Lentera Hukum, Volume 6 Issue 1 (2019), pp. 1-16
ISSN 2355-4673 (Print) 2621-3710 (Online)
https://doi.org/10.19184/ ejlh.v6i1.9567
Published by the University of Jember, Indonesia
Available online 28 April 2019

Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia

Rizky Karo Karo
Pelita Harapan University, Indonesia
rizky.karo.karo@uph.edu

Agnes Sebastian
Universitas Pelita Harapan, Indonesia
sebastian.agnes@gmail.com

ABSTRACT
The development of technology has led to the sales and purchases of products and services online. However, the absence of a physical store prevents the prospective buyers from physically assessing the quality of the product/service. This leads to the emerging issue of online shop fraud. This paper aims to analyse the scope of online shop fraud within Indonesian laws and regulations, as well as the legal enforcement by Indonesian authorities to eradicate online shop fraud. This research uses the normative juridical method, which utilises secondary data such as books, journals and relevant legal products. This research finds that the Criminal Act of online shop fraud is regulated under Article 28 paragraph 1 of Law Number 11 Year 2008 following its amendment to Law Number 19 Year 2016 on Electronic Information and Transaction. The current efforts for legal enforcement of online shop fraud is performed in both preventive and repressive manners.

KEYWORDS: Online Shop, Fraud, Cybercrime.

HOW TO CITE:
Karo, Rizky Karo & Agnes Sebastian. *"Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia"* (2019) 6:1 Lentera Hukum 1–16.

Submitted: January 25, 2019 **Revised:** February 03, 2019 **Accepted:** February 21, 2019

I. INTRODUCTION

Globalisation has introduced sophisticated and modern technologies, which profoundly impacts the development of a country.[1] With globalisation, new technologies and information are easily accessible, especially with the existence of the internet. Such accessibility causes priority to shift, resulting in basic human needs that improve daily activities and eventually lead to change in culture, economy, security, as well as law.

Humans have increasingly become more dependant towards technology, including smartphones, laptops and the internet. Such dependency has been due to the need to improve the quality of life by incorporating accessible technology and information within all sectors of life, such as government administration, business, banking, education, healthcare, etc. It is almost impossible to live as a modern man without the existence of the internet. Although the technological developments positively impact the lives of the people, there is also a possibility for such technological improvements to draw in various kinds of crimes that develop alongside modern technologies, i.e. cybercrime, which may result in a bigger impact than conventional crimes.[2] The frequency of cybercrime committed is prevalent in Indonesia,` considering that cybercrime investigation is harder to conduct as it can be anonymous and conducted by everyone regardless of location.

According to Merriam-Webster Dictionary, cybercrime is a crime committed electronically. Several crimes that are classified as cybercrimes are online gambling, skimming, phishing, identity theft, defamation, fraud and many more. Prior to the enactment of Law No. 11 Year 2008 regarding Electronic Information and Transaction ('UU ITE'), the applicable law to cybercrime was the Indonesian Criminal Code, thus rendering cybercrime as a conventional crime. However, such Criminal Code was seen not fit to supplement the law enforcement of cybercrime, as cybercrime is committed through an electronic system, which means that the evidence to prove such crime would likely also be electronic. Thus, the UU ITE serves as a *lex specialis*, a special law which regulates on cybercrime specifically.

In contrast to traditional sales and purchase transactions, online transactions can be performed with ease without having to physically go outdoors to purchase objects or services. Products ranging from clothing to doctor consultation can be found online. There are several places where online transactions may occur, firstly, through social media, such as Instagram or Facebook, secondly, through online e-commerce platform such as Tokopedia, Bukalapak, etc. and thirdly, through online commerce websites such as ikea.com, adidas.co.id, etc. (generally managed directly by the company). Transactions through social media are the trickiest out of the three. This is because social media accounts are not designed for e-commerce transactions to occur. Not only are the accounts not verifiable, the object of sale cannot be physically inspected, which

---

1 Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: Rajawali Pers, 2013), p. 1.

