eduvest

Vol 1, No 4, April -, 2021
p-ISSN 2775-3735- e-ISSN 2775-3727

ISLAMIC CRIMINAL LAW ANALYSIS OF CYBER CRIMES ON CONSUMERS IN E-COMMERCE TRANSACTIONS

Jaenudin, Rasyida Rofiatun Nisa
UIN Sunan Gunung Djati Bandung
E-mail: jaenudin67@yahoo.co.id, rasyidaicha@gmail.com

Received:**April 3th, 2021**
Revised: **April 14th, 2021**
Approved:**April 16th, 2021**

Abstract

The purpose of this research is to study cyber crime in e-commerce transactions from the perspective of Islamic criminal law and how to deal with cyber crimes that harm consumers in e-commerce transactions according to the analysis of Islamic criminal law. This research is a normative legal research where laws are conceptualized as written regulations, or laws are conceptualized as rules or norms, the latter being a benchmark for human behavior, and considered appropriate to review written regulations. The results showed that cybercrime is a form of crime in the modern era. Therefore, according to the analysis of Islamic criminal law, cyber crimes can be punished by Ta'zir. For Syrians, ta'zir is a sanction based on disobedience, because it does not explicitly state the crimes contained in the Koran and Hadith.

***Keywords**:* Cyber Crime, E-Commerce, Islamic criminal law

INTRODUCTION

The development of e-commerce transactions cannot be separated from the growth of the internet, because e-commerce runs through the internet network. The rapid growth of internet users has made the internet an effective medium for companies to sell goods or services to potential consumers around the world (Halim, 2010). E-commerce is a modern business model that does not actually represent merchants and does not have an original signature. The existence of e-commerce can form a healthy competition between large and small businesses in the process of fighting for market share (Siregar et al., 2020). Even market share crosses national borders because activities on the Internet can reach the entire world. Some things in the real world may be far away and difficult to reach, but things in the virtual world can appear as if the world is nearby. Besides having many advantages, e-commerce can also cause many losses (Irmawati, 2011). This can open doors for criminals. The most obvious gap in the convenience provided by this technology is that there are no face-to-face transactions between buyers and sellers (Hardiawan & Sugiono, 2013). The negative impact of these technological developments gave birth to a new legal system called cybercrimes (Raodia, 2019).

Advances and convenience in technology have brought gaps for some people, and crime has changed (Setiawan, 2018). Many cases of fraud in e-commerce services occur, using two modes, namely hacking and online fraud. In this mode, the perpetrator will enter through the victim's account, then consume the balance that has been deposited by the consumer or take over the victim's credit card. If fraud occurs, the perpetrator usually represents a service company / online shop then asks for a code or password to verify the data (Utami, 2019).

The National Police's Criminal Investigation Agency's Cyber Crime Bureau revealed that the number of cybercrimes continues to increase every year, especially in e-

commerce-related fraud and hacking. In the end, the criminal motive for the purpose of money takes advantage of the payment gateway facility or currency deposit facility, where consumers first deposit a certain amount of currency for online transactions.

The increase in cybercrime-related to e-commerce is also caused by the easy access of criminals to fake account numbers and fake cellphone numbers to help criminals commit malicious acts without leaving any real traces (Sari et al., 2020). The emergence of abusive behavior in e-commerce transactions will raise various legal problems so that legal protection is needed for e-commerce transactions.

In Indonesia, currently, there is Law Number 11 of 2008 concerning Electronic Information and Transactions, which is considered as the law in Indonesia which regulates cybercrimes. This law defines cybercrimes or electronic crimes as an attempt to enter and or use computer facilities or computer networks without permission and unlawfully with or without causing changes and or damage to the computer facilities that are entered or used (Marita, 2015).

Islam emphasizes the existence of morals in buying and selling, such as healthy competition, honesty, openness, and justice. The application of these ethical values is the responsibility of every trader, including e-commerce transactions. For a Muslim, these values reflect his belief in Allah SWT. Even the Prophet Muhammad played the role of Mukhtasib (supervisor) in the market. He immediately criticized trade transactions that did not respect moral values (Rivai, 2012).

