
**ANALYSIS OF CRIMINAL SANCTIONS ON PERPETRATORS OF
ONLINE BUYING AND SELLING FRAUD****¹Bella Monica Rahma Hamida, ^{2*}Normalita Destyarini**

Universitas Duta Bangsa Surakarta, Surakarta, Indonesia

normalita_destyarini@udb.ac.id

DOI:

Submit: 20-Februari-2023

Diterima: 20-Maret-2023

Dipublikasikan 30-Mei-2023

Abstract

Online buying and selling fraud, commonly referred to as e-commerce fraud, is a prevalent criminal activity that involves deceiving individuals for financial gain through fraudulent online transactions. This form of fraud encompasses various practices, including non-delivery of goods, sale of counterfeit products, identity theft, and phishing schemes. To combat this issue, legal systems impose criminal sanctions on individuals involved in online buying and selling fraud. The analysis of these criminal sanctions reveals that they aim to deter and punish perpetrators while providing restitution to victims. The specific nature and severity of sanctions differ across jurisdictions, as they are influenced by the legal framework, cybercrime legislation, and consumer protection laws of each country. Understanding the range of criminal sanctions is crucial in developing effective measures to prevent and address online buying and selling fraud in a globalized digital landscape. In this era of technological advancement, people prefer to buy things online. But with the development of technology, the idea of crime by unscrupulous actors has also developed. One example is the criminal act of fraud. Fraud is a condition carried out by anyone with the intention of benefiting them selves or others unlawfully. Then the method used to conduct this research is the normative method. The type of data used in this research is secondary data. This secondary data is obtained by researchers from other research results, journals, books, and other sources that are collected and compiled so that they can solve cases.

Keywords Online buying and selling fraud, Criminal sanctions, Perpetrators**Abstrak**

Penipuan jual beli online, umumnya disebut sebagai penipuan e-niaga, adalah aktivitas kriminal umum yang melibatkan penipuan individu untuk keuntungan finansial melalui transaksi online penipuan. Bentuk penipuan ini mencakup berbagai praktik, termasuk tidak terkirimnya barang, penjualan produk palsu, pencurian identitas, dan skema phishing. Untuk mengatasi masalah ini, sistem hukum memberlakukan sanksi pidana terhadap individu yang terlibat dalam penipuan jual beli online. Analisis sanksi pidana ini mengungkapkan bahwa mereka bertujuan untuk menakut-nakuti dan menghukum pelaku sekaligus memberikan restitusi kepada korban. Sifat khusus dan tingkat keparahan sanksi berbeda di seluruh yurisdiksi, karena dipengaruhi oleh kerangka hukum, undang-undang kejahatan dunia maya, dan undang-undang perlindungan konsumen di setiap negara. Memahami berbagai sanksi pidana sangat penting dalam mengembangkan langkah-langkah efektif untuk mencegah dan mengatasi penipuan jual beli online dalam lanskap digital global. Di era kemajuan teknologi ini, orang lebih suka membeli barang secara online. Namun seiring berkembangnya teknologi, ide kejahatan oleh oknum juga berkembang. Salah satu contohnya adalah tindak pidana penipuan. Penipuan adalah suatu keadaan yang dilakukan oleh seseorang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Maka metode yang digunakan untuk melakukan penelitian ini adalah metode normatif. Jenis data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder ini diperoleh peneliti dari hasil penelitian lain, jurnal, buku, dan sumber lain yang dikumpulkan dan disusun sehingga dapat memecahkan kasus.

Kata kunci: Penipuan Jual Beli Online, Sanksi Pidana, Pelaku**INTRODUCTION**

In this increasingly advanced life, society is increasingly helped by the existence of e-commerce. e-commerce itself stands for electronic commerce which means a buying and selling activity or trading activity that utilises technology as a place to trade. or trading activities that utilise technology as a place with the advancement of technology in society that makes buying and selling done online. society that makes buying and selling done online,

not a few are also crime is committed. this is no longer uncommon in our society. One example of crime is fraud.

