LEGAL PROTECTION OF ONLINE FRAUD VICTIMS IN THE DIGITAL ERA

Rahmayanti
Panca Budi Development University
Email : rahmayanti@dosen.pancabudi.ac.id

ABSTRACT

The development of the times is always followed by technological developments,digital technology has had a major influence on human life. Where technology now makes it very easy to do activities, but this convenience is misused by certainelements, giving rise to new problems that are accepted by humans, such as online fraud in today's digital era. The form of legal protection for victims of online fraud is seen from the perspective of the Electronic Information and Transaction Law. The research objective is to find out legal protection, barriersand solutions for victims of online fraud in the digital era. The method used is normative legal research with statutory and conceptual approaches. Crimes committed by perpetrators of online fraud crimes.

Keywords: Victims, Online Fraud, Digital Age

INTRODUCTION

Science, technology and art ushered people into the digital era which gave birth to the internet as a network and also a symbol of exclusivity.[1]The internet is described as a collectionof computer networks consisting of a number of smaller networks that have different networksystems.

Criminal acts occur in society, one of which is the crime of fraud, even today there aremany criminal acts of fraud with various forms and developments, showing the higher level ofintellectuality of increasingly complex fraud crimes. Acts of fraud are always there and even tend to increase and develop in society along with economic progress, even though these acts of fraud are seen from any angle as highly reprehensible, because they can create mutual distrust and as a result damage the order of people's lives. Fraud is an act of a person or groupof people giving the impression that something is true and not false to make other people givecredence. Formally, deception is defined as the act of "persuading others by trickery,

The digital era is a contemporary development that has an influence in encouraging theemergence of various possibilities regarding world changes that will take place. The influenceof the digital era can remove various obstacles and obstacles that make each other more and more. There are two impacts from the development of this digital era,

the first is a positive impact, namely the progress of information and technology that facilitates and accelerates access to the information needed. Such as access in business interests, buying and selling transactions from companies or companies, and the process of communicating is not hinderedat any time and place. The second negative impact of technological sophistication is cybercrime.

The legal construction governing criminal acts through electronic means is currently regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), so that with the passing of thislaw as intended, the law in the field of information technology has become a separate field to ensnare perpetrators of criminal acts using electronic means. Referring to Article 35 in conjunction with Article 51 paragraph (1) of the ITE Law which states that "Every person intentionally and without rights or against the law manipulates, creates, changes, removes, tampering with electronic information and/or electronic documents with the aim that the electronic information and/or electronic documents are deemed as authentic data is punishableby imprisonment for a maximum of 12 (twelve) years and/or a fine of up to Rp. 12,000,000,000.00 (twelve billion rupiah)". In general, the regulation of a criminal act of fraud is contained inArticle 378 of