Original Article

law& pass International Journal of Law, Public Administration and Social Studies https://lawpass.org

Juridical Study on Investigation of Fraud Crime Cases in E-Commerce in Indonesia

Shinta Widhaningroem[1]*, Yeni Widowaty[2]
Master of Law, Post Graduate Programe Universitas Muhammadiyah Yogyakarta, Indonesia

*Corresponding author: shintawdhh@gmail.com

Abstract
Fraud crimes in e-commerce in Indonesia are increasing along with technological advances and the widespread use of the internet in buying and selling transactions. Many victims, especially women, who are attracted to the various products offered online are the main targets of this crime. This study aims to examine legal policies and law enforcement against e-commerce fraud crimes in Indonesia and identify obstacles law enforcement faces. The method used in this study is descriptive analysis with a normative juridical approach. The data used comes from literature studies and analysis of e-commerce fraud cases that have occurred. The results showed that legal policies related to fraud crimes in e-commerce in Indonesia are based on applicable criminal law principles, namely ius penile and danius pungent. Despite a clear legal foundation, law enforcement still faces various obstacles, including law enforcement officials' need to understand information technology, differences in legal interpretation, and low public awareness in reporting cybercrimes. Effective law enforcement requires collaborative efforts between governments, law enforcement officials, and communities, as well as capacity building and socialization related to online transaction security.

Keywords: crime, fraud, e-commerce.

Introduction
The development of information and communication technology has brought significant changes in various aspects of life, including in the world of trade. E-commerce or electronic commerce has become one of the most popular ways for people to make transactions. E-commerce is all electronic transactions, including credit card transactions and the infrastructure required for electronic commerce operations. (Semerádová & Weinlich, 2022) E-commerce transactions allow the purchase of almost any good or service, including publications, music, airline tickets, and financial products such as stock trading and online banking. (Gupta, Kushwaha, Badhera, Chatterjee, & Gonzalez, 2023)

E-commerce is considered as the sale and purchase of goods and services over the internet in exchange for money and data transfer to complete transactions. E-commerce is at the forefront of transforming marketing strategies, based on new technologies, and facilitating product information and improving decision making. (Rosário & Raimundo, 2021)

In Indonesia, the growth of e-commerce is very rapid, driven by wider internet penetration and changes in consumer behavior that are increasingly comfortable shopping online. E-commerce has the potential to reach a larger audience and provide unlimited time to complete a

transaction. This process is very beneficial to many parties, both sellers and buyers. (Fernando, Prabowo, & Gatc, 2023; Irwanda, Ferary, Kamila, & Soebari, 2022; Risald, 2021) However, this development is also accompanied by an increase in cases of fraud committed through e-commerce platforms or virtual stores.

Fraud in e-commerce includes various modus operandi, such as the sale of counterfeit goods, goods that are never delivered despite being paid, as well as misuse of consumers' personal data. (Rantesalu, 2022; Sari, Febrianti, & Fauziah, 2022)

The Ministry of Communication and Information Technology (Kominfo) recorded the number of fraud victims Online It reached 130 thousand people in 2022, with a fraudulent bank account mode.(Sudoyo, 2023) In the YLKI report, related reports e-sommerce In 2022, it was related to 4 things. Starting from non-conforming goods (20%), Refund (32%), unilateral cancellation (8%), and non-arrival of goods (7%). Meanwhile, the National Consumer Protection Agency (BPKN) received 1,136 related public complaints e-commerce in the period 2017 to February 2023. (Bestari, 2023)

This phenomenon harms consumers financially and reduces public trust in the electronic trading system. Therefore, there is a need for effective policies and regulations to overcome this problem.

In Indonesia, virtual store fraud is becoming an increasingly important issue, along with the increase in e-commerce transactions. Although the government has issued various regulations to protect consumers, such as Law Number 8 of 1999 concerning Consumer Protection and Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), fraud cases are still rife. This shows the gap between the policies that have been implemented and the reality on the ground.