2 *Ibid*. p. 11-12.

means that these types of transactions occur solely based on trust. In contrast, online e-commerce platforms act like a bridge between sellers and buyers. In this type of transaction, the seller sells its products through the e-commerce platform and all transactions must go through the platform's account, which makes it more secure than social media online shops. Online commerce websites are in general managed by the company, where transactions occur directly between buyer and seller as if the website is a store.

Although online shopping may seem alluring for its accessibility and relatively cheaper prices, there are risks involved in such transactions, such as online shop frauds. As an example, Kristinus purchased two pump machines through the website at www.wildanwijayagroup.com and transferred down payment through internet banking in the amount of Rp. 23,130,000.[3] However, the pump machine was never delievered to Kristinus.[4] The cybercrime police arrested Bantaqia, Friman and Said Jauhari, who were believed to be the perpetrators in Kristinus's fraud case.[5] To minimise such fraudulent crime from reoccurring, not only does the law need to be clear on this matter, but also the law enforcer must be able to track down the perpetrator with a modern technological method so that law enforcers are up to par.

Based on the background, the author will be addressing the scope of online shop fraud within Indonesian legal products and legal enforcement performed by Indonesian authorities, in the effort to eradicate online shop fraud. This aims to identify the relevant Indonesian regulations that regulate online shop fraud and to obtain knowledge of countermeasures that are taken by the authorities to eradicate online shop fraud.

This research paper utilises the normative law research method, which is popularly referred to as doctrinal law research or library research.[6] This research method is directed to written legal products, expert's opinions, books, journals, legal norms and legal principles as the main data to analyse the question of this particular research paper.[7] Then, the researcher will continue analysing the theory, structure, substance and consistency of relevant articles within the written legal products and law books/journals. Therefore, the normative law research analyses the material qualitatively.

For the purpose of normative juridical research method, the author will incorporate mostly secondary data that is also popularly known as library legal materials. Information that have been processed by other sources, regardless of being in the form of literatures such as laws, expert's opinion and any other library materials are

---

[3] Mei Amelia R, "Terlibat Penipuan Jual-Beli Online, Mahasiswa Ini Ditangkap Polisi", Detiknews.com, https://news.detik.com/berita/d-3474703/terlibat-penipuan-jual-beli-online-mahasiswa-ini-ditangkap-polisi, accessed 18 July 2018.

[4] *Ibid*.

[5] *Ibid*.

[6] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, (Jakarta: PT Raja Grafindo Persada, 2003), p. 13.

[7] Meray Hendrik Mezak, "Jenis, Metode dan Pendekatan dalam Penelitian Hukum," Law Review Vol. V, No. 3, Maret 2006, p. 91.

considered as secondary data.[8] The type of library legal materials used are primary legal material, secondary legal material and tertiary legal material.[9] Primary legal material includes legal materials which have authoritative properties i.e. the 1945 Constitution, Indonesian Criminal Code, Law No. 8 Year 1981 regarding Criminal Procedure, Law No. 11 Year 2008 regarding Electronic Information and Transaction ('UU ITE'), and other relevant laws and regulations. Secondary legal material is the derivative of the primary legal material as the result of observations upon laws and regulations related to the research. Secondary legal material includes books, law journals and articles. Tertiary legal material that provides explanatory pointers to primary legal material and secondary legal material are legal dictionaries, language dictionaries and encyclopedias.

II. REGULATION ON ONLINE SHOP FRAUD

Electronic transactions are paperless, as they are processed through electronic means. The evidence to prove the existence of such electronic transactions as a consequence will also be electronic. The criminal code, however, do not recognise electronic evidence as admissible, for it only provides that admissible evidence in article 184 paragraph 1 as: "legal means of proof shall be: a. the testimony of a witness; b. the testimony of an expert; c. a document; d. an indication; e. the testimony of the accused." However, due to the emerging need to admit such electronic evidence in court as globalisation and modernisation requires so, UU ITE provides the grounds to admit electronic evidence. Specifically, under article 5 paragraph 1 of UU ITE, electronic information and/or electronic documents and/or their printouts are admissible evidence. The general provisions article 1 paragraph 1 and article 1 paragraph 4 of UU ITE provides that:

