Legal Brief, Volume 11, No 5, (2022), pp. 3095-3103
ISSN 1979-522X (Print)| 2722-4643 (Online)
Published by IHSA Institute (Institut Hukum Sumberdaya Alam)
DOI: 10.35335/legal

Analysis of Law Enforcement Related to the Fraud of Online Shopping Digital Payment System

Nabila Anisahaq[1], Kuswardani[2]
[1,2]Faculty of Law, Universitas Muhammadiyah, Indonesia

ARTICLE INFO

Article history:

Received Nov 4, 2022
Revised Nov 21, 2022
Accepted Dec 7, 2022

Keywords:

Criminal Acts;
Digital Payments
Fictitious Transactions;
Fraud;
Law enforcement.

ABSTRACT

In the internet world, the potential for criminals to commit crimes is very large and very difficult to catch. It is because between people who are in this virtual world are mostly fictitious or the identity of the person is not real. The perpetrators violate the rules and norms of applicable law to gain more profit and enrich themselves. Online business makes the scammers are easier to take crime action. This research is normative legal research through a normative juridical approach. The data used secondary data covering primary legal material. The case with the transaction mode using QRIS has a relationship between Article 28 paragraph (1) of the ITE Law and Article 378 of the Indonesian Criminal Code, as seen from the elements that regulate the act on the article. In addition, it is also related to Article 4 of the Consumer Protection Law regulates the rights of consumers (QRIS users), which if violated is threatened with imprisonment for a maximum of 5 (five) years or a fine of at most 2 billion rupiahs. Using the Criminal Procedure Code as a basis to prove the non-conventional crime is very difficult to prove it because of the limitations of valid evidence according to Article 184 of the Criminal Procedure Code. In order to be more precisely prove the guilt of a person who committed a crime in the land of cyber/internet, the special law that can be used in this case is the Electronic Information and Transaction (ITE) Law which can be used to prove one's guilt in its evidence.

ABSTRAK

Di dalam dunia Internet, potensi pelaku kejahatan melakukan kejahatan sangat besar dan sangat sulit untuk ditangkap karena antara orang yang ada di dalam dunia maya ini sebagian besar fiktif atau identitas orang per orang tidak nyata. Demi mendapatkan keuntungan dan memperkaya diri sendiri, para pelaku melanggar aturan dan norma-norma hukum yang berlaku. Bisnis secara online mempermudah para pelaku penipuan dalam melakukan aksinya. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan yuridis normatif. Data yang digunakan adalah data sekunder meliputi bahan hukum primer. Hasil penelitian menunjukan bahwa kasus dengan modus bertransaksi menggunakan QRIS memiliki keterkaitan antara Pasal 28 Ayat (1) UU ITE dan Pasal 378 KUHP, dilihat dari unsur-unsur yang mengatur perbuatan terhadap pasal tersebut. Dan juga Pasal 4 UU Perlindungan Konsumen mengatur Hak Konsumen (pengguna QRIS), yang jika dilanggar diancam dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp 2 miliar. Jika mengunakan KUHAP sebagai dasar untuk membuktikan kejahatan non konvensional tersebut sangat lah sulit untuk membuktikannya karena keterbatasan alat bukti yang sah menurut Pasal 184 KUHAP, untuk lebih tepatnya membuktikan kesalahan seseorang yang melakukan kejahatan diranah siber/internet maka undang-undang yang bersifat khususlah yang dapat digunakan dalam hal ini adalah UU ITE yang dapat digunakan untuk membuktikan kesalahan seseorang dalam pembuktian tersebut.