Investigating fraud cases in e-commerce is an important stage in law enforcement against criminal acts in cyberspace. The investigation is conducted to gather sufficient evidence to strengthen the case and determine the perpetrators and the modus operandi used to commit fraud. The initial stage in the investigation process usually starts with receiving reports from victims or related parties. This report forms the basis for initiating an investigation and determining the next steps to be taken by law enforcement officials.

Investigating e-commerce fraud cases requires a different approach compared to conventional fraud. Digital evidence collection, electronic forensic analysis, and coordination with e-commerce platforms are becoming important parts of the investigation process. In addition, e-commerce fraud cases often involve actors outside Indonesia's jurisdiction, thus requiring international cooperation in law enforcement.

The Indonesian police have developed various law implementation measures for e-commerce fraud. This includes establishing a special cyber crime unit, training for law enforcement officials on digital forensics, and educational campaigns to raise public awareness about the safety of online transactions. Despite this, challenges remain, such as limited technological resources, lack of cooperation from e-commerce platforms, and complexity in handling cross-border cases.

This study aims to evaluate the extent of virtual store fraud in Indonesian policies and regulations and the enforcement measures put in place by the Indonesian police to prevent such fraud. By evaluating the effectiveness of existing policies and regulations, areas that need improvement can be found to ensure that the Indonesian legal system can be more responsive to the development of crime in the digital world.

Method

The research method used in writing this journal article is a normative juridical approach that will be combined with an analysis of relevant laws and regulations and case studies of e-commerce fraud in Indonesia. This approach will allow researchers to identify and analyze existing legal frameworks and review their implementation and effectiveness in handling cases of e-commerce fraud. By analyzing existing laws and regulations, researchers will evaluate the clarity and consistency of existing regulations in handling e-commerce fraud cases.

Secondary data will be an important component of this study. Researchers will collect data from various sources, such as police reports, law journals, and scientific literature on e-commerce fraud in Indonesia. These data will be analyzed in depth to provide a comprehensive picture of the current state of e-commerce fraud, including trends, patterns, and characteristics of existing cases. This data analysis will be the foundation for compiling findings and conclusions in journal articles.

This research method will be carried out in a systematic and structured manner. First, researchers will conduct a literature review to gather relevant information about the applicable legal framework and previous research on e-commerce fraud. Furthermore, researchers will analyze relevant laws and regulations, including the ITE Law, the Criminal Code, and regulations related to consumer protection.

Fraud Crimes in e-Commerce in Indonesia

Everyone often makes buying and selling transactions, especially in today's increasingly advanced technological era. This transaction can be completed online to purchase and sell an item without the buyer visiting the item's location. Sold simply by looking at a glance at the motif or type of item you want to buy, as seen in the picture. But without realizing it, the existence of an online business can have a bad impact, namely when unscrupulous people take advantage of the appearance of online businesses to commit unlawful fraud against their victims.

Nowadays, it is very common for other people (humans) to commit fraud crimes through electronic media and internet services when trading online. Most victims are women because of the variety of goods provided in this online media, ranging from bags, clothes, make-up equipment, and others related to women's needs in beautifying themselves to look more trendy and their friends (Sunardi, Fadlil, & Kusuma, 2022).

This is what causes the formation of illegal acts of fraud in internet media that occur a lot today. The crimes that occur can only be committed by those who understand and understand information technology, which it utilizes to commit fraud. This is what causes many victims of

fraud who do not understand and understand information technology, so it is difficult to hold them accountable for criminal acts that occur. Fraud crimes committed in online media are regulated in Law Number 19 of 2016 concerning Electronic Information and Transactions. The ITE Law provides an important legal foundation in law enforcement against cybercrime, including fraud in online transactions. However, the law enforcement process can be more complicated for victims who lack an understanding of information technology. They may need help understanding how to report online crimes or how to obtain the evidence needed to follow up on cases.

Most criminals have increasing options for committing crimes, and fraud through the Internet continues to occur in various forms. One way is to create a fake website with this site, where goods are distributed at varying prices based on their various forms at generally easy-to-pay prices to attract buyers to the price given. In addition, some individuals commit online business fraud by breaking into other people's account details and conducting money transfer operations from the price of the goods provided.