Basically, Indonesia has implemented several products of Islamic law, such as Qanun Hukum Jinayat and Fatwa DSN-MUI No. in Aceh. 05 / DSN-MUI / IV / 2000 About Greetings. Buying and selling online refers to buying and selling via advance trading, where the buying and selling contract via advance trading is a greeting. The Sharia Business Lawbook, (Mardani, 2014) explains that salam is a financing service related to buying and selling, financing, and ordering goods at once. A survey conducted by Kaspersky Lab in 26 countries/regions shows that Indonesia is one of the countries with the largest number of online fraud victims in the world, with 26% of consumers being victims (Manuhutu et al., 2021) Indonesia is still weak.

In addition, cybercrime occurs because of weak personal and social control (Habibi & Liviani, 2020). This is because such crimes are virtual crimes that are not visible to the naked eye. Normatively, cybercrime is a conventional crime but has new modes such as pornography, fraud, and defamation (Simbolon, 2018). By using the internet as a means of crime, criminal sanctions can be imposed in accordance with the provisions of the Criminal Law. At that moment similarly, new types of cybercrime such as hackers have emerged, which are not covered by the Criminal Law so that there is a legal vacuum.

As one of the makers of national criminal law, Islamic criminal law needs to conduct research and analysis on the contribution and important role of cybercrime which is not conducive to consumer e-commerce transactions. Cybercrime in Islamic criminal law is not much different in terms of its features and elements (Aulia, 2017). For example, theft, the elements contained in the theft are the property of both, such as theft does not belong to their rights, stealing without everyone's knowledge, wanting to own the item. and other elements. In terms of characteristics, both of them also have similarities, namely that there has been a legal incident.

Previously, there was a research that was relevant to this research, namely research conducted by (Mohammad Haidar Ali, 2012) with the title Cyber Crime according to the Law of the Republic of Indonesia Number 11 of 2008 concerning ITE (Islamic Criminal Law Perspective). In this research, cybercrime is seen from the point of view of Islamic criminal law, which is the main foundation for the juridical aspects, is the

theory of maqasid al-shari'ah that puts the principles that are the main considerations of legal objectives,

namely the realization of human benefit both in the world. Afterlife, namely the realization and maintenance of al-masalih al-khamsah or five basic needs in human life which include the maintenance of religion *(hifz al-din),* soul *(hifz alnafs),* descent or honor *(hifz al-nasl),* property *(hifz al -mal),* and reason *(hifz all).* So that the reality in cybercrime practices is considered to violate these five basic needs in human life. The criminal sanctions for fraud, decency, gambling, threats, destruction, and theft can be seen in the ITE Law. Whereas in Islamic criminal law, criminal sanctions are determined based on Jarimah Hudud, Jarimah *Qishas* and *Diyat*, and *Jarimah Ta'zir.*

In contrast to previous studies, this study focuses more on the analysis of cybercrimes that harm consumers in e-commerce transactions. So the main focus of this research is not only on cybercrime but also on the handling of e-commerce victims. Therefore, the purpose of this research is to study cybercrime in e-commerce transactions from the perspective of Islamic criminal law and how to deal with cyber crimes that harm consumers in e-commerce transactions according to the analysis of Islamic criminal law.

RESEARCH METHODS

This research uses the normative juridical method, namely by reviewing or analyzing supporting data in the form of legal materials (especially primary and secondary law). Understanding law as a set of rules or active norms in the legal system that governs human life. The norm in this study is descriptive analysis research, namely research that describes in detail the results of the analysis of relevant legal principles, legal systems, levels of vertical and horizontal synchronization, legal comparisons and positive law catalogs. Descriptive research aims to provide data that is as accurate as possible about humans, conditions, or other symptoms (Soekanto & Sulistyowati, 2013).