Corresponding Author:

Nabila Anisahaq,
Faculty of Law,

Universitas Muhammadiyah,
Ahmad Yani, Pabelan, Kartasura, Indonesia
E-mail: nabilaanisa44@gmail.com

I. INTRODUCTION

Nowadays, advances in information and communication technology make it easier for people to provide and receive any kind of information (Azizah Mutiara, 2020). People can easily communicate without distance, space, and time boundaries. Along with the development of technology, people are also required to be able to follow every development that is happening. The development of technology today is not only for the sake of establishing communication and socializing but also leads to a World Business Network Without Borders. Business Network in question is trading activities online through the internet (Nugraha, 2018).

Trading activities by utilizing the internet media is known as electronic commerce, or abbreviated e-commerce (Deans et al., n.d.). It is a business activities involving consumers, manufacturing, service providers, and intermediary traders using computer networks. E-Commerce can also be understood as a process of buying and selling goods and services carried out through a computer network that is the internet (Tamilarasi & Elamathi, 2020).

The use of e-commerce in transactions can be done quickly, easily, and at a lower cost (Prasetyo, 2018). Business transactions between countries that usually spend several days in a conventional business can be shortened to a few minutes using internet services. In its implementation, there is no delay as a result of constraints thereby reducing the possibility of making mistakes in typing, which allows getting more information about the business so as to support the effectiveness and efficiency of a company or business (Ahmad et al., 2018).

Latest report from PPRO Financial. Ltd. which is the world's leading payment services company on payments and e-commerce stated that Indonesia has the highest growth reaching 78% per year. Other countries for the top five highest growth markets were Mexico 59%, Philippines 51%, Colombia 45%, and United Arab Emirates (UAE) 33%. Meanwhile, according to the data from the Investment Coordinating Board (BKPM), the value of investment in the e-commerce sector reached more than US$ 5 billion, making it one of the most strategic economic sectors (Kesuma et al., 2020).

Currently, the crime that occurs can not be categorized as physical crime, but crime is also experiencing development along with the flow of modernization of life. Online business has become a trend today, but it opens the reproach for parties who are not responsible for committing a crime that causes harm to others. In the internet world, the potential for criminals to commit crimes is very large and very difficult to catch. It is because people who are in this virtual world are mostly fictitious or the identity of the person is not real. The perpetrators violate the rules and norms of applicable law to gain more profit and enrich themselves. Online business makes the scammers are easier to take crime action.(Sundari, 2019; Ulum, 2020) Indonesia is one of the fastest growing e-commerce markets in the world. However, there is a high fraud rates, with an average of 25 percent of Indonesians having experienced fraud through various e-commerce and services (Liliana Sanchez et al., 2020; Rahmad, 2019).

Fraud with the mode of selling via the internet on the market makes many people interested in buying it. Although online business fraud has been partially exposed, but the prosecution of individuals against these actions is suspected that many have not reached the legal realm. This is because victims of online fraud are reluctant to report to law enforcement, and this type of fraud is still categorized as an ordinary offense (Arifin, 2019).

The lack and unclear of law enforcement firm on the perpetrators of online business fraud is often a trigger for this fraud to be occur. In addition, the author found that the basis of the legal issues are only two rules, namely through Article 378, which states that "Anyone with the intent to benefit themselves or others against the law, by using fake names or dignity, by deception or by a series of lies moves someone to hand something to him, or to give debt or write off receivables, is threatened by fraud with imprisonment of 4 years" and also the Article 28 paragraph (1) which states that "Everyone intentionally, and without the right to spread hoax and misleading news that results in consumer losses in electronic transactions" which provides legal sanctions on the perpetrators of this fraud (Wahyuning Ismoyo, 2014).

II. RESEARCH METHOD

This research is normative legal research through a normative juridical approach. The data used secondary data covering primary legal materials consisting of: the Constitution of the Republic of Indonesia year 1945, the Criminal Code (KUHP), the Criminal Procedure Code (KUHAP), Law Number 19 the year 2016 on Amendments to Law Number 11 the year 2008 on Information and Electronic Transactions as well as other legislation. In addition, secondary legal materials were also used which include the opinions of criminal law experts contained in literature, journals, and articles both in printed and in electronic form. This study also employed tertiary legal materials which include legal dictionaries and legal encyclopedias on fraud through fictitious transactions in the use of QRIS as an online shopping digital payment system. The data were obtained through the study of literature and then analyzed by qualitative analysis methods with descriptive parsing (exposure).