This online fraud crime is carried out by providing goods at very cheap prices on the market to attract customers interested in buying and selling goods. The act of committing fraud online or targeting someone who uses the Internet is a common occurrence that affects people's daily lives. The increasing demand for internet users can also open up opportunities for criminal acts, including committing fraud.

One common technique in these online fraud crimes is account hijacking; when criminals take control of accounts, they believe will be valuable to them, including well-known social media accounts. Therefore, thieves will take advantage of such accounts to post items to be sold on the Internet. This arouses people's interest in buying these items and encourages them to think critically about the authenticity and quality of these items. Some are even willing to send money directly to accounts that have been burglarized.

e-Commerce Fraud Crime Law Policy in Indonesia

Criminal law is a rule that regulates behavior not by the implied or implied principle of legalization. It is applied and enforced in the community. There are two generally accepted notions of criminal law, namely ius poenaledand ius puniend. The definition of impartial criminal law is Ius poenaled. Criminal law is a statutory provision that can be enforced upon certain changes that meet certain requirements to be carried out as a crime.

Regarding fraud crimes in e-commerce, ius poenale establishes various provisions prohibiting and punishing fraudulent acts in online transactions. Criminal law enforcement is carried out to provide a deterrent effect to the perpetrators of crimes and prevent the recurrence of unlawful acts. In addition, the concept of danius puniend refers to the right of the state or authority to punish perpetrators of crimes by predetermined provisions. In the case of e-commerce fraud, danius puniend allows law enforcement officials to crack down and punish fraudsters according to the severity of the actions carried out and the impact on victims.

In theory, e-commerce-based fraud is synonymous with fraud perpetrated through traditional means. Evidence or methods of action involving electronic systems (computers, internet, and telecommunications equipment) lie in the difference. Therefore, Article 378 of the Criminal Code and Article 28 paragraph (1) of Law Number 19 of 2016 concerning Electronic Information and Transactions must continue accommodating law enforcement related to fraud crimes to strengthen its legal basis. ITE laws and regulations as special laws and regulations (Lex Specialist Derogat Lex Generale) can be a legal basis and guideline for individuals in the public sphere in online activities. In addition, the ITE Law is combined with several provisions of the Criminal Code, which are intended to facilitate the resolution of cases. This law is expected to function as an ius constituendum, namely laws and regulations that anticipate problems and accommodate developments, taking into account the demands and challenges associated with the development of global communication, including the adverse effects of information technology advances that have occurred. A wide influence on society. (Alkhairi, Purba, Eryzha, Windarto, & Wanto, 2019)

Furthermore, regarding law enforcement barriers to e-commerce-based crimes, there are still five factors at play. Among them are (1) legal factors themselves, where there are still regulations that do not specifically explain fraud crimes involving e-commerce, and (2) law enforcement factors, namely, there are still law enforcement officials who do not understand the regulations, so they cause multiple interpretations in their application. (3) factors, namely infrastructure and facilities that support law enforcement and can assist in the discovery of criminal acts; (4) Community factors: community reluctance to litigate in court and lack of awareness of the problems faced are examples; (5) Cultural factors: the more modern and high the culture of a nation, the more modern the crime in form, nature, and way of implementation (Anwar, Erwiyanto, & Romadon, 2023; Rahmanto, 2019)

In the study of misuse of information technology, online fraud crimes are included in the group of Illegal Content crimes or Computer Related Fraud. Entering data or information about something that is untrue, immoral, and/or may violate the law or disturb public order on the internet is considered illegal material. Fraud committed with the aim of harming others or for personal gain is called Computer Related Fraud. (Putri, Sudarti, & Siregar, 2024)

Online fraud is defined as fraudulent activities carried out through the use of computers, such as data manipulation or computer system breaches. If computer fraud results in direct financial gain or loss of property of others, it should be considered a crime. The perpetrator obtains financial benefits unlawfully, both for his personal interests and for the benefit of others.(Hidayat et al., 2023) The broad definition of "loss of property" includes loss of cash as well as tangible or intangible assets that have marketable value. In other words, online fraud is defined as a criminal offense in which the perpetrator creates a fraudulent scheme using the internet component to steal the property or interests, inheritance, or rights of others through false statements, either by providing false information or by concealing the true information.

