Juridical Analysis of Online Fraud Crimes and Various Forms of Fraud on Social Media

Zeno Eronu Zalukhu, Suci Ramadani, Ismaidar

Abstract

Online fraud through social media is a form of cybercrime that is growing rapidly along with advances in communication and information technology. This phenomenon not only causes significant material losses but also impacts public trust in the use of social media. This research method uses normative legal research by analyzing legal documents, legal principles, and literature studies. The results indicate that although relevant laws and regulations are sufficient, challenges remain in their implementation and enforcement due to technological dynamics and limited digital evidence. Thus, it is hoped that legal protection for victims of online fraud on social media can be maximized and encourage the creation of a safe and trustworthy digital ecosystem.

***Keywords**:* Fraud, Social Media, Victims, Legal Protection.

Zeno Eronu Zalukhu[1]
[1]Magister of Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: zenoeronuz@gmail.com

Suci Ramadani[2], Ismaidar[3]
[2,3]Lecturer Of Management Study Program, Universitas Pembangunan Panca Budi, Indonesia
e-mail: suciramadani@dosen.pancabudi.ac.id[2], ismaidarisma@gmail.com[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The development of internet technology is recognized to have provided many conveniences, especially in helping human work. However, this technological advancement has also led to the emergence of new types of crimes affecting many people. Along with the rapid growth of internet technology, certain individuals have also misused this technological tool to commit crimes (Ingkeatubun & Rosando, 2024). One of the negative impacts of modern technology is the increasing occurrence of fraud through the internet, which has become common in society. Criminal acts of fraud committed through online media often take place on online marketplaces such as Bukalapak, Tokopedia, and Lazada, or on social media platforms like Twitter and Facebook (Herrenauw, Titahelu & Saimima, 2022).[1]

In its development, the modus operandi of crimes has evolved alongside human civilization. As society and technology progress, humans increasingly utilize digital technology facilities to interact with one another. Almost all economic activities in the world now rely on the internet and electronic systems. One aspect of economic activity is transactions conducted through the internet, popularly known as e-commerce. The advancement of the internet has created a modern world known as cyberspace, where individuals interact without geographical boundaries and without meeting face-to-face, but through electronic transactions.

In Indonesia, the presence of information technology has been regulated through Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions (hereinafter referred to as the ITE Law). The ITE Law serves as the first legal framework to regulate electronic transaction activities in Indonesia and provides legal innovation aimed at ensuring legal certainty and protection for the public in conducting electronic transactions.[2]

The researcher chose this topic based on a real-life experience that happened directly to me. There was a phone call received by my friend from someone claiming to represent a marketplace, saying that I had been selected to receive a prize or souvenir that would be sent to the address listed on my ID card. My friend was told not to make any payment whatsoever. A few days later, a courier arrived at the address provided by my friend to deliver the item, again without requiring any payment. My friend told me about the incident, and I told him that I had never made any purchases on that marketplace. I advised him not to respond to any calls from unknown numbers, whether through mobile phones or WhatsApp. After the souvenir delivery, my friend began receiving multiple calls from unknown numbers trying to contact him. From this incident, I concluded that it was a type of scam or fraud scheme. This experience led me to explore more deeply the various types of online fraud and the laws related to such crimes.

Research Methodology

This type of research employs normative legal research. The normative juridical method is a legal research approach conducted on legal principles and the level of legal synchronization. Normative legal research can also be referred to as doctrinal legal research. The normative juridical method primarily involves library research, which relies mainly on secondary data sources — including primary legal materials such as collections of laws and regulations, secondary legal materials such as scholarly works of legal experts, and tertiary legal materials derived from internet sources.

In this study, a qualitative normative juridical research method was used, which involves examining and analyzing data without the use of diagrams or numerical data. The data sources used in this research consist of secondary data, categorized as follows:

1. Primary legal materials, namely regulations and laws in force in Indonesia that are relevant to the issues under study;
2. Secondary legal materials, obtained from various written references such as journals, scientific articles, documentary books, and other legal literature;

3. Tertiary legal materials, based on information sources available on the internet. [3]

Discussion

3.1 Juridical Analysis of Online Fraud Crimes

Today, rapid development has driven various sectors to evolve, one of which is the technology and information sector. Many countries are striving to advance technological development, including Indonesia. The development of technology and information is driven by the public's need to access various things more quickly. This has made technology and information play an essential role in social life in Indonesia.

However, besides its positive impacts, online buying and selling activities have also triggered the emergence of new crimes, commonly referred to as cybercrime. The term *cybercrime* generally refers to criminal acts characterized by the involvement of individuals who possess knowledge and control over information technology such as the internet and mobile devices. One form of crime committed through online media is fraud (Ramli, 2021). This issue has prompted the establishment of laws that regulate and address online fraud crimes in Indonesia.

Indonesia's positive law that regulates online crimes (cybercrime) is contained in Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). Before the enactment of the ITE Law, the most commonly used legal framework for handling cybercrimes was the Criminal Code (KUHP) and the Criminal Procedure Code (KUHAP).