Meanwhile, normative legal research always focuses on secondary data sources. The data collection technique used was literature study from secondary data that had been analyzed.

RESULTS AND DISCUSSION

Cybercrime is a form of crime that has emerged in the modern era. Therefore, according to the analysis of Islamic criminal law, cyber crimes can be punished by Ta'zir. Ta'zir means prevention *(al-man'u)* according to the language. According to the term ta'zir, it is an educational punishment (*ta'dib*) in the sense that is meant through intimidation (*tankif*). For Syrians, taz'ir is a sanction based on disobedience, because it does not explicitly state the crimes contained in the Koran and Hadith. The kinds of ta'zir punishments can take the following form:

a) Death penalty;
b) If or whip 10 times;
c) Exile, boycott or prison;
d) Cross;
e) Compensation *(ghuramah)* or by means of confiscation;
f) Warning or advice;
g) Revocation of some assets (hurman);
h) Reproach *(taubikh);*
i) Preaching *(tasyhir);*

The form of ta'zir sanctions is only limited to these forms. The Caliph or Judge *(qadhi)* is given the right by the Shari'a to choose between the forms of sanctions and

determine the level, he may not determine sanctions other than that. The case of ta'zir is generally divided into:

a. Honor violations;
b. Offense against glory;
c. Deeds that destroy reason;
d. Violation of security disturbance of property;
e. Subversion;
f. Offenses related to religion;

From the perspective of Islamic criminal law, cybercrime includes actions that undermine social values in the world of information technology, and these actions have an impact on the entire society at home and abroad. When the traffic of cyberspace users becomes an economic and social victim, especially in the e-commerce market through fraudulent online shopping behavior, this behavior is detrimental to many consumers, you will feel this impact.

Therefore, cybercrime is prohibited by Allah SWT. Because Allah does not like people who harm and harm others. Destruction in any form is not justified, because it is an act that is contrary to universal values. Allah SWT expressly says in Surah Al-Maidah verse 64:

> *"The Jews say:" Allah's hand is bound ", actually their hands are bound and they are the ones who are damned because of what they have said. (Not so), but God's hands are open; He spent as He wanted. And the Quran that was revealed to you from your Lord will certainly increase iniquity and disbelief for most of them. And We have caused enmity and hatred between them until the Day of Resurrection. Every time they kindle the fire of war, Allah extinguishes it and they do damage on the face of the earth and Allah does not like those who do damage,".*

This verse confirms that destruction is prohibited by Allah SWT. In any form and anywhere, it still doesn't make sense. Hacker behavior is a very important part of the behavior and conduct of cybercriminals, and that behavior is prohibited in this paragraph. The foundation of the prohibition can cause things that are not good for others.

In Islamic criminal law, cybercrime is part of Jarimah ta'zir. Jarimah ta'zir is the finger and the punishment of syara which is hesitant, and the power to decide is given to the ulil amri (government/judge), with the consideration that this punishment can prevent the perpetrator from repeating and punishing. The sentence was adjusted according to the level of crime. Based on the method used, it can be seen that criminal sanctions for e-commerce services or so-called card swiping according to the ITE law are included in Article 30 and Article 31. These provisions are basically for visiting other people without the knowledge of the owner. Electronic system. In Islamic criminal law, the use of the qias method can see sanctions to eradicate crime, because the legal illusion is similar to theft.

Among the conventional laws that are deemed insufficient to solve cybercrime problems, the ITE law is expected to be the right answer. Islamic criminal law is Allah's Islamic law which contains the interests of the world and the future of human life. Basically, sharia law contains the basic obligations of every person to carry out Islamic teachings. The concept of the basic obligation of Sharia law is to make Allah the owner of all rights, including all the rights of oneself and others.

Everyone is a person who carries out Allah's orders and is obliged to carry out Allah's orders for the benefit of himself and others (H.Zainuddin Ali, 2019). The Criminal Code views cybercrime as a real crime whose modus operandi has been modernized and

whose substance is similar to Islamic Criminal Law. However, in the process of

determining the type of crime, there are similarities in the elements inherent in these types of crimes.