Hill and Marion define online fraud or internet-based fraud by referring to a type of fraud that uses internet media such as chat rooms, emails, message boards, or websites to conduct fraudulent transactions with financial institution media such as banks or other financial

institutions. other institutions that have a certain relationship.(Hill & Marion, 2016) From Hill and Marion's understanding, it means that online fraud is fraud by using internet services or internet access software to deceive victims with the aim of taking advantage of them.

Online trading scams are undoubtedly widespread on social media networks. First of all, more and more people are looking for easy and efficient ways to meet their needs. However, some people have evil motives and seek to exploit the losses of others for their own benefit, even if it means engaging in fraudulent activities. There are many ways to commit e-commerce scams, ranging from easy to challenging. The actions taken against victims of virtual store fraud are real and serious, even if they are done online. Since ecommerce scams use computers, mobile phones, and the internet, they fall under the category of computer-related and unauthorized access scams for spreading misleading information. (Sefitrios & Chandra, 2021) According to the Indonesian Criminal Code for online shops, access to computer systems is not restricted and criminal access must be done deliberately. Therefore, a person acts by bypassing security measures, gaining access to computer data or pursuing other nefarious purposes, or by studying computers connected to other computer systems.

Therefore, there is a link between computer-related fraud and e-commerce. when the items sold look different from the real thing, or even when the credibility of the virtual store is questioned. Customers are disadvantaged if the vendor acts recklessly because he is unable to fulfill his duty to provide the requested product. Generally, in a transactional agreement, all rights and obligations begin with the agreement to trade and buy merchandise.(Djanggih, 2018) When selling goods online, the seller has the responsibility to deliver the goods to the client and provide accurate and honest information about the goods he sells.

In contrast, transactional agreements incur obligations. Merchants who use the internet to market and sell their goods are obliged to provide accurate and correct information about the goods they sell, as well as fulfill their delivery obligations to clients.(Djanggih, 2018, ibid) In addition, the merchant has the right to take care of his merchandise and get paid for the merchandise he sells. In order for the product to be safely sold and delivered to the customer, the buyer must pay for the goods he bought, which he bought from the merchant at a predetermined price. They also have a responsibility to truthfully disclose information about themselves, including names, addresses, and telephone numbers.

In the end, online fraud and convection will be defeated if buyers and sellers fulfill their obligations as stipulated in online transactions. Because internet fraud is threatened by article 138 of the Criminal Code and article 28 paragraph 1 of the ITE Law. (Naro et al., 2022)

Law Enforcement of e-Commerce Fraud in Indonesia

Law enforcement in Indonesia is currently experiencing difficulties in keeping pace with the rise of cybercrime. The rise in crimes involving e-commerce is indicative of this. According to Athifahputih, the lack of facilities and infrastructure, the low legal awareness of the public in eradicating information technology crimes, and the lack of law enforcement officers who have in-depth knowledge of information technology (internet) all contribute to law enforcement

challenges. In addition, there are still many law enforcement officials in areas who are digitally literate, so they are not ready to face an increase in criminal activity. Because, there are still many law enforcement agencies in places that do not have an Internet network.(Athifahputih, 2022)

Meanwhile, Perkasa, Nyoman, and Bambang provided clarifications based on the findings of the study on law enforcement barriers to e-commerce-based fraud, such as: (1) Digital Evidence. Due to the need for adequate infrastructure and capabilities, the search for digital evidence remains a challenge. (2) Dissent. Different views among law enforcement officials regarding the interpretation of cybercrime through articles published by the public, investigators, public prosecutors, and judges will have an impact on the final outcome of the case, causing legal ambiguity for victims seeking compensation. (3) Investigator expertise. Police investigators are still lacking, both in number and caliber. Therefore, police detectives need training in order to understand and be proficient in the methods used by cybercriminals. (4) Public Attention and Awareness. Currently, public awareness of the need to report cybercrime incidents to the authorities is still relatively small. Some people are reluctant to report it because they believe that a small financial loss can justify it. In addition, they believe that the cost of going to court will exceed the losses caused. To help law enforcement catch cyber criminals roaming in cyberspace, the public is still required to report every cybercrime incident to the authorities.(Perkasa, Serikat, & Turisno, 2016)