> "*Electronic information means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, access codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.*"
>
> "*Electronic document means any electronic information that is created, forwarded, sent, received, or stored in analogue, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via computers or electronic systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, access codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them.*"

---

[8] Mukti Fajar and Yulianto Achmad, *Dualisme Penelitian Hukum-Normatif dan Empiris,* (Yogyakarta: Pustaka Pelajar, 2015), p. 34.

[9] Peter Mahmud Marzuki, *Metode Penelitian Hukum,* (Jakarta: Kencana, 2006), p. 141.

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site for a long term basis. The perception that the internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce[10].

The existence of UU ITE lays out the foundation for electronic transactions, as well as information and communication technology. Where prior to this enactment, there are no specific laws that regulate electronic transactions, information and communication technology. Electronic proof was not considered as admissible, rendering it difficult to prove and prosecute cybercrime. The government's effort to provide for legal certainty in the sake of justice has a profound impact to the development of cybercrime legal enforcement, as electronic evidence becomes admissible in court. Hence, there is clear legal protection for victims of cybercrime and legally binding effects towards perpetrators of cybercrime.

Electronic information and documents shall fulfil formal and material requirements in order to be considered as admissible evidence. The formal requirement is that the electronic information and documents are not required by law to be made in writing or in notarial deed as stipulated in article 5 paragraph 4; whereas the material requirement, in its essence, requires the electronic information and documents to be accessible, reliable, authentic, secure, and verifiable as stipulated in article 6, article 15 and article 16 of UU ITE. To determine whether or not electronic information or documents are admissible as digital evidence, it must go through digital forensic process.[11]

The concept of cybercrime is not so much different from that of conventional crime, as both include conduct, whether act or omission, causing a breach of rules of law and counterbalanced by the sanction of the state. The Council of Europe's Cybercrime Treaty uses the term "Cybercrime" to refer to offences ranging from criminal activity against data to content and copyright infringement[12].

Technology development drives humans to follow the current trend of the modern internet and technology era. The misuse of technology and internet leads to cybercrime. Prior to the enactment of UU ITE, crimes within the cyberspace are prosecuted on the basis of Indonesian Criminal Code as it provides a foundational and broader scope of crime. Thus, referring to traditional means of fraud, such crime is punishable based on article 378 of Indonesian Criminal Code which stipulates that:

---

[10] Hemraj Saini, *etc*, "Cybercrimes and their Impacts: A review", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2 ,Mar-Apr 2012, P.206.

[11] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana,* (Jakarta: Tatanusa, 2012).

[12] Peterson Obara Magutu, etc, *Effects of Cybercrime on State Security: Types, Impact and Mitigations With the Fiber Optice Deployment in Kenya*, Journal of Information Assurance & Cybersecurity, Vol. 2011 (2011). DOI: 10.5171/2011.618585, p.3-4

> *"any person who intentionally and unlawfully benefit himself or another, either by assuming a false name or a false capacity, or by crafty artifices, or by a web of fictions, induces someone to deliver any property or to negotiate a loan or to annul a debt, shall, being guilty of fraud, be punished by a maximum imprisonment of four years."*

UU ITE does not specifically regulate fraud, however, under article 28 paragraph 1, the law regulates on crime related to electronic transaction, which causes loss to the consumer. Article 28 paragraph 1 of UU ITE stipulates that: "any person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in electronic transactions." Meanwhile, electronic transaction is defined in article 2 paragraph 1 UU ITE as: "a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media." The sanction to such crime is imprisonment for maximum 6 years and/or fine in the maximum amount of Rp. 1,000,000,000.