Currently, crimes that occur cannot be categorised as physical crimes, but crimes today are also evolving. as physical crimes only, but crimes today have also developed in line with the modernisation of life. along with the modernisation of life. Wahidi and Labib said that "Online business online business has become a trend now a days, but it opens a flaw for irresponsible parties to commit a crime that cause sirresponsible parties to commit a crime that causes harm to others". harm to others"

According to Article 378 of the Criminal Code, the offence of deception is a condition committed by any person with intent to unlawfully benefit themselves or others, by using a false name or dignity or another person unlawfully, by using a false name or false dignity, by deceit, or by a series of lies, moves the person false name or dignity, by deceit, or by a series of lies, moves another person to hand over something to him. to hand over something to him. According to R. Sugandhi, fraud is a person's action by deceit, a series of lies, a false name, a false situation with the intention of benefiting himself. false name, false circumstances with the intention of benefiting themselves with no rights.

Police Headquarters revealed that during the period of September to December 2017 the total amount of losses of people who have made online transactions through e-commerce services reached Rp 2.2 billion. online transactions through e-commerce services reached Rp 2.2 billion.¹⁵ Kasubdit II Directorate of Cyber Crime at the National Police Headquarters, Commissioner of Police, Asep Safruddin, recognised the activities of people who shop online. Safruddin recognised that online shopping is becoming a trend in Indonesia. is becoming a trend in Indonesia. However, according to him, this is in line with the high level of crime that is getting bigger against people who doing online shopping. A clear example is the case of fraud in Tanjung Selor, North Kalimantan through Facebook. the incident occurred on 30 December 2022. 2022 the victim saw a post of a car for sale in the Facebook group buying and selling cars in the Berau region. group, then the victim communicated with the Facebook account that posted an advert for a 2008 Honda Jazz car. who posted an advert for a 2008 Honda Jazz car and the account included a mobile phone number. The account included a mobile phone number. Subsequently, the victim contacted the number using her personal WhatsApp. using his personal WhatsApp. Finally, in the WA conversation the victim was sent some photos of the car and ID card to convince the victim. After the victim was interested, the victim invited the suspect to meet with the victim's brother in Tanjung Selor. However, the suspect asked for operational money to go to Tanjung Selor. The victim sent funds totalling Rp 2,800,000 to the MNC bank account under the name of Pranciskus Ola for operational purposes. in the name of Pranciskus Ola for operational purposes. However, the suspect did not go to Tanjung Selor but to Tana Tidung with the reason that the suspect delivered the unit to the customer in Tana Tidung. unit to the customer in Tana Tidung. The suspect then sent another photo of a Toyota Calya car to the victim and said that the unit was in Tarakan. unit was in Tarakan. The victim told the victim's friend to check according to the address given by the suspect. the address given by the suspect. After checking the car was available and because the victim received information from the victim's friend that the car existed, then the victim contacted the suspect again and sent Rp 30,000,000 twice to the same account. twice to the same account. After transferring the victim's number was blocked by the suspect. The suspect's mode of opening a bank account using online banking service features, by entering ID card data and scanned photos of the victim's face. Then the suspect looks for car posts that are sold by the original owner of the car. of the car. After getting a photo of the car in a Facebook post the suspect took it and posted it to another

Facebook buying and selling group with a much cheaper price. with a much cheaper price. With the description above, the author makes the title "analysis of criminal sanctions on perpetrators of online buying and selling fraud".

METHODS

This type of research is normative research. According to Peter Mahmud Marzuki, normative legal research is a process to find legal rules, legal principles, and legal doctrines to answer the legal issues at hand. It is said to be doctrinal, because this research is carried out only on written regulations or other materials. The approach used is a case approach. The object of study of this case approach is the court's consideration to arrive at a decision. Which will be a reference for compiling arguments to solve cases.

The type of data used in this research is secondary data. This secondary data is obtained by researchers from other research results, journals, books, and other sources that are collected and compiled so that they can solve cases .

In this study using data sourced from other research results, books, journals, laws, and other sources that will be compiled so as to produce the data needed in the study.

Data analysis is the process of processing data with the aim of finding information that can be used as a basis for making decisions for the solution of a problem raised. The conclusion in this research uses a qualitative normative method. Using normative because of how to examine library materials. Using qualitative methods because it focuses on in-depth observations.

