Online Fraud Law Enforcement

Dadi Waluyo[1], Rineke Sara[2]
{dwaluyo@unis.ac.id}

Universitas Borobudur, Jakarta, Indonesia[12]

Abstract. The article describes the criminal act of fraud committed online by using normative juridical methods, accompanied by literature as data collection to be analyzed descriptively in finding comprehensive research results. The study results indicate that the development of crime has penetrated the virtual world and requires prevention and countermeasures through the ITE Law and Cyber Police Law Enforcement.

Keywords: Law; Online Fraud; Criminal

1 Introduction

The concept of the State of Indonesia as a state of the law is a concept that was developed by its founders as part of regulating every regulation without any arbitrariness, for this reason, with the inclusion of various developing technologies, the law is expected to be able to pursue so that no party is at a loss for that in principle, the state in principle the state is given the obligation to provide welfare and prosperity not only on the management of natural resources but on security guarantees.[1] In this era of modernization globalization, advances in science and technology have brought humans the ease of interacting with each other almost without national and regional boundaries, the convenience also creates the potential for people to commit crimes. Many entrepreneurs use electronic media to promote their goods/services online because it is easier and less expensive.

In Indonesia, there have been many shops in electronic media, including in the jurisdiction of the Yogyakarta Regional Police, ranging from large companies to home sellers (individuals). Advances in computer technology, information technology, and communication technology give rise to a new crime that has different characteristics from conventional criminal acts. Misuse of computers as one of the impacts of these three developments cannot be separated from its unique nature so that it brings new problems that are rather complicated to solve, regarding problems. Computer crime is related to the professional code of ethics because it is still in the context of the profession, namely in the IT field. Which then escalated into a crime in cyberspace or known as cybercrime. This also disrupts the business world in cybercrime where many users are greatly harmed.

However, in reality, these developments present a complex problem. The problems that arise are more diverse, including ecological, economic, political, and social problems. People have used technology in their daily lives, one of which is information and communication technology such as mobile phones, the internet, and other electronic media. In addition to having a large positive impact, information and communication technology also has a negative side.

ICLSSEE 2022, April 16, Jakarta, Indonesia

DOI 10.4108/eai.16-4-2022.2319750

Various crimes can be committed such as prostitution, gambling in cyberspace (internet), breaking into Automated Teller Machines (ATM), theft of company data via the internet, and fraud through electronic media. Therefore, we need a law to regulate it.

The quick advancement of data innovation has impacted all parts of life, including the material legitimate perspectives. The advances in data innovation, among others, are set apart by the far-reaching utilization of electronic media, going from the utilization of cell phones to progressively refined PCs. The utilization of electronic media including strategies to gather, plan, store, process, report, investigate and additionally scatter data is something usually finished by somebody in this cutting-edge time.

Progress in the field of telecommunication and information technology science and technology also supports the expansion of the space for transactions of goods and/or services to cross the boundaries of a country. Data innovation and electronic media are viewed as trailblazer images, which will coordinate every world framework, both in socio-social, monetary, and monetary angles. From little neighborhood and public frameworks, the course of globalization is moving quick, even excessively quick toward a worldwide framework.

The internet is growing so rapidly as the culture of modern society, it is said to be culture because through the internet various activities of cyber society such as thinking, creating, and acting can be expressed in it, at anytime and anywhere. Its presence has formed a separate world known as the virtual world (cyberspace) or pseudo world, which is a world of computer-based communication that offers a new reality in the form of virtual (indirect and not real).

Barda Nawawi Arief expressed that cybercrime is another structure or aspect of the present wrongdoing that has gotten the consideration of the more extensive local area in the worldwide local area, it is likewise one of the dim sides of mechanical advances that adversely affect all cutting-edge life today. Propels in innovation make it more straightforward for an individual to have the option to get to whatever is required, both with respect to data, exchanges, and numerous different things. The utilization of data innovation has changed human conduct a great deal. Web innovation affects the world economy.