Fraud conducted in electronic transaction is essentially providing false and misleading information in such transaction that would, otherwise, not have occurred. Fraud is motivated by one's goal to benefit himself and/or to cause loss to others. In relation to the motive of fraud, disseminating false and misleading information can be equated to fraud.[13] In contrast to the article 378 of Indonesian Criminal Code on Fraud, the criteria of what constitutes as a conventional fraud is rather general and broad as it involves the following elements:

1. Subjective element comprising intent, bad faith, benefit himself or another, and unlawful; and
2. Objective element consisting of a person, induces other person (deliver a property, negotiate a loan, annul a debt), and by means of (false name, false capacity, crafty artifices, a web of fictions).

Hence, in simple terms, a fraud:

1. Induces other people to deliver a property, negotiate a loan or annul a debt
2. The goal is to benefit himself or other people
3. Inducement is done by means of using false name, false capacity, crafty artifices or web of lies.

Differing from article 378 of Indonesian Criminal Code, the UU ITE regulates a constricting understanding and application scope to fraud. Fraud is implicitly regulated under false and misleading information, which is distributed through the internet. A limitation on article 28 paragraph 1 of UU ITE is applied as the scope of application of such UU ITE article only extends towards electronic transactions. Fraud in UU ITE is limited to a legal act conducted through electronic transaction between producer and consumer, in which elements of false and misleading information is disseminated in the internet.

Online shopping fraud has become an epidemic in the internet. On one side, there is an increasing number of people who wish to fulfil their needs with ease and

---

[13] Budi Suhariyanto, *supra* note 1, p. 124.

efficiency. On the other side, there are people who have bad motives and wish to benefit themselves through any means possible, including fraud. There are many modes of fraud, ranging from simple modes to complex modes. Although online shop fraud is conducted virtually, the act and effect are real.

Fraud in online shop utilises computer, mobile devices and internet, thus it can be categorised as illegal access and computer related fraud by publishing false and misleading contents. Illegal access, as defined by the Cybercrime Convention 2001, is stipulated as:

> *"committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Based on article 8 of The Convention on Cybercrime 2001, computer related fraud is stipulated as:

> *"intentionally and without right, the causing of a loss of property to another person by:*
>
> *a. any input, alteration, deletion or suppression of computer data;*
>
> *b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."*

Computer related fraud is often found in online shopping, whereby the advertised product is described differently from the real product, or even the legitimacy of the online shop itself is fake. Such irresponsible acts cause loss to the consumer, as the seller fails to perform its duty in delivering the agreed upon product. In electronic sales and purchase transactions, there are several parties involved:

1. seller who advertises and sells product through the internet;
2. buyer who purchases product offered by seller through the internet;
3. bank who acts as a medium for money transfer from the buyer to the seller; and
4. internet provider.

Once there is an agreement to sell and buy a product, rights and obligations arise out of the transactional agreement. The seller who advertises and offers his/her product through the internet has the obligation to provide truthful and accurate information regarding the advertised product, as well as having the obligation to deliver the product to the buyer. In turn, the seller has the right to obtain payment for the product sale, as well as the right to protection from the seller who may have bad faith in conducting such electronic transaction. As for the buyer, he/she has the obligation to pay for the product, which he/she has bought from the seller in the amount agreed upon, as well as the obligation to truthfully disclose personal information such as name, phone number and address for the sake of delivering the product. In turn, the buyer has the right to receiver accurate and complete information of the product of sale as well as the legal protection from bad faith sellers.

In online transactions, the seller and the buyer do not meet directly to conduct sales and purchase transactions. As a result, exchange of money must be done through bank transfers. Banks act as the intermediary body between the seller and the buyer. In electronic sale and purchase transactions, the bank's function is to channel funds or to

account transfers from the buyer as payment of a product to the seller, as online transactions usually do not allow for direct payment of cash due to the seller and buyer being in different locations.

Internet providers have the obligation to provide internet access to both the seller and the buyer. In order for the seller and buyer to perform online transactions, they must obtain access to the internet. However, agreement to provide internet is separate and irrelevant to this case, as the internet provider acts as a seller who offers its product, i.e. internet to parties who wishes to have access to the internet.