Jarimah is stated in Islamic Criminal Law as a criminal offense or a criminal act. If this is related to cybercrime then it becomes a fingertip, but cybercrime is a crime committed in cyberspace through electronic media and the internet. Jarimah is done in the real world. Looking at the reality of the cyber world, laws related to cybercrime must be focused on discussing Islamic criminal law because existing laws have not been implemented optimally. This is because existing laws are not taken from clear sources as legal products. In contrast to the situation of Islamic criminal law, the origin of Islamic criminal law is clearly derived from the Koran and the Sunnah. The clarity and purity of these sources can result in a legitimate and accountable product.

Electronic media is an alternative method of conducting e-commerce business transactions so that the consequence of this is that the payment system is very vulnerable to cybercrime. If the consequences of this act cause harm to other parties in the form of material or non-material or non-material disturbances (such as peace, dignity, customs, etc.), it can be said to be a criminal event. The reasons for this dangerous behavior include the character of a person who tends to benefit himself, even though the result of the choice or behavior is harmful to others. Therefore, cybercrime has become part of the same object of criminal behavior, which can be classified as a finger in Islamic criminal law. In this case, what needs to be emphasized is the extent to which criminal acts are resolved in cyberspace according to Islamic criminal law.

Abdul Wahid and Mohammad Labib wrote in their book: "Mayatara crime (cybercrime)". This book seeks to provide several solutions to the serious phenomenon of the new world of crime called cybercrime, which is described from the perspective of the sociology of law, legal criminology, and the application of alternative law. If the early prevention aspects are not explained in detail, this is considered insufficient (Wahid & Labib, 2015).

Therefore, it is necessary to emphasize prevention from an early age. Cybercrime is part of the same object of criminal behavior, which can be classified as a finger in Islamic criminal law. In this case, what needs to be emphasized is the extent to which the resolution of cybercrime is in accordance with Islamic criminal law. According to the division of Jarimah in Islamic criminal law, cybercrime is classified as Jarimah ta'zir.

This is due to the lack of Al-Quran text that explains the problem of cybercrime. However, if followed up further, you can find that Jarimah is included in the Jarimah Hudud category. This includes charges of adultery (slander), gambling or lottery, theft, and fraud. In general, cybercrime focuses more on types of criminal cases where physical contact does not occur in person and therefore does not involve cases involving physical contact. For example, in Articles 30 (1), (2), and (3), the ITE Law becomes the legal basis for combating crime (credit card crimes). In this case, there are several possibilities that can be done to sort out the perpetrators of the crime, namely theft or embezzlement of public funds. It could be argued that the perpetrator stole because he took things he shouldn't have done illegally. The object of theft can be various, one of which is through the use of e-commerce platforms.

It is called embezzlement because it uses a common method, namely changing or adding to data by entering false information into computer data. This operation is called data spoofing. Data processing from large companies (such as banks) usually involves some unethical people.

CONCLUSION

Cybercrime is a form of crime that has emerged in today's modern era. Thus, cybercrime according to the analysis of Islamic Criminal Law can be called ta'zir. Ta'zir according to the language means prevention (al-man'u). As for according to the term ta'ziricipation, it is educational (ta'dib) in the sense of delivering by means of frightening (tankif).

According Syrians, Ta'zir is a sanction based on disobedience, because the actions are not explicitly contained in the Koran and Hadith. From the perspective of Islamic criminal law, cybercrime includes acts that undermine social values in the world of information technology, and these acts have an impact on the entire society at home and abroad. When the traffic of cyberspace users becomes an economic and social victim, especially in the e-commerce market through fraudulent online shopping behavior, this behavior is detrimental to many consumers, you will feel this impact. Therefore, cybercrime is prohibited by Allah SWT. Because Allah does not like people who harm others.

REFERENCES

Ali, H. Zainuddin. (2019). Islamic Law: Introduction to Islamic Law in Indonesia.