The term *online fraud* refers to acts of deception experienced by internet users. Online fraud may involve stealing personal data, which can lead to identity theft, or using internet services to deceive victims or carry out fraudulent transactions. Such fraud can occur through chat, social media, email, or websites. Online fraud is often facilitated by the convenience of internet-based transactions — such as paying bills, shopping, making online reservations, or working remotely. Unfortunately, these conveniences are often exploited and misused by irresponsible individuals (Team, 2022).[4]

Etymologically, the term *penipuan* (fraud) is derived from the root word *tipu* (deceive), with the prefix *pe-* and suffix *-an*, meaning an act of deception carried out by a person whose behavior is inconsistent with the truth. From a legal standpoint, the crime of fraud does not have an explicit definition. The articles in the Criminal Code (KUHP) related to fraud do not provide a specific definition but rather contain elements that serve as references for determining whether an act can be classified as fraud.

Provisions concerning fraud are found in Book II of the Indonesian Criminal Code, Chapter XXV (Articles 378 to 395), all of which are categorized under *bedrog* or acts of deceit. The general form of fraud is stated in Article 378 of the Criminal Code, which reads:

"Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false circumstances, by deceit or false pretenses, or by a series of lies, persuades someone to hand over an item, to incur debt, or to eliminate a debt, shall be punished for fraud."[5]

It is important to remember that aside from the legal aspect, we as users of information technology must always remain cautious and vigilant when using the internet. There are many ways to avoid becoming a victim of cyber fraud, such as not clicking suspicious links, protecting personal data, ignoring emails or messages that request personal information, and

other precautionary measures. By increasing awareness of the dangers of cyber fraud, we can prevent cybercrimes and create a safer and more trustworthy digital environment.[6]

3.2 Law Regulating Online Fraud Crimes

In the practice of e-commerce transactions conducted through social media platforms such as Facebook, the requirements for imposing criminal liability on perpetrators of online crimes include the fulfillment of all elements of a criminal act and the ability to prove that the act was carried out intentionally and with full awareness that it is punishable by law.

The researcher found that law enforcement officers often face difficulties in uncovering cybercrime cases. These challenges arise from several factors, such as banking bureaucracy, lack of coordination between investigators and mobile or internet service providers, the limited number of personnel with expertise in information technology, and insufficient special equipment to handle IT-related crimes. Based on these realities, online fraud cases—such as those committed via Facebook—eventually led to the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which became Indonesia's first law governing information technology and electronic transactions. This law was a crucial legislative product that established a legal foundation for the use of information technology and electronic transactions. Later, the law was amended and updated through Law No. 19 of 2016 on Electronic Information and Transactions.

Online fraud committed through social media platforms like Facebook can be identified under several provisions within Chapter XI (Criminal Provisions) of the ITE Law, which prohibit certain acts closely related to fraudulent behavior. Specifically, Article 28 Paragraph (1) of Law No. 19 of 2016 states:

"Every person who knowingly and without authority spreads false and misleading information that results in consumer losses in electronic transactions shall be subject to criminal sanctions."

The penalties for such offenses are regulated under Article 45A Paragraph (1), which reads:

"Every person who knowingly and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing materials as referred to in Article 28 Paragraph (1) shall be subject to imprisonment for up to six (6) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah)."

In addition to the ITE Law, acts of online fraud can also be regulated under the Indonesian Criminal Code (KUHP), specifically Article 378 Paragraph (1), which states:

"Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, through deceit, or a series of lies, induces another person to hand over an item, provide credit, or eliminate a debt, shall be punished for fraud with imprisonment for up to four (4) years."

Criminal law serves as a tool or means to address this problem, and it is expected to provide an appropriate solution. Therefore, the development of criminal law must be further strengthened and implemented in a focused and integrated manner. This includes codification, unification of certain legal fields, and the drafting of new legislation to effectively respond to emerging criminal acts.

While Article 378 of the Criminal Code clearly stipulates that those who commit fraud shall be subject to criminal sanctions, its enforcement remains less effective. Effective law

enforcement requires not only the existence of legal provisions but also competent law enforcement officers and institutions authorized to handle criminal cases — such as the Police, the Attorney General's Office, and the Courts.

In recent years, cases of online fraud have continued to increase, despite being clearly regulated under Article 378 of the Criminal Code and Article 28 Paragraph (1) of Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law).[7]

3.3 Legal Protection for Victims of Fraud Crimes

Economic crimes as criminal offenses can only be punished if they are regulated by law. The Criminal Code (KUHP) serves as the primary legal framework for conventional crimes such as forgery, fraud, and other similar offenses. Every case of fraud—whether occurring online (cyber fraud) or offline (traditional fraud)—always involves one party suffering a loss and another gaining an unlawful benefit. Referring to this, the Criminal Code (KUHP) stipulates several rights that victims are entitled to, as follows:

1. The right to file a complaint (as stipulated in Article 108 Paragraph (1) of the KUHP);
2. The right to oversee investigators and public prosecutors (as stipulated in Articles 77 in conjunction with Article 80 of the KUHP);
3. The right to pursue compensation claims resulting from criminal acts through the combination of civil and criminal proceedings (Articles 96 to 101 of the KUHP).

