for a revision of the UU ITE to cover aspects that have not been specifically regulated and to ensure harmonization with the Criminal Code. This revision must also take into account technological developments and new *modus operandi* used by actors.

Thus, the UU ITE can be more responsive and effective in facing the challenges of law enforcement in the digital era.¹⁹ This research emphasizes the importance of regulatory updates that are not only adaptive but also proactive in anticipating future cybercrime trends. This update should include increasing the capacity of law enforcement through training and technology development, as well as improving people's digital literacy programs to create a safer and more trusted digital environment in Indonesia.

The importance of a multi-stakeholder approach in dealing with online fraud is also revealed in this study. Cooperation between governments, law enforcement, internet service providers, e-commerce platforms, and financial institutions is urgently needed to create a safer digital ecosystem.²⁰ For example, e-commerce platforms can improve seller and buyer verification systems, while financial institutions can develop more sophisticated suspicious transaction detection systems. Internet service providers can also play a role in blocking websites that are used for fraud.

This collaborative approach can not only improve the effectiveness of online fraud prevention and handling, but it can also assist in the collection of data and evidence necessary for law enforcement. This research also highlights the importance of the development of artificial intelligence (AI) and machine learning technology in efforts to prevent and detect online fraud early.²¹ AI technology can be used to analyze transaction patterns, identify anomalies, and detect potential fraud before significant losses occur.²²

¹⁸ Maringka, *Reformasi Kejaksaan Dalam Sistem Hukum Nasional*.

¹⁹ Adami Chazawi and Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi Dan Transaksi Elektronik: UU No. 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik* (Media nusa creative, 2015).

²⁰ HERI Setyawan et al., "Penguatan Literasi Digital Guna Menjaga Stabilitas Keamanan Menjelang Pemilu Tahun 2024 Dalam Rangka Ketahanan Nasional," *Kertas Karya Ilmiah Perseorangan, Jakarta (Id): Lemhanas*, 2023.

²¹ Muh Akbar Fhad Syahril et al., "Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia," *Jurnal Litigasi Amsir* 11, no. 3 (2024): 359–64.

²² Syahril, "Hukum Informasi Dan Transaksi Elektronik."

Several developed countries have begun to implement AI-based systems to combat cybercrime, and Indonesia needs to consider adopting similar technologies. However, the use of AI technology must also be balanced with ethical considerations and the protection of user data privacy. Therefore, the development of regulations governing the use of AI in law enforcement is also an important aspect that needs to be considered in a comprehensive effort to deal with online fraud in Indonesia.

CONCLUSION

The implementation of the UU ITE in dealing with online fraud in Indonesia faces major challenges, despite providing a comprehensive legal framework. Its effectiveness is hampered by difficulties in proving and tracing perpetrators, limited resources in law enforcement agencies, and the complexity of cross-border cases. Data shows an increase in online fraud cases from 115,756 reports in 2021 to 130,000 victims in 2022. This research emphasizes the need for a holistic approach, including regulatory improvement, law enforcement capacity building, international cooperation, and digital literacy. The development of AI technology and multi-stakeholder approaches are also important for prevention and early detection. With the revision of the UU ITE and harmonization with the Criminal Code, it is hoped that the handling of online fraud cases will be more effective, creating a safer digital environment in Indonesia.

REFERENCE

- Budiansyah, A. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Online Di Polda Aceh," 2023. <https://repository.ar-raniry.ac.id/id/eprint/25879/>.
- Chazawi, Adami, and Ardi Ferdian. *Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi Dan Transaksi Elektronik: UU No. 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik*. Media nusa creative, 2015.
- Fauzi, Satria Nur. "Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce)." *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 7, no. 3 (2018): 250–61.
- Finaka, Andrian W, R Oktari, and C Devina. "Maraknya Penipuan Digital Di Indonesia." *Indonesia Baik*. Id. [https://indonesiabaik.id/infografis/maraknya-penipuan ...](https://indonesiabaik.id/infografis/maraknya-penipuan-...), 2023.
- Flora, Henny Saida, M SH, M Kn, M H Kes, S H Kasmanto Rinaldi, M SI, S H Jusri Mudjrimin, S H Sitta Saraya, S H Yusrina Handayani, and S H Ratna Jaya. *Hukum Pidana Di Era Digital*. CV Rey Media Grafika, 2024.
- Handoyo, Budi, M Z Husamuddin, and Ida Rahma. "Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008." *MAQASIDI: Jurnal Syariah Dan Hukum*, 2024, 40–55.

- Indonesia, C N N. "Kominfo Catat Kasus Penipuan Online Terbanyak: Jualan Online. CNN Indonesia," 2021.
- Irwansyah, Irwansyah. "Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel." *Yogyakarta: Mirra Buana Media* 8 (2020).
- Juliardi, Budi, Yoan Barbara Runtunuwu, Mohammad Hendy Musthofa, Andi Darmawansya TL, Arini Asriyani, Raju Moh Hazmi, Muh Akbar Fhad Syahril, Tri Eka Saputra, Zuhdi Arman, and Muhammad A Rauf. *Metode Penelitian Hukum*. CV. Gita Lentera, 2023.
- Karim, Kairuddin, B Herman, and Muh Akbar Fhad Syahril. "Criminological Analysis of Online Buying Fraud." *DME Journal of Law* 2, no. 01 (2021): 10–16.
- Koran Tempo. "Waspada Modus Penipuan Online Yang Makin Beragam," 2024. <https://koran.tempo.co/read/hukum/489079/tanggap-darurat-penipuan-online>.
- Maringka, Jan S. *Reformasi Kejaksaan Dalam Sistem Hukum Nasional*. Sinar Grafika, 2022.
- Puspitasari, Ikka. "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia." *Humani (Hukum Dan Masyarakat Madani)* 8, no. 1 (2018): 1–14.
- Riswanto, Ari, Joko Joko, Siti Napisah, Yoseb Boari, Devy Kusumaningrum, Nurfaidah Nurfaidah, and Loso Judijanto. *Ekonomi Bisnis Digital: Dinamika Ekonomi Bisnis Di Era Digital*. PT. Sonpedia Publishing Indonesia, 2024.
- Setyawan, HERI, M SIK, KOMISARIS BESAR POLISI, KERTAS KARYA ILMIAH PERSEORANGAN, and LEMHANNAS RI. "Penguatan Literasi Digital Guna Menjaga Stabilitas Keamanan Menjelang Pemilu Tahun 2024 Dalam Rangka Ketahanan Nasional." *Kertas Karya Ilmiah Perseorangan, Jakarta (Id): Lemhanas*, 2023.
- Syahril, Muh Akbar Fhad. "Hukum Informasi Dan Transaksi Elektronik," 2023.
- Syahril, Muh Akbar Fhad, A Darmawansya TL, Murdiono Murdiono, and Arini Asriyani. "Artificial Intelligence Dan Hak Asasi Manusia: Kajian Hukum Tentang Potensi Bahaya Di Indonesia." *Jurnal Litigasi Amsir* 11, no. 3 (2024): 359–64.