III. RESULTS AND DISCUSSIONS

Law Enforcement on Fraud Criminal Acts through Fictitious Transactions in the Use of QRIS as an Online Shopping Digital Payment System

Law enforcement can be formulated as an effort to implement the law as it should be, observe its implementation so that there is no violation, and if there is a violation, it needs to restore the violated law to be re-enforced. The definition of law enforcement in a narrow sense is an action activity on any violation or deviation from legislation through the criminal justice process involving the role of police officers, prosecutors, advocates or lawyers, and judicial bodies. Meanwhile, in a broad sense, it is an activity to implement and apply the law and take legal action on any violation of the law committed by the subject of the law either through judicial procedures or through arbitration procedures and other dispute resolution mechanisms (alternative disputes or conflict resolution). Law enforcement is closely related to compliance for users and implementers of legislation. In this case both the public and state officials, namely law enforcement (Muhlashin, 2021).

Law enforcement is an effort that aims to improve order and legal certainty in society. This situation can be done by regulating the functions, duties, and authorities of institutions in charge of enforcing the law according to the proportion of their respective scope, and based on a good cooperation system and supporting the goals to be achieved (Hasaziduhu Moho, 2019). The main purpose of law enforcement is to realize a sense of justice, legal certainty, and benefit in society. In its process, it must reflect aspects of legal certainty and order. Law enforcement is also required the moral elements, the moral relationship with law enforcement that determines a success or failure in law enforcement as expected by the purpose of law. Furthermore, the moral and ethical aspects of criminal law enforcement is a matter related to criminal law enforcement that is a process of discovery of facts, impartial (impartial) and full of resolution or problem solving and must be done fairly and appropriately(Agiyanto, 2018).

The law regulates society properly and usefully by establishing what is required, what is allowed and/or vice versa. Thus, the law draws a line between what is in accordance with the law and what

is against compared to what is the law (which is normatively interpreted as what should be), it is against the law that is actually more of a concern than law enforcement itself. Therefore, it can be stated that law enforcement (especially criminal law) is a reaction to an unlawful act. The efforts of state apparatus in addressing an act against the law and addressing other law enforcement issues are the core law enforcement discussion (HR, 2021).

Criminal law enforcement is currently an urgent need for fundamental changes in order to achieve the goal of a better and humane criminal. This need is in line with the strong desire to be able to realize a fairer law enforcement on every form of criminal law violation in the reform era. In this era, there is a great need for openness, democracy, human rights protection, law enforcement and justice/truth in all aspects of social life, nation, and state. In addition, the pattern of interaction and development of life in today's society is growing or changing very quickly followed by technology that is also growing rapidly so that the existing positive law is expected to also be able to follow existing developments and provide legal certainty for all communities. It is also understood that the level of society development where the law is enforced in fact affects the pattern of law enforcement, because in modern society that is rational and has a high level of specialization and differentiation so that the organization of law enforcement is also required to accommodate the existing problems (Suyanto, 2018).

Related to this research, law enforcement on fraud through fictitious transactions in the use of QRIS as an online shopping digital payment system, seems to be still based on existing positive laws (Criminal Code and laws that specifically regulate it) but in its implementation the use of the rule of law is still not maximized because based on the data previously submitted has increased. Therefore, the author wants to explore more deeply related legal rules that can ensnare the perpetrators of online-based fraud (Rahmad, 2019).