Ali, Mohammad Haidar. (2012). Cyber Crime According to the Law of the Republic of Indonesia Number 11 of 2008 concerning ITE (Islamic Criminal Law Perspective). Alauddin State Islamic University Makassar.

Aulia, Alifa Akbar. (2017). Penalties for the perpetrators of criminal defamation through the internet according to Islamic criminal law. UIN Walisongo.

Habibi, Miftakhur Rokhman, & Liviani, Isnatul. (2020). Information Technology Crimes (Cyber Crime) and Countermeasures in the Indonesian Legal System. Al-Qanun: Journal of Islamic Law Thought and Renewal, 23 (2), 400–426.

Halim, Abdul Barkatullah. (2010). Consumer Rights. Bandung: Nusa Media.

Hardiawan, Anandya Cahya, & Sugiono, Sugiono. (2013). The Influence of Trust, Convenience, and Quality of Information on Online Purchasing Decisions (Studies on Users of the Online Buying and Selling Site Tokobagus. Com). Faculty of Economics and Business.

Irmawati, Dewi. (2011). Utilization of E-Commerce in the Business World. Scientific Journal of Business Oration – Issn, 2085, 1375.

Manuhutu, Melda Agnes, Muttaqin, Muttaqin, Irmayani, Deci, Tamara, Tomi, Gustiana, Zelvi, Hazriani, Hazriani, Manullang, Sardjana Orba, Jamaludin, Jamaludin, Iskandar, Akbar, & Negara, Edi Surya. (2021). Introduction to Information Technology Forensics. Our Writing Foundation.

Mardani. (2014). Sharia Business Law. Jakarta: Kencana Prenada Media Group.

Marita, Lita Sari. (2015). Cyber Crime and the Application of Cyber Law in the Eradication of Cyber Law in Indonesia. Horizons-Journal of Humanities, 15 (2).

Raodia, Raodia. (2019). The Influence of Technology Development on the Occurrence of Mayantara Crime (Cybercrime). Jurisprudentie: Department of Law, Faculty of Sharia and Law, 6 (2), 230–239.

Rivai, Veitzal. (2012). The specialty of Islamic economics in accelerating the economic growth of the people. Journal Analytica Islamica, 1 (2), 330–389.

Sari, Ika Yusnita, Muttaqin, Muttaqin, Jamaludin, Jamaludin, Simarmata, Janner, Rahman, M.Arif, Iskandar, Akbar, Pakpahan, Andrew Fernando, Abdul Karim

Sugianto, Giap, Yo Ceng, & Hazriani, Hazriani. (2020). Data and Information Security. Our Writing Foundation.

Setiawan, Daryanto. (2018). The Impact of Information and Communication Technology Development on Culture. Symbolic Journal: Research And Learning In Communication Study, 4 (1), 62–72.

Simbolon, arise. (2018). Criminal Law Policy Against the Crime of Defamation or Defamation through the Internet in Indonesia as Cybercrime. Faculty of Law, Unissula.

Siregar, Dodi, Purnomo, Agung, Mastuti, Rini, Napitupulu, Darmawan, Sadalia, Isfenti, Sutiksno, Dian Utami, Putra, Surya Hendra, Sahir, Syafrida Hafni, Revida, Erika, & Simarmata, Janner. (2020). Technopreneurship: Strategy And Innovation. Our Writing Foundation.

Soekanto, Soerjono, & Sulistyowati, Budi. (2013). Sociology of an Introduction, Cet. 45; Pt. Raja Grafindo Persada, Jakarta.

Utami, Muthiah Nafisah. (2019). Crime of Hacking (Hacking) and Extortion of 3000 Websites in 44 Countries by Surabaya Black Hat Associated with Uu No. 19 of 2016 concerning Information Technology and Electronic (ITE). Faculty of Law Unpas.

Wahid, Abdul, & Labib, Mohammad. (2015). Mayantara's Crimes, Aditama Bandung: Pt. Refika.