The ITE Law requires victims of online trading fraud to take legal action. Merchants can be sued as first defendants and virtual store suppliers as code defendants. Furthermore, in order to get payment for these sales services, the virtual store supplier must offer compensation.(Naro et al., 2022) According to Indonesia's procedural law, victims of internet fraud are allowed to attach evidence, which includes screenshots of mobile phone payments, emails, transcripts of dialogues, and other types of media. As business actors, all sellers have the responsibility to carry out their operations correctly and reliably, provide accurate, honest, and transparent information about the condition and warranty of goods, and make records of use, repair, and maintenance.(Wulandari, Husein, & Pulungan, 2020)

In addition, based on Indonesian Law No. 8 of 1999, virtual store providers remain liable for legal losses even if they claim or deny responsibility for any data transfers. Prosecution and prevention are two countermeasures taken by the authorities.(Fajar & Achmad, 2015) The National Police Binmas & Community Development Unit conducts socialization and community development as a preventive effort.

Information to the public against cybercrime should focus on educating the public about online transactions and precautions that need to be taken before engaging in any online activity. Likewise with all acts of oppression carried out by investigators on a case that can result in the prosecution of these unlawful acts.(Ekasari et al., 2019) To stop the occurrence of fraud crimes in the real world, the Indonesian government must also conduct socialization that supports the phrase "buyer beware". The slogan 'Buyer beware' serves to maintain and inform the wider community in conducting virtual transactions, namely about the validity of the transaction.

Cybercrime scams often require victims to make a statement to law enforcement regarding the true nature of the offense. Primary evidence in the form of electronic data or the manner in

which electronic data and information are published must be included in the report. From there, an investigation is carried out to ascertain the veracity of a type of fraud. Cybercrime investigations are carried out in accordance with the criminal procedural regulations of the ITE Law, in accordance with Article 42 which regulates procedural law regarding law in Indonesia.(Saleh, 2022) This burdens the overall policy, namely the criminal procedure laws and regulations and remains in effect if the provisions of the criminal procedure of the ITE laws and regulations are violated. Therefore, the ITE Law requires the existence of a "lex specialist" to determine which situations fall within a more specific scope in terms of data innovation and virtual business.

The Criminal Code does not recognize electronic books as everything that can be read. He admitted high evidence through article 184; That is, the only valid evidence is the testimony of witnesses, experts, and fraudsters.

The increasing modernity of cybercrime and widespread globalization have driven a growing urge to admit electronic evidence in court.(Jingga & Limantara, 2015) Therefore, the ITE Law in Indonesia, which regulates electronic information and transactions, seeks to provide a foundation for the receipt of electronic evidence. More specifically, printed findings or electronic data are evidence allowed according to article five paragraph one of the ITE Law. Electronic data is a collection of electronic data, including but not limited to writing, sound, images, telex, and perforations, which have been processed to give meaning to the person capable of interpreting them, in accordance with the general provisions of article 1. paragraph 4 of the ITE Law.

In addition, since hackers violate people's privacy and seek to rob them of the clarity of their pages, users who visit certain pages may find it annoying and impossible to remain on the site for long periods of time. Of course, as more and more people realize how often credit card fraud occurs on social networking sites, e-commerce takes a toll on it. Fortunately, Indonesia's Electronic Information and Transactions Law (UU ITE) has laid the foundation for innovation in the field of information and communication and electronic transactions. Before its adoption, there were no definite regulations governing electronic transactions. Electronic evidence is also allowed, making it more difficult to verify and apprehend offenders.(Siregar & Tenoyo, 2015) Since electronic evidence is now allowed in the criminal justice system, the Indonesian government's efforts to create legal certainty for justice have had a significant influence on the development of cybercrime law enforcement.(Ashoer, 2016) Therefore, those who are victims of cybercriminals have clear legal protections, and those who commit cyber-related crimes also have legal ties.