In a juridical sense, the definition of fraud is included in the formulation of criminal acts contained in the Criminal Code. However, the formulation of fraud in the criminal code is not a definition but only to establish the elements of an act so that it can be stated to be fraud and punish the perpetrators. Article 378 states that “Anyone who, with the intention of benefiting himself or others against his rights, using a fake name or fake character or using deception or false wording, moves another person to hand an object or enter into a debt agreement or to cancel a receivable, by mistake having committed fraud, shall be punished by imprisonment for a term of four years (Arifin, 2019).

Fraud that occurs in cyberspace today can be done in various ways, ranging from simple to complex ways. Fraud in a simple way for example by sending false news or acting as someone else illegally and committing fraud via the internet. On the other hand, fraud in the complex way can be seen from the workings of the perpetrators who are grouped or have a network. Regarding this condition, the regulation of fraud in the Criminal code is felt to find limitations in accommodating sanctions or punishment for the action (Prasetyo, 2018). Criminals commit fraud on computer systems. Second, the series of criminal act offenders is difficult to be categorized into the ways set forth in the Criminal Code because as mentioned earlier, the ways set forth in the Criminal Code addressed to the person not to the computer system (Rahmad, 2019).

The determination of a person to be declared as a perpetrator of online fraud must at least fulfill all the elements of the crime and the purpose of the act can be proven that it was deliberately carried out in a state of awareness of the denunciation of the act by law. Although the elements in Article 378 of the Criminal Code are fully fulfilled, there are elements of online fraud that are not met in the regulation of Article 378 of the Criminal Code.

Providing legal certainty and enforcing the law on online-based fraud crimes, the Government of Indonesia issued Law Number 11 of 2008 concerning Electronic Information and Transactions (”UU ITE"), which was later amended by Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions ("UU 19/2016") (Harahap &

Maharani, 2020). As a special law (*Lex Specialist Derogat Lex Generale*), the Electronic Information and Transaction Law can at least be a guideline and legal basis for community members in their activities in cyberspace. In addition, the Electronic Information and Transaction (ITE) Law also has a connection to several articles regulated in the Criminal Code which aims to facilitate case resolution. Given the challenges and demands of global communication development, the law is expected as ius constituendum which is legislation accommodating to the development and anticipatory to the problems, including the negative impact of advances in information technology that has a broad impact on society (Setiawan, 2021).

Cyber Crime Regulation (cybercrime) in the Electronic Information and Transaction (ITE) Law and other laws contain implications of the legal protection of electronics and computer systems or electronic systems that are protected and not public, both private and state property and other legal interests, such as wealth, honor, decency, state security, and others that can be the target object or object of cybercrime (Siregar, 2021). Related to the legal protection provided by the current ITE Law, it is also felt that it does not directly regulate conventional fraud crimes or online fraud crimes. However, related to the fraud definition that has an impact on the victim's losses in electronic transactions, there are provisions governing these losses in Article 28 paragraph (1) of the ITE Law which states that “Everyone intentionally, and without the right to spread fake and misleading news that results in consumer losses in electronic transactions”. The elements in Article 28 paragraph (1) of the ITE Law are identical and have some similarities to conventional fraud crimes regulated in Article 378 of the Criminal Code and have special characteristics, namely the recognition of evidence, electronic media, and the expansion of jurisdiction in the ITE Law (Harahap & Maharani, 2020).

The formulation of the elements contained in Article 28 paragraph (1) of the ITE Law and Article 378 can be understood to regulate different objects. Article 378 of the criminal code regulates fraud, while Article 28 paragraph (1) of the ITE Law regulates fake news that causes consumer losses in electronic transactions. However, the two articles have similarities, which can result in harm to others (Harahap & Maharani, 2020).

Regulation regarding the spread of fake and misleading news is understood to be very necessary in order to protect consumers who conduct commercial transactions electronically or online. Electronic trading can ideally be carried out easily and quickly so that the transaction process must be based on trust between the parties to the transaction. This trust is assumed to be obtained if the parties that have transaction know each other based on the experience of previous transactions or the results of discussions directly before the transaction is made. Although not regulated in detail but the principles in e-commerce implicitly regulate the principles of contract in an electronic transaction.