Principally, online transactions and conventional transactions are the same. To conduct online and conventional transactions, these following stages are involved:

1. **Offering**. The seller advertises and offers products through internet website. Product catalogue can be found in the website page which is accessible to everyone. Purchase can be made through the website, email address, internet messenger or any other method of communication.
2. **Agreement**. If the buyer agrees to purchase the product sold by the seller, the buyer may accept the offer by confirming order with the seller either through the website, email address, internet messenger or any other method of communication based on the seller's policy.
3. **Payment**. Payment can be made directly through cash on delivery or indirectly through bank transfer.
4. **Delivery**. Once payment has been made, the seller shall deliver the product to the agreed upon destination either through third-party carrier or direct delivery by the seller. After the product has been delivered, the transaction is therefore completed.

The difference between online and conventional transactions are the place of transaction. Online fraud and conventional fraud are also similar in nature, despite being different in terms of the means of such action. Both differences lie in the involvement of electronic systems i.e. computer, internet, communication devices in online transaction and online fraud. Hence, online fraud can be prosecuted under article 378 of criminal code[14], as well as article 28 paragraph 1 of UU ITE. And if each person is proven against, according to article 45A verse 1 of UU ITE[15], they will be threatened with imprisonment and/or forfeit 1 billion Rupiah.

---

[14] Article 378 KUHP "Any person who with intent to unlawfully benefit himself or another, either by assuming a false name or a false capacity, or by crafty artifices, or by a web of fictions, induces someone to deliver any property or to negotiate a loan or to annul a debt, shall, being guilty of fraud, be punished by a maximum imprisonment of four years.

[15] Article 45A paragraph (1) UU ITE "Any Person who intentionally and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions as intended by Article 28 paragraph (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp 1,000,000,000 (one billion rupiah)."

III. COUNTERMEASURES TO ERADICATE ONLINE SHOP FRAUD

In analysts' opinions, consumers can sue a lawsuit to the court, according to Law No.8 Year 1999 about Consumer Protection (*in Bahasa, UU 8/1999 tentang Perlindungan Konsumen*). According to Article 23 Law No.8 Year 1999, consumers file the lawsuit to the judiciary at the consumer's domicile (*lex specialis*), this is different from Article 118 paragraph (1) *Herzien Indlandsch Reglement (lex generalis)*. Consumers can sue the online store providers as co-defendants and sellers as the 1st defendant. Online store providers also have the responsibility to provide compensation because they provide these sales services.

Consumers have to attach evidences, such as electronic evidence of conversations, electronic mail, payments screenshots from their smartphone, laptop computers. Those electronic documents are valid evidence in accordance with the procedural law in Indonesia (Article 5 Paragraph 1 and Paragraph 2 Law ITE).

The sellers as business actors have an obligation to: a. have good intentions in carrying out their business activities; b. provide true, clear and honest information about the condition and the guarantee of goods and / or services and provide an explanation of usage, repair and maintenance; c. treat or serve consumers correctly and honestly and not discriminatory; d. provide compensation, and / or compensation for loss of use, use and utilization of traded goods and / or services; e. provide compensation, compensation and / or replacement if the goods and / or services received or utilized not in accordance with the agreement (Article 7 Law No.8 Year 1999).

Even though online shop providers make a statement or disclaimer that they are not responsible for transactions, according to the Law No.8 Year 1999 they still have a civil responsibility. The countermeasures that can be taken by the authorities are preventive measures and repressive measures. The preventive countermeasure effort by the police includes socialisation and community guidance by the Community and Society Development Unit of National Police of Republic of Indonesia. The socialisation in respect to cybercrime should be aimed at equipping the community with knowledge of electronic transactions and proper measures that should be taken, prior to being involved in electronic transactions. While repressive countermeasures are performed by investigators of a case, which leads to the prosecution of crime.