To be accepted as evidence in court, electronic data and documents must meet formal requirements. In accordance with article five paragraph four, there is no requirement that all electronic data and documents must be made by laws and regulations or in a notarial deed. However, as mentioned in article 16 of the ITE Law, electronic data and documents must be accessible, trustworthy, secure, verifiable, and trustworthy in order to be accepted in court.(Koto, 2021) One important technique to control whether or not electronic data or documents are accepted as digital evidence in court is digital forensic procedures. In general, cybercrime is

defined similarly to foreseeable crime. Collectively, such actions represent actions that violate policy values and are compensated with state approval.

In addition, people who use technology extensively tend to keep up with the latest online trends, which often results in crime. Cybercrimes were prosecuted under the Criminal Code, which provides a wider scope of crimes, prior to the introduction of Indonesia's electronic information and transactions law.(Koto, 2021) Although article 28 paragraph one of the policy that regulates criminal acts related to electronic transactions that harm customers does not specifically regulate fraud, the ITE Law regulates it.

Article 28 of the ITE Law Paragraph One stipulates that whoever intentionally and without permission spreads false and misleading information that causes customers to lose money through electronic transactions, is threatened with a maximum prison sentence of six years and a maximum fine of Rp. 1,000,000,000. This is because fraud carried out through electronic transactions provides false and misleading information that motivates perpetrators to take advantage while harming innocent victims.

Article 28 of the first paragraph of the ITE Law states that anyone who intentionally and without rights disseminates false and misleading data that results in customer losses in electronic transactions shall be punished with a maximum imprisonment of six years and a maximum fine of Rp1,000,000,000.(Chen, Razani, Roosmalati, & Eusy, 2017) This is because fraud carried out through electronic transactions offers incorrect and misleading data and is a motivation to benefit oneself while causing harm to innocent victims.

Conclusion

Fraud crimes in e-commerce in Indonesia are increasingly rife, along with technological advances and the increasing use of the Internet in buying and selling transactions. The large number of victims, especially women who are attracted to the various products offered online, shows that this crime is very detrimental. Perpetrators take advantage of the weaknesses of victims who do not understand information technology to launch their actions, such as creating fake websites, stealing account details, or hijacking social media accounts to attract buyers at very low prices. The impact of these actions is devastating and often difficult for victims who do not understand how to report crimes online or gather the necessary evidence.

Legal policies related to fraud crimes in e-commerce in Indonesia are based on applicable criminal law principles, namely ius poenale and danius puniend. Implementing these legal provisions is expected to create a safer and more trusted online business environment for all parties involved. E-commerce fraud is regulated in Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), which provides an important legal foundation in law enforcement against cybercrime. Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law are the basis for law enforcement against fraud in online transactions. Despite this, law enforcement still faces many obstacles, such as law enforcement officials' need to understand information technology, dissent in legal interpretation, and lack of public awareness and participation in reporting cybercrimes.

Effective law enforcement against e-commerce fraud crimes requires a collaborative effort between governments, law enforcement officials, and communities. The government needs to increase socialization regarding the security of online transactions and support the public to be more vigilant and careful. In addition, it is important to strengthen the capacity of law enforcement officials through specialized training related to cybercrime and information technology. Thus, law enforcement can run more effectively and provide better protection for victims of e-commerce fraud crimes.

References

Alkhairi, P., Purba, L. P., Eryzha, A., Windarto, A. P., & Wanto, A. (2019). The Analysis of the ELECTREE II Algorithm in Determining the Doubts of the Community Doing Business Online. Journal of Physics: Conference Series, 1255(1), 12010. https://doi.org/10.1088/1742-6596/1255/1/012010

Anwar, M. N., Erwiyanto, E., & Romadon, I. (2023). Penegakan Hukum Terhadap Tindak Pidana Pidana Penipuan Berbasis Transaksi Elektronik. Kedudukan Justice Collaborator Sebagai Saksi dan Tersangka Dalam Pidana Umum, 3(1), 1224–1233.