Providing maximum protection and law enforcement, the provisions of Article 28 paragraph (1) of the ITE Law are also in accordance with Law Number 8 of 1999 concerning Consumer Protection which aims to increase awareness and independence of consumers to protect themselves and create a system of protection for consumers by providing legal certainty and information disclosure and access to information.

Related to law enforcement on online-based fraud crime, the focus of Consumer Protection is on Article 4 points C and H, which state that consumers have the right to obtain accurate, transparent, and honest information about the conditions and guarantees of goods and/or services and are entitled to compensation, and/or replacement if the goods and/or services received are not in accordance with the agreement or not as they should.

A derivative of the ITE Law, Article 49 Paragraph (1) of Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) also provides protection to consumers by affirming that business actors who offer products through electronic systems must provide complete and correct information related to contract terms, manufacturers, and products offered. It is further emphasized that business actors are obliged to provide clarity of

information about contract offers or advertisements. If the goods received are not in accordance with the agreement Article 49 paragraph (3) Government Regulation of Operation and Electronic System and Transaction (PSTE) also regulates specifically about this, which states that “business actors are obliged to give a time limit to consumers to return goods sent if they are not in accordance with the agreement or there are hidden defects (Setiawan, 2021).

Electronic documents that can be used as the evidence must be documents that can be maintained authenticity and accounted for the truth, electronic documents are very easy to manipulate so that not all electronic documents can be used as evidence. In Article 6 of the ITE Law states that " electronic information and/or electronic documents are considered valid as long as the information contained therein can be accessed displayed, guaranteed integrity, and can be accounted for so as to explain a situation. In the ITE Law, it is regulated that electronic information/electronic documents and/or printed results are valid legal evidence, and an extension of valid evidence in accordance with the applicable procedural law in Indonesia. The expansion in question is the recognition of information and/or electronic documents and their printouts as valid evidence in court, so that now the its evidence has increased by one that previously did not exist (Siregar, 2021).

Science and technology development apparently not only provides the dynamics of the development of human civilization but also has an impact on the emergence of new dimensions of crime, including cybercrime. In line with this, the development of legal science must also be able to reach it as an effort to overcome and ensure order in society. In a legal perspective, this effort is realized through criminal law. Handling the development of criminal acts of cybercrime seen in the implementation of juridical to determine law (jurisdiction to enforce) based on Indonesian criminal law through Laws of Electronic Information and Transaction (ITE). Therefore, in order to enforce the law, law enforcement officers should use the ITE Law as a complement to the criminal code that has existed so far. It can be understood that the purpose of making laws and regulations and policy-making is essentially an integral part of efforts to protect the Community (social Defense) and efforts to achieve public welfare (social welfare) (Aminah, 2020).

In addition, from the point of view by criminal policy, crime prevention efforts on online-based fraud are no longer carried out solely partially with criminal law (penal facilities), but must also be taken with an integral/ systematic approach through special laws. As a form of high-tech crime that can also transcend national borders (transnational/transborder) is common that the countermeasures of cybercrime must also be noted through the technology approach (techno prevention). The formation of the Electronic Information and Transaction Law that regulates cybercrime must still be followed up with various efforts so that the ITE Law is effective for perpetrators and the community. Adequate infrastructure and capabilities of law enforcement officers in the field of information and communication technology are also very important in preventing and combating these crimes (Rahmad, 2019).