The repressive countermeasure is conducted based on the existence of cases. Fraud in cybercrime requires the victim to report the existence of such a crime to the authority. The report shall be accompanied with preliminary evidence in the form of electronic data or information and/or printed forms of electronic data or information. To prove the existence of such fraud, investigation must be conducted. The procedural law in relation to UU ITE is regulated under article 42, whereby investigation of cybercrime acts shall be conducted based on the provisions of criminal procedure within UU ITE. This implicates that the general law, i.e. criminal procedural law, is still applicable should there be gaps in the UU ITE in regards to the criminal procedure provisions. Thus, the UU ITE serves as a *lex specialis*, whereby the provisions within UU

ITE shall prevail as it contains a more specific regulation within the scope of information technology and electronic transactions. Such provisions can be found in article 284 paragraph 2 of criminal procedural law, whereby it stipulates that: "within two years after the promulgation of this law, all cases shall be subject to the provisions of this law, with temporary exception for special provisions on criminal procedure as referred to in certain laws, until they are amended and or are declared to no longer be in effect." In conjunction with article 42 of UU ITE, these provisions mean that procedural law within the UU ITE shall apply as special provisions; thus, exceptions to the criminal procedural law.

In comparison to the criminal procedural law, there is no differentiation in terms of the qualification of an investigator. Article 43 of UU ITE qualify the investigator of the National Police of Republic of Indonesia and certain civil servants tasked within the scope of information technology and electronic transactions; granted that the investigation must be made with due regard to privacy protection, confidentiality, public services, and data integrity/data entirety. Investigators shall commence an investigative proceeding by collecting admissible evidences in accordance to article 184 paragraph 1 of criminal procedural law jo. Article 5 of UU ITE to fulfil the elements of a crime. The investigator has the obligation to follow through the investigation process by tracking down the source of such electronic documents. The source of electronic documents is referred to as an IP address, found within the server of the website used.[16]

Virtual worlds contain unique social environments, in which new and distinctive forms of delinquent behaviour arise. Consequently, it has been argued that traditional explanations are unsatisfactory for explaining cyber delinquency, and thus new theories are needed17. Based on Government Regulation (Peraturan Pemerintah RI) No.82 Year 2012 about Management of Electronic Systems and Transactions (Penyelenggaraan Sistem dan Transaksi Elektronik), electronic system providers must guarantee: a. availability of service level agreements; b. availability of information security agreements against Information Technology services used; and c. information security and means of internal communication which is held.

The investigation stage then shall be verified and examined during court proceedings to establish relation between the evidence to the crime. Since the filing of a crime is reported by the victim, the investigator has the obligation to solve the crime and serve the victim, as an upholder of justice. The investigator must collect facts which will be constructed into a material truth. Material truth is considered as "the one

---

[16] Teguh Arifiyadi, "Cara Penyidik Melacak Pelaku Penipuan dalam Jual Beli Online", Hukumonline.com, http://www.hukumonline.com/klinik/detail/lt4f814bf6c2ca4/penipuan-bisnis-jual-beli-online, accessed 18 July 2018.

[17] Josja J. Rokven, Etc, "Juvenvile Delinquency in the Virtual Wolrd: Similarities and Differences between Cyber-Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands. International Journal of Cyber Criminology, Vol.12 Issue 1 Jan-Jun 2018, DOI: 10.5281. P.29

which makes possible to recompose the facts exactly as they happened."[18] This is in contrast to formal truth. which is dependent on logical reasoning to interpret.[19]

Depending on where the server is located, different levels of complexity may arise. Should the location of the server be outside of the territory of Republic of Indonesia, the investigator must comply with foreign laws to gather the IP address from abroad. Different procedures may apply to different countries, which makes the investigator's task more complicated. Indonesia may seek legal assistance from other signatory countries of treaty on mutual legal assistance ('MLA') in criminal matters. Indonesia has ratified the treaty as Law No. 1 Year 2006 regarding Mutual Legal Assistance in Criminal Matters. Currently, the signatories are Brunei Darussalam, Indonesia, Cambodia, Laos, Malaysia, Myanmar, Philippine, Singapore, Thailand and Vietnam.