The legal provisions applicable to fraud perpetrators depend on the specific acts they commit, since each case may involve different methods, motives, and circumstances. The resolution of such cases can refer to the legal doctrine of *Lex Specialis Derogat Legi Generalis*, which means that a specific legal rule overrides a general one. In this context, Article 28 Paragraph (1) of the ITE Law serves as a *Lex Specialis* that takes precedence over Article 378 of the KUHP. This legal principle establishes that when two laws regulate the same matter, the more specific law prevails over the general one.

The legal protection provided under the Law on Electronic Information and Transactions (ITE Law) is an effort to resolve such cases through criminal legal channels. Therefore, a more specific legal framework is needed to regulate electronic transactions. The ITE Law has undergone several amendments to ensure legal certainty for those engaging in electronic transactions, to foster economic growth, to prevent crimes based on information technology, and to protect the public in their use of such technologies.[8]

Several preventive measures can be taken when receiving suspicious messages or calls involving online fraud schemes, including:

1. Critically evaluate any message or phone call received before taking any action;
2. Do not be easily lured by promises of wealth or rewards, as there is no such thing as instant riches;
3. Avoid clicking on links sent via messages from unknown numbers; if they come from known contacts, confirm their authenticity first;
4. Never share personal data with others without a legitimate reason;
5. Block suspicious numbers or report them to the authorities if there are indications of fraud;
6. Inform friends, family, or social media contacts if you receive messages or calls that appear to be part of a fraud scheme.[9]

Conclusion

Online fraud is a term used to describe acts of deception experienced by internet users. Such fraud may involve stealing personal data, which can lead to identity theft, or the misuse of internet services to deceive victims or carry out fraudulent transactions. Online fraud can occur through chats, social media, emails, or websites. This crime is often driven by the convenience of online transactions — such as paying bills, shopping, making online reservations, or even working remotely. Unfortunately, these conveniences are often exploited and misused by irresponsible individuals.

Indonesia's positive law governing online crimes (cybercrime) is contained in Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). Before the enactment of the ITE Law, the legal framework most frequently used to address cybercrimes consisted of the Criminal Code (KUHP) and the Criminal Procedure Code (KUHAP).

Article 378 of the Criminal Code (KUHP) regulates criminal acts of fraud; Article 19 Paragraph (1) of Law No. 8 of 1999 concerns Consumer Protection; and Law of the Republic of Indonesia No. 1 of 2024, which serves as the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, further strengthens legal enforcement related to online fraud.

The legal protection stipulated under the Electronic Information and Transactions Law (ITE Law) serves as an effort to resolve cases of online fraud through criminal legal channels, ensuring justice for victims and providing a legal basis for prosecuting perpetrators of cybercrimes.

References

[1] Adrianto, Thalib, H.,&Ilyas,M. (2024). "*Penegakan Hukum Terhadap Tindak Pidana Penipuan Online".* Jurnal Of Lex Philosopy. 5 (2)

[2] Kamran,M.,&Maskun. (2021). "*Penipuan Dalam Jual Beli Online: Prespektif Hukum Telematika".* Balobe Law Journal. 1 (1)

[3] Mulyadi.,Nurdin,A.A.,Anjani,A.A.,Alamsyah,F.D.,Sifana,F.,Yudistio,M.A.,Maulana,M .K.,Rabbani,R.A.A. (2024)."Analisis Penipuan Online Melalui Media Sosial Dalam Prespektif Kriminologi". *Media Hukum Indonesia* 2 (2)

[4] Devi Trisnawati. 2023.*"Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik".* Jurnal Ilmu Sosial. 2 (9)

[5] Wibisono,C.S.,&Mahanani,A.E.E. (2023). "*Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial (Twitter)".* Jurnal Hukum, Politik Dan Ilmu Sosial. 2 (2)

[6] Wahyudi,A.,Mahdi,U.,Media,M.A. (2024).*"Analisis Yuridis Terhadap Tindak Pidana Penipuan Siber Dengan Modus Operandi Business Email".* Jurnal Ilmu Hukum. 4 (2)

[7] Prabhaswara,S. (2023). "*Analisis Yuridis Terhadap Tindak Pidana Penipuan Didalam Penggunaan Media Sosial".* Jurnal Bevinding. 1 (3)

[8] Amalia,E.Y.,&Isnawati,M. (2024). *"Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Transaksi Jual Beli Pada Marketplace".* Perspektif Hukum. 24 (1)

[9] Riti,Y.F. (2024). *"Penyuluhan Dan Edukasi Identifikasi Modus Penipuan Melalui Media Sosial Bagi Masyarakat".* Jurnal CSDS. 3 (1)