The web has brought the world economy into another stage which is all the more famously known as advanced financial aspects or the computerized economy. Activities on the internet can reach all parts of the world beyond national boundaries. Something in the real world is far from ahead, in the virtual world it can be presented as if the world is close. As an initial note, one can understand that sellers and buyers are consumers of the operation of an electronic system that has been developed by a certain party (developer) or organized by a certain party (provider). So as an initial study, the responsibility of the developer and/or operator of the electronic system should be absolute (strict liability), i.e. as long as the existing system can be believed to be running as it should, the new risk can be said to be transferred fairly to its users.[2]

In addition to having a large positive impact, internet uses also harms people's lives, one of which is the emergence of crime. Negative impacts can arise if there is an error caused by computer equipment which will result in great loss for the user or interested parties and the errors that intentionally lead to computer abuse.

It is undeniable that advances in technology and knowledge can make progress regarding crime also developing. The perpetrators of any crime do not know the place or in any way as long as it can be used as a place to commit crimes. In the world of the Internet, the potential for criminals to commit crimes is huge and very difficult to catch because most of the people in this virtual world are fictitious or the identity of each person is not real. Crimes that occur on the Internet are known as Cybercrimes (crimes in cyberspace).[3] The crime was committed by using a computer as a means of action, a form of this crime is the crime of fraud using electronic transactions.[4]

Various modes of fraud through online media also continue to emerge and perpetrators are getting neater in smoothing their actions in fraud, this can be seen from the many fake buying and selling websites that are made in such a way and offer various products at prices below normal prices, to attract the victim's interest in buying, and there is also fraud by sacrificing other people's accounts to be the result of a criminal act of fraud in which the perpetrator has transferred to the seller's account more than the agreed price for various reasons and asks for the excess to be returned to his account, but in reality, the money is the result of the perpetrator's fraud against the victim in another place where the perpetrator pretends to sell a certain item and gives the victim's previous account number. Legitimate issues that are many times looked in internet-based extortion wrongdoings are connected with the conveyance of data, correspondence, as well as electronic exchanges, to be specific as far as proof and matters connected with lawful activities helped out through electronic frameworks.

2 Research Methods

The technique utilized by the creator is a standardizing juridical examination strategy with library research for of information assortment. Scholarly examinations are taken from optional legitimate materials, existing writing, as well as works as postulations and articles, likewise take essential lawful materials, in particular related regulations, and the Criminal Code.[5] The data that has been obtained is then analyzed descriptively to produce a comprehensive study.

3 Results and Discussion

A little about the conditions that occur in this society can lead to various issues in the settlement of criminal acts in the field of information technology. This paper-less condition makes issues in demonstrating data that is handled, put away, or sent electronically. The straightforwardness with which an individual purposes any personality to do different kinds of electronic exchanges anyplace can make it challenging for policing to decide the character and area of the genuine culprits. The presence of electronic proof in the law enforcement framework in Indonesia and how it very well may be acknowledged in court as legitimate proof will turn into a urgent subject in the following couple of years, particularly with the institution of Law Number 11 of 2008 concerning Electronic Information and Transactions.

The improvement of data innovation, including the web, additionally presents difficulties for the advancement of regulation in Indonesia. Regulation in Indonesia is expected to adjust to the social changes that happen. Social changes and lawful changes or the other way around don't necessarily in all cases occur together. It intends that in specific conditions the advancement of regulation might be abandoned by the improvement of different components of society and its way of life or maybe the inverse. [6]

Cybercrime is a form of crime that arises because of internet technology. The rapid development in the use of internet services invites offense to occur. With the increasing number of requests for internet access, crimes against the use of information technology are increasing following the development of the technology itself. More and more parties are harmed by the actions of cyber criminals if there is no availability of law that regulates it. Before the ITE Law enactment, law enforcement officials used the Criminal Code in dealing with cybercrime cases.

The arrangements contained in the Criminal Code with respect to cybercrime are as yet worldwide in nature. Teguh Arifiady orders a few things that are explicitly controlled in the

Criminal Code and are organized in light of the degree of force of the event of the case, to be specific [3] :

a. Provisions relating to the theft offense in Article 362 of the Criminal Code
b. Arrangements connecting with the obliteration/annihilation of products are contained in Article 406 of the Criminal Code
c. The offense with respect to erotic entertainment is contained in Article 282 of the Criminal Code 4
d. The offense in regards to misrepresentation is contained in Article 378 of the Criminal Code
e. Arrangements connecting with the demonstration of entering or crossing the region of someone else,
f. The offense in regards to misappropriation is contained in Article 372 of the Criminal Code and 374 of the Criminal Code
g. Wrongdoings against public request are contained in Article 154 of the Criminal Code
h. The offense regarding insult is contained in Article 311 of the Criminal Code.
i. The offense regarding letter falsification is contained in Article 263 of the Criminal Code
j. Provisions regarding the disclosure of secrets are contained in Article 112 of the Criminal Code, Article 113 of the Criminal Code, & Article 114 of the Criminal Code
k. The offense regarding gambling is contained in Article 303 of the Criminal Code