Related to law enforcement, an important material in the Electronic Information and Transaction Law is the recognition of the expansion of valid evidence in accordance with the applicable procedural law in Indonesia. The expansion in question is the recognition of information, documents, and electronic signatures as evidence. This means that there is now one more piece of evidence that can be used in court. Information and electronic documents as well as electronic signatures that are part of it can be valid evidence as confirmed in Article 5 Paragraph (1) of the Electronic Information and Transaction (ITE) Law. Juridical recognition through Article 5 Paragraph (1) of the ITE Law on electronic evidence actually has a juridical effect on the recognition of electronic evidence as part of the valid evidences. Recognition of electronic evidence is a step forward in the law of evidence. If there is a civil case that disputes an electronic document in the form of an electronic contract, then its document can be used as a reference for the parties to resolve the case or the judge who will decide the case (Harahap & Maharani, 2020).

In terms of handling cybercrime cases, especially electronic transaction fraud, it is necessary to specialize the investigative apparatus which can be considered as one of the ways to carry out law enforcement efforts on cybercrime. The specialization starts from the existence of education that is directed to master the technical as well as the basics of knowledge in the field of computer technology. This is also confirmed through Article 43 of the ITE Law which states that "Besides the Investigators of Police Officials of the Republic of Indonesia, certain Civil Servants within the government area whose scope of duties and responsibilities in the field of Information Technology and Electronic Transactions are given special authority as investigators as referred to in the Law on Criminal Procedure".

In the end to ensnare the perpetrators of online-based crimes, the legal basis that can be given is Article 378 of the Criminal Code. However, Article 378 of the Criminal Code of the crime of fraud can not be used to burden the perpetrators of online fraud to account for their actions because there are some obstacles in burdening criminal sanctions, such as obstacles in the evidence where it is limited by the Criminal Procedure Code. Therefore, to strengthen the legal basis, it can be added to Article 28 paragraph (1) in conjunction with Article 45 paragraph (2) of the Electronic Information and Transaction (ITE) Law. Article 28 paragraph (1) the ITE Law can only be used in online fraud crimes that are characterized by online buying and selling activities, while Article 378 of the Criminal Code can only be used to ensnare perpetrators of conventional fraud, in other words, Article 28 paragraph (1) the ITE Law is a lex specialist from Article 378 of the Criminal Code which is a lex generalis of fraud crimes.

Barriers in Law Enforcement on E-commerce-based Criminal Acts

Law enforcement in Indonesia is currently allegedly experiencing difficulties in dealing with the outbreak of cybercrime. This can be reflected in the increasing number of online-based criminal acts that can be seen in the introduction in this paper.

Law enforcement is motivated by the lack of law enforcement officers who understand the ins and outs of information technology (internet), limited facilities and infrastructure, as well as the lack of public legal awareness in an effort to counter criminal acts of information technology. In addition, law enforcement officers in the region area were not ready to anticipate the rise of this crime because there are still many law enforcement officers who stutter technology (*gaptek*). This is caused by many law enforcement institutions in the area with unsupported internet networks.

Article 28 paragraph (1) of the ITE Law states that "Any person intentionally, and without the right to spread fake and misleading news that results in consumer losses in electronic transactions." Meanwhile, the Article 378 of the Criminal Code states that "Anyone who with the intent to benefit themselves or others unlawfully, by using a false name or false dignity, by deception, or a series of lies, move others to deliver something to him, or to give debt or write off receivables, threatened with fraud with imprisonment for a maximum of four years (Alweni, 2019).

From the formulations of Article 28 paragraph (1) UU ITE and Article 378 Indonesian Criminal Code, both of them regulate different things. Article 378 of the criminal code regulates fraud, while Article 28 paragraph (1) of the ITE Law regulates fake news that causes consumer losses in electronic transactions. The formulation of Article 28 paragraph (1) UU ITE does not require an element of benefiting oneself or others as stipulated in Article 378 of the Criminal Code on fraud so that in the evidence it is felt that there are still difficulties or even multiple interpretations for law enforcement officers to ensnare perpetrators of online-based fraud (Siregar, 2021; Tolstoy et al., 2021).