Ashoer, M. (2016). The Impact of Perceived Risk on Consumer Purchase Intention in Indonesia; A Social Commerce Study. Proceeding of the International Conference on Accounting, Management, Economics and Social Sciences (ICAMESS). Jakarta, Indonesia: Millenium Hotel,.

Athifahputih, P. Y. R. (2022). Penegakan Hukum Terhadap Penyebaran Berita Hoax Di Lihat Dari Tinjauan Hukum. Jurnal Hukum dan Pembangunan Ekonomi, 10(1), 64–77. https://doi.org/10.20961/hpe.v10i1.62843

Bestari, N. P. (2023). Korban Penipuan Ecommerce RI Makin Banyak, Cek Data Terbaru! Diambil 30 Mei 2024, dari CNBC Indonesia website: https://www.cnbcindonesia.com/tech/20230302140853-37-418315/korban-penipuan-ecommerce-ri-makin-banyak-cek-data-terbaru

Chen, L., Razani, F. Z., Roosmalati, M., & Eusy, W. Y. (2017). Attitudes Toward Online Shopping in Asian Emerging Markets: a Comparison on the Younger Generations in China and Indonesia. Journal of China Marketing, 6(2), 1–26.

Djanggih, H. (2018). The Phenomenon of Cyber Crimes Which Impact Children as Victims in Indonesia. Yuridika, 33(2), 212–231. https://doi.org/10.20473/ydk.v33i2.7536

Ekasari, R., Agustya, D., Yucha, N., Arif, D., Darno, Retnowati, D., … Puji Lestari, L. (2019). Effect of Price, Product Quality, and Service Quality on Customer Satisfaction on Online Product Purchases. Journal of Physics: Conference Series, 1175(1), 12287. https://doi.org/10.1088/1742-6596/1175/1/012287

Fajar, M., & Achmad, Y. (2015). Dualisme Penelitian Hukum. Yogyakarta: Pustaka Pelajar.

Fernando, E., Prabowo, Y. D., & Gatc, J. (2023). Literature Study E-Commerce: Background, Methods Development System, Trend Topic, and Features. Journal of Applied Research In

Computer Science and Information Systems, 1(1), 42–47. https://doi.org/10.61098/jarcis.v1i1.49

Gupta, S., Kushwaha, P. S., Badhera, U., Chatterjee, P., & Gonzalez, E. D. R. S. (2023). Identification of Benefits, Challenges, and Pathways in E-commerce Industries: An Integrated Two-Phase Decision-Making Model. Sustainable Operations and Computers, 4, 200–218. https://doi.org/10.1016/j.susoc.2023.08.005

Hidayat, S., Herman, Handrawan, Haris, O. K., Tatawu, G., & Fajar, N. (2023). Kebijakan Hukum Perlindungan Data Privasi dari Kejahatan Dunia Maya. Halu Oleo Legal Research, 5(3), 985–1002. https://doi.org/10.33772/holresch.v5i3.341

Hill, J. B., & Marion, N. E. (2016). Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. California: Praeger Security International.

Irwanda, F., Ferary, S. A., Kamila, S. A., & Soebari, B. F. K. (2022). Perancangan Sistem Informasi Penjualan UMKM Andin dan Tudung Saji Berbasis Website Menggunakan Metode Waterfall. KARYA: Jurnal Pengabdian Kepada Masyarakat, 2(3), 125–131.