Legal assistance includes identifying and locating persons, deposing a person in foreign state by direct meeting/teleconference/direct broadcast, arranging for a person to be presented in Indonesia to provide legal means of proof, etc. Proper and extensive diplomatic channels must be pursued through a request made by the investigator to the National Chief Police or the Attorney General, who then pass on the request to the Minister of Foreign Affairs. The Minister of Foreign Affairs will reach out to the relevant country's government and request for legal assistance. However, MLA is only applicable in certain cases and for certain requests. The issue of jurisdiction may remain due to the limitation of MLA applicability. As a result, cybercrime cases are often left unsolved.

Despite having knowledge of the IP address, this does not directly lead to the perpetrator's identity and location. Nowadays, there are many sophisticated technologies that could mask the location and identity of the cybercrime perpetrator, such as a falsifying IP address and bouncing off the IP address tracking to various parts of the world.

However, in the case of online shopping, it is more likely for the fraud perpetrator to be discovered, as money transfers are usually conducted directly to the account of fraud. Once the identity has been discovered, the authority shall then proceed to proving the technical aspects of online shop fraud. All documents or electronic information shall be seized by the investigator in order to develop a strategy in obtaining the material truth.

Although article 28 paragraph 1 of UU ITE on dissemination of false or misleading information is utilised in proving fraud in electronic transactions, the legislature should provide for specific provisions on online fraud. Hence, the countermeasure effort could be further enforced to repress any account of fraud in the future, as legal certainty is served. It is crucial for there to be a provision on online fraud to legally protect consumers who wish to conduct a commercial electronic transaction, especially when almost everything can be bought online easily and quickly.

---

[18] Lenio L. Streck, *A ficção da verdade real e os sintomas da falta de compreensão filosófica da ciência processual* (Porto Alegre: Revista do Ministério Público do Rs, 2011).

[19] *Ibid*.

Online transactions are based on mutual trust. Such trust is assumed by both seller and buyer to continue on with the transaction. In the case where seller and buyer are both acquainted with each other, trust can be built as they negotiate and conduct sales and purchase transactions. More often than not, parties to the transaction may not know of eachother. Considering that online sellers and buyers are strangers to each other, there should be prudential measures taken not only by sellers but also by the buyers. In legal aspects, both parties should establish a contract to protect the interest of each party and to protect them from loss that may incur as a result of the transaction. The contract shall contain the rights and obligations of each party for the transactions. However, for simple transactions, such contracts may not be needed for reasons of convenience. As a result, the rights and obligations of both parties become vague whilst the seller have the upper hand, as it is common practice for the seller to act arbitrarily, especially having received payment. To ensure protection to the consumer from such unfair acts, the UU ITE shall establish a clear and certain provision on the legitimacy of electronic transaction, as well as fraud in electronic transactions.

In addition to criminal sanctions, providers of electronic systems can be given administrative sanctions in the form of a. written warning; b. administrative fine; c. temporary termination; and / or d. excluded from the list in Indonesia Ministry of Communication and Informatics [PP 82/2012 Article 84 (2)]. Administrative sanctions are given by the Minister or the leader of the Supervisory Agency and related Sector Regulators in accordance with the provisions of legislation.

IV. CONCLUSION

Essentially, online fraud is equitable to conventional means of fraud. The difference lies in the means of fraud execution. Where online fraud involves electronic devices or systems, such as computers, smart phones, the internet, social media, etc. The regulation on online fraud can be found in article 378 of Criminal Code regarding fraud and/or article 28 paragraph 1 of Law No. 11 Year 2008 regarding Electronic Information and Transactions jo. Law No. 19 Year 2016 regarding the dissemination of false and misleading information, which results in consumer's loss in electronic transactions.