RESULT

The government created legislation related to the use of technology and information by the government, known as Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, in order to create a sense of security, comfort, and justice. The ITE Law can at least be a guideline and legal basis for members of the public in doing activities in cyberspace. In addition, the ITE Law also has links to several articles regulated in the Criminal Code which aim to facilitate the resolution of a case related to information technology.

Based on the statement of Article 4 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, the author interprets that the Articles in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions have implications for the realization of what has been stated in Article 4 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Including Article 28 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions must be able to achieve the objectives of the establishment of the ITE Law.

Based on the statement of Article 4 of Law Number 19 of 2016 on the Amendment to Law No. 11 of 2008 concerning Information and Electronic Transactions, the author interprets that the Articles in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions has implications for the realisation of what is being realised. on Electronic Information and Transactions has implications for the realisation of what has been which has been mentioned in Article 4 of Law Number 19 of 2016 concerning the amendment of Law Number 11 of 2008 concerning Electronic Information and Transactions. Amendment to Law Number 11

of 2008 concerning Information and Electronic Transactions. This includes Article 28 paragraph (1) of Law Number 19 Year 2016 on the Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions. Year 2016 on the Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions must be able to create the objectives of the law. Information and Electronic Transactions must be able to create the purpose of the establishment of the ITE Law.

However, to determine whether someone violates Article 28 paragraph (1) of the ITE Law or not, there are several implementation guidelines that must be considered as follows

1. The criminal offence in Article 28 paragraph (1) of the ITE Law is not a criminal offence against the act of spreading false news (hoax) in general, but rather the act of spreading false news in the context of electronic transactions such as online trading transactions;
2. Fake news or information sent through messaging application services, online broadcasting, websites/social media, marketplaces, advertisements, and/or other transaction services through electronic systems;
3. The form of electronic transactions can be in the form of an agreement between business actors/sellers and consumers or buyers;
4. Article 28 paragraph (1) of the ITE Law cannot be imposed on parties who make defaults and / or experiencing force majeure;
5. Article 28 paragraph (1) of the ITE Law is a material offence, so that consumer losses as a result of false news must be calculated and determined. news must be calculated and determined;
6. The definition of "consumer" in Article 28 paragraph (1) of the ITE Law refers to the Consumer Protection Law

In the case of online fraud, losses are not only felt by consumers, but also by businesses. Here are some common forms of online fraud in the field of buying and selling:

1. Goods/products received are not as ordered;
2. The goods/products are counterfeit;
3. The identity of the business actor or consumer is fictitious;
4. Fraudulent price discounts on the goods/products offered, i.e. the goods/products received are used, unfit for use, or even not delivered.

CONCLUSION

Article 28 paragraph (1) of the ITE Law can only be used for victims of fraud in electronic transactions, namely only limited to producers and consumers, while victims of fraud who are not consumers, such as victims of phishing-type fraud cannot be charged with the Article. Then a person who intentionally, and without the right to spread false and misleading news resulting in consumer losses in electronic transactions shall be sentenced to imprisonment for a maximum of 6 years and / or a maximum fine of Rp1 billion, the contents of Article 28 paragraph (1) of the ITE Law.

REFERENCES

- Anton Hendrik Samudra. “Modus Operandi Dan Problematika Penanggulangan Tindak Pidana Penipuan Daring.” *Mimbar Hukum: Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada* no 31 vol (2019).
- Chazawi, Adam. *Tindak Pidana Informasi & Transaksi Elektronik – Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi ITE*. Malang: Bayumedia Publishing, 2011.
- Iman Sjahputra, 2010, *Konsumen Masih Dirugikan dalam Transaksi Elektronik*, Jakarta
- Sutisna. 2001. *Perilaku Konsumen dan Komunikasi Pemasaran*. PT. Remaja

Rosdakarya:

Bandung

Sri Wulandari. 2019. Mekanisme Penyidikan Tindak Pidana Penipuan Yang Menggunakan Media Transaksi Elektronik. Jurnal Spektrum Hukum.

Steven Harnad. "The Fourth Revolution in the Means of Production of Knowledge, Public-Access Computer System Review 2 (1): 39-53." Post-Gutenberg Galaxy, 1993.<http://cogprints.org/1580/00/harnad91.post>