Infrastructure factor is one of the weak factors of law enforcement on its fraud. For example, computer facilities available today only function as administrative activities, while e - commerce-based crimes are carried out using networked computers and high technology capacity and are complicated so that law enforcement officers are still finding it difficult to track, detect, or compensate

for the activities of the perpetrators of these crimes. The same thing can also be seen in the lack of ability and skills of law enforcement officers in the field of computers, which resulted in tactical, technical investigation, prosecution, and examination in court that is not controlled because it involves the existing system in the computer (Rahayu & Day, 2017).

The community factor is felt to be an obstacle in law enforcement on e-commerce-based fraud crimes where there are still many people who are reluctant to report fraud crimes, causing difficulties for law enforcement officers to take action against the perpetrators of these crimes. Another factor that is felt by the community is that when the problem is brought to the court process, it is assumed that it will require greater funds during the procedure compared to the losses suffered. Cultural factors are allegedly also the cause of weak law enforcement on e-commerce-based fraud crimes. When people try to communicate with people in different cultures and better adjust their differences, it proves that culture can be learned. However, culture does not always provide positive behavior for humans, but it can also cause negative behavior (Susanto, 2016).

IV. CONCLUSION

The case with the transaction mode using QRIS has a relationship between Article 28 paragraph (1) of the Electronic Information and Transaction (ITE) Law and Article 378 of the Indonesian Criminal Code, as seen from the elements that regulate the act against the article. In addition, it is also related to Article 4 of the Consumer Protection Law regulates the rights of consumers (QRIS users), which if violated is threatened with imprisonment for a maximum of 5 (five) years or a fine of at most 2 billion rupiahs. Using the Criminal Procedure Code as a basis to prove the non-conventional crime is very difficult to prove it because of the limitations of valid evidence according to Article 184 of the Criminal Procedure Code. In order to be more precisely prove the guilt of a person who committed a crime in the land of cyber/internet, the special law that can be used in this case is the ITE Law which can be used to prove one's guilt in the proof. Law enforcement in Indonesia is currently experiencing difficulties dealing with the spread of cybercrime. This can be reflected in the increasing crime of internet-based fraud.

Reference

Agiyanto, U. (2018). Penegakan Hukum di Indonesia : Eksplorasi Konsep Keadilan Berdimensi Ketuhanan. *Hukum Ransendental*, *4*.

Ahmad, D., Ariessanti, H. D., & Awaliyah, K. (2018). Implementation of E-Commerce Website to Increase Online Sales of Case Study of Baby Wise BSD Tangerang. *Aptisi Transactions on Management (ATM)*, *1*(1), 11–16. https://doi.org/10.33050/atm.v1i1.680

Alweni, M. K. (2019). Kajian Tindak Pidana Pemerasan Berdasarkan Pasal 368 KUHP. *Jurnal Lex Crimen*, *8*(3).

Aminah, S. (2020). *Pelecehan Seksual Non Fisik: Kejahatan Yang Tidak Dihukum*. Bahasan.Id.

Arifin, R. (2019). Penegakan Hukum Tindak Pidana Penipuan Secara Online Berdasarkan Pasal 378 Kuhp. *Dinamika: Jurnal Ilmiah Ilmu Hukum*, *25*(4).

Azizah Mutiara, V. (2020). Teknologi Informasi Komunikasi dan Perkembangannya. *Teknologi Informasi Komunikasi Dan Perkembangannya*, *1*(Perkembangan pada TIK).

Deans, P. C., Press, I. R. M., & Rossi, M. (n.d.). *E-Commerce and Technologies* (J. Travers (ed.)). IRM Press Publisher of innovative scholarly and professional information technology titles in the cyberage.

Harahap, I. R., & Maharani, D. (2020). Penerapan dan Pandangan Keagamaan Terhadap Undang-Undang ITE di Indonesia. *Journal of Social Responsibility …*, *1*(1).

Hasaziduhu Moho. (2019). Penegakan Hukum di Indonesia Menurut Aspek Kepastian Hukum, Keadilan, dan Kemanfaatan. *Universitas Dharmawangsa*, *13*(1).