As online shop fraud requires the victim to first report the existence of such crime to the police. The police shall be equipped with sufficient knowledge and understanding in the field of electronic information and transaction technologies as well as cybercrime. As it is within the police's duty to serve the people, it is only just to the victims of cyber fraud to be served by police officers, who have had proper training and education in light of legal justice as well as safety in both conventional world as well as cyber world. In order to implement this, the Electronic Information and Transaction Law should further regulate and specify the requirement of investigators, or any other relevant authorities, to be certified by a certain body that supports the eligibility of the authority.

The government should also provide socialisation, which promotes the "buyer beware" slogan to prevent unwanted crime of fraud from happening in the real world and in the cyber world. The "buyer beware" motto is necessary to educate the general population on conducting online transactions, including performing due diligence on the legality or the validity of the transaction.

REFERENCES

Ali, Mahrus. 2012. *Dasar-Dasar Hukum Pidana*. Jakarta: Sinar Grafika.

Amiruddin dan H. Zainal Asikin. 2006. *Pengantar Metode Penelitian Hukum*. Jakarta: PT Raja Grafindo Persada.

Arifiyadi, Teguh. "Cara Penyidik Melacak Pelaku Penipuan dalam Jual Beli Online". Hukumonline.com. http://www.hukumonline.com/klinik/detail/lt4f814bf6c2ca4/penipuan-bisnis-jual-beli-online. Accessed 18 July 2018.

Budhijanto, Danrivanto. 2013. *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi*. Bandung: PT. Refika Aditama.

Fajar, Mukti dan Yulianto Achmad. 2015. *Dualisme Penelitian Hukum-Normatif dan Empiris.* Yogyakarta: Pustaka Pelajar.

Magutu, Peterson Obara. 2011. *Effects of Cybercrime on State Security: Types, Impact and Mitigations With the Fiber Optice Deployment in Kenya*, Journal of Information Assurance & Cybersecurity, Vol. 2011.

Makarim, Edmon. 2003. *Kompilasi Hukum Telematika*. Jakarta: RajaGrafindo Persada.

Marzuki, Peter Mahmud. 2005. *Penelitian Hukum*. Jakarta: Kencana.

Mezak, Meray Hendrik. 2006. "Jenis Metode dan Pendekatan dalam Penelitian Hukum". Tangerang: *Law Review Fakultas Hukum Universitas Pelita Harapan*. Vol. V, No. 3.

Moeljatno. 2008. *Asas-Asas Hukum Pidana*. Jakarta: Rieneka Cipta.

Muhammad, Abdulkadir. 2004. *Hukum dan Penelitian Hukum*. Bandung: PT Citra Aditya Bakti.

Partodihardjo, Soemarno. 2008. *Tanya jawab Sekitar Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Gramedia Pustaka Utama.

Prodjodikoro, Wirjono. 2003. *Tindak Pidana Tertentu di Indonesia.* Bandung: Refika Aditama.

Rokven, Josja J. 2018. "Juvenvile Delinquency in the Virtual Wolrd: Similarities and Differences between Cyber-Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands. International Journal of Cyber Criminology, Vol.12 Issue 1 Jan-Jun 2018.

R., Mei Amelia. "Terlibat Penipuan Jual-Beli Online, Mahasiswa Ini Ditangkap Polisi". Detiknews.com. https://news.detik.com/berita/d-3474703/terlibat-penipuan-jual-beli-online-mahasiswa-ini-ditangkap-polisi. Accessed 18 July 2018.

Saini, Hemraj. 2012. "Cybercrimes and their Impacts: A review", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2 ,Mar-Apr 2012, ISSN: 2248-9622.

Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.

Soekanto, Soerjono. 1986. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia-Press.

Soekanto, Soerjono dan Sri Mamudji. 2003. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: PT Raja Grafindo Persada.

Streck, Lenio L. 2011. *A ficção da verdade real e os sintomas da falta de compreensão filosófica da ciência processual*. Porto Alegre: Revista do Ministério Público do Rs.

Suhariyanto, Budi. 2013. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers.

Syamsuddin, Rahman & Ismail Aris. 2014. *Merajut Hukum di Indonesia*. Bogor: Mitra Wacana Media.

This page is intentionally left blank