Jingga, F., & Limantara, N. (2015). The Development of Indonesia Small Medium Enterprise(SME) Rating and Review Portal. International Journal of Multimedia and Ubiquitous Engineering, 10(3), 211–218. https://doi.org/10.14257/IJMUE.2015.10.3.20

Koto, I. (2021). Cyber Crime According to the ITE Law. International Journal Reglement & Society (IJRS), 2(2), 103–110. https://doi.org/10.55357/ijrs.v2i2.124

Naro, W., Syatar, A., Majdy Amiruddin, M., Haq, I., Abubakar, A., & Risal, C. (2022). Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia. International Journal of Criminology and Sociology, 9, 572–586. https://doi.org/10.6000/1929-4409.2020.09.56

Perkasa, R. E., Serikat, N. P., & Turisno, B. E. (2016). Perlindungan Hukum Pidana Terhadap Konsumen Dalam Transaksi Jual/beli Online (E-commerce) Di Indonesia. Diponegoro Law Journal, 5(4), 1–13. https://doi.org/10.14710/dlj.2016.13361

Putri, D. E., Sudarti, E., & Siregar, E. (2024). Tindak Pidana Penipuan Melalui Aplikasi Digital (Gagasan Pemikiran Pertanggungjawaban Oleh Bank). PAMPAS: Journal of Criminal Law, 5(1), 72–87. https://doi.org/10.22437/pampas.v5i1.31716

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. Jurnal Penelitian Hukum De Jure, 19(1), 31–52. https://doi.org/10.30641/dejure.2019.V19.31-52

Rantesalu, H. (2022). Penanggulangan Kejahatan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur. Janaloka, 1(2), 70–94.

Risald, R. (2021). Implementasi Sistem Penjualan Online Berbasis e-Commerce Pada Usaha UKM IKE Suti Menggunakan Metode Waterfall. Journal of Information and Technology, 1(1), 37–42. https://doi.org/10.32938/jitu.v1i1.1393

Rosário, A., & Raimundo, R. (2021). Consumer Marketing Strategy and E-Commerce in the Last Decade: A Literature Review. Journal of Theoretical and Applied Electronic Commerce Research, Vol. 16, hal. 3003–3024. https://doi.org/10.3390/jtaer16070164

Saleh, G. (2022). Juridical Analysis of the Crime of Online Store Fraud in Indonesia. Jurnal Hukum dan Peradilan, 11(1), 151–175. https://doi.org/10.25216/jhp.11.1.2022.151-175

Sari, E. P., Febrianti, D. A., & Fauziah, R. H. (2022). Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory. Deviance Jurnal kriminologi, 6(2), 153–168. https://doi.org/10.36080/djk.1882

Sefitrios, S., & Chandra, T. Y. (2021). The Process and Performance of Combating Cyber Crimes In Indonesia. SALAM: Jurnal Sosial dan Budaya Syar-i, 8(4), 975–986. https://doi.org/10.15408/sjsbs.v8i4.21795

Semerádová, T., & Weinlich, P. (2022). Achieving Business Competitiveness in a Digital Environment: Opportunities in E-commerce and Online Marketing. In T. Semerádová & P. Weinlich (Ed.), The Broad and Narrow Definition of E-Commerce (hal. 1–26). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93131-5_1

Siregar, S. V., & Tenoyo, B. (2015). Fraud Awareness Survey of Private Sector in Indonesia. Journal of Financial Crime, 22(3), 329–346. https://doi.org/10.1108/JFC-03-2014-0016

Sudoyo, W. (2023). Catatan Kominfo, Korban Penipuan Online Capai 130 Ribu pada 2022. Diambil 30 Mei 2024, dari Infopublik: Portal Berita Info Publik website: https://infopublik.id/kategori/nasional-sosial-budaya/715547/catatan-kominfo-korban-penipuan-online-capai-130-ribu-pada-2022

Sunardi, S., Fadlil, A., & Kusuma, N. M. P. (2022). Implementasi Data Mining dengan Algoritma Naïve Bayes untuk Profiling Korban Penipuan Online di Indonesia. Jurnal Media Informatika Budidarma, 6(3), 1562–1572. https://doi.org/10.30865/mib.v6i3.3999

Wulandari, Y., Husein, R., & Pulungan, A. H. (2020). Types of Speech Functions Used by Online Shopping Frauds. Linguistik Terapan, 17(3), 291–300. https://doi.org/10.24114/lt.v17i3.2245