HR, M. A. (2021). Lemahnya Penegakan Hukum Di Indonesia. *JISH: Jurnal Ilmu Syariah Dan Hukum*, *3*(1). https://doi.org/10.36915/jish.v3i1.16

Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Penipuan Melalui Media Elektronik. *Jurnal Preferensi Hukum*, *1*(2). https://doi.org/10.22225/jph.1.2.2345.72-77

Liliana Sanchez, A., Mustaqim, M., & Satory, A. (2020). Interpretasi Hukum Perkara Penipuan Online Modus Investasi Kajian Undang-Undang No.42/2009 dan Undang-Undang No25/2007. *Borneo Law Review*, *4*(2). https://doi.org/10.35334/bolrev.v4i2.1714

Muhlashin, I. (2021). Negara Hukum, Demokrasi dan Penegakan Hukum di Indonesia. *Jurnal Al-Qadau; Peradilan Dan Hukum Keluarga*, *4*(1).

Nugraha, D. (2018). Transformasi Sistem Revolusi Industri 4.0. *Workshop Technopreneurship Road to TBIC 2019*, *1*(30 September 2018).

Prasetyo, R. D. (2018). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia. *Hukum Dan Masyarakat Madani*, *8*(1).

Rahayu, R., & Day, J. (2017). E-commerce adoption by SMEs in developing countries: evidence from Indonesia. *Eurasian Business Review*, *7*(1). https://doi.org/10.1007/s40821-016-0044-6

Rahmad, N. (2019). Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online. *Jurnal Hukum Ekonomi Syariah*, *3*(2).

Setiawan, M. N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3) dilihat dari Sosio-Politik Hukum Pidana Indonesia. *DATIN Law Jurnal*, *3*.

Siregar, E. Y. (2021). PENGARUH KOMUNIKASI DAN KEBIJAKAN UU ITE TERHADAP TINDAK PIDANA PENIPUAN JUAL BELI BARANG ONLINE DI INSTAGRAM. *EKSEKUSI*, *3*(1). https://doi.org/10.24014/je.v3i1.12592

Sundari, C. (2019). Revolusi Industri 4.0 Merupakan Peluang Dan Tantangan Bisnis Bagi Generasi Milenial Di Indonesia. *Prosiding SEMINAR NASIONAL DAN CALL FOR PAPERS*, *Fintech dan E-Commerce untuk Mendorong Pertumbuhan UMKM dan Industri Kreatif*.

Susanto, A. (2016). Analisis Kondisi Digital Poverty di Indonesia. *Jurnal Penelitian Pos Dan Informatika*, *6*(2). https://doi.org/10.17933/jppi.2016.060204

Suyanto. (2018). Pengantar Hukum Pidana. *Deepublish*.

Tamilarasi, R., & Elamathi, N. (2020). E-COMMERCE- BUSINESS- TECHNOLOGY- SOCIETY. *International Journal of Engineering Technologies and Management Research*, *4*(10). https://doi.org/10.29121/ijetmr.v4.i10.2017.103

Tolstoy, D., Nordman, E. R., Hånell, S. M., & Özbek, N. (2021). The development of international e-commerce in retail SMEs: An effectuation perspective. *Journal of World Business*, *56*(3). https://doi.org/10.1016/j.jwb.2020.101165

Ulum, M. (2020). Prinsip-Prinsip Jual Beli Online dalam Islam dan Penerapannya pada e-Commerce Islam di Indonesia. *Jurnal Dinamika Ekonomi & Bisnis*, *17*(1). https://doi.org/10.34001/jdeb.v17i1.1115

Wahyuning Ismoyo, D. (2014). Kendala Penyidik Dalam Mengungkap Tindak Pidana Penipuan Online Melalui Media Elektronik Internet (Studi di Polres Malang Kota). *Jurnal Hukum*.