Article 42 of the ITE Law specifies those examinations of cybercrimes are done in view of the arrangements of the criminal system regulation and the arrangements of the ITE Law. That is, every one of the guidelines contained in the Criminal Procedure Code actually apply as broad arrangements (lex generalis) aside from those that are strayed by the ITE Law as extraordinary arrangements (lex specialis). All in all, arrangements in regards to examinations that are not directed in the ITE Law will keep on applying as controlled in the Criminal Procedure Code.

This course of action is additionally in accordance with the arrangements in Article 284 passage (2) of the Criminal Procedure Code, in particular that all cases apply the arrangements of the Criminal Procedure Code, with the brief exemption of the exceptional arrangements for criminal strategies as alluded to in specific regulations until there are changes to the dam or it is proclaimed as of now not substantial. The ITE Law is one illustration of "unique arrangements for criminal methods as alluded to in specific regulations" and these exceptional arrangements for criminal techniques stay basically prior to being audited, changed, or denied.[4]

The ITE Law has regulated criminal acts of illegal access (Article 30), interference with Computer Systems (Article 32 of the ITE Law). In addition to these criminal acts, the ITE Law also stipulates additional criminal acts as regulated in Article 36 "… intentionally and without rights or against the law committing acts as referred to in Article 27 to Article 34 that result in harm to other people". However, if to conclude a computer-related fraud investigator must prove these criminal acts first, it can cause problems and inefficiency.

Regulations regarding the spread of false and misleading news are necessary to protect consumers who conduct commercial transactions electronically. Electronic trading can be carried out easily and quickly. Ideally, transactions should be based on mutual trust. This trust is assumed to be obtained if the transacting parties know each other based on previous transaction experiences or direct discussions before the transaction. From a legal point of view, the parties need to make a contract to protect their interests and protect them from losses that may arise in the future. The contract contains the rights and obligations of each party to the transaction. In addition, this contract is also usually terminated with a choice of law and/or legal jurisdiction that can be accepted by the parties in the event of a dispute or dispute. This becomes a very important provision if the transaction is carried out by parties of different nationalities.

4 Conclusion

Online misrepresentation is equivalent to ordinary extortion. The thing that matters is just in the method for activity, to be specific utilizing Electronic Systems (PCs, web, media transmission gadgets). The legitimate plan in regards to the lawbreaker demonstration of misrepresentation is as yet restricted in the utilization of the Criminal Code and depends on Law Number 11 of 2008 concerning Information and Electronic Transactions. Cops frequently experience troubles and snags in catching culprits of fake wrongdoings.

This criminal demonstration of extortion can be accused of Article 378 of the Criminal Code as a lawbreaker demonstration of misrepresentation or Article 28 passage (1) of the ITE Law concerning the guideline with respect to the spread of bogus and misdirecting news that hurts customers. Or on the other hand it tends to be charged in light of the two articles on the double, to be specific, 378 of the Criminal Code related to Article 28 passage (1) related to Article 45 section (1) of Law No. 11 of 2008 concerning misrepresentation and additionally ITE violations.

References

[1] R. S. Luhukay, "Karakteristik Tanggung Gugat Perusahaan Terhadap Lingkungan Dalam Menciptakan Kesejahteraan Rakyat," J. Meta Yuridis, vol. 2, no. 2, p. 14, 2019.

[2] A. Raharjo, Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: PT Citra Aditya Bakti, 2002.

[3] Anton, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online," J. Nurani, vol. 17, no. 2, p. 271, 2017.

[4] Supanto, "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy," J. Yustitia, vol. 6, no. 1, p. 54, 2016.

[5] I. M. P. Diantha, "Metodologi Penelitian Hukum Normatif," Teor. Metodol. Penelit. a., 2017.

[6] A. Ali, Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudance). Jakarta: Kencana Predana Media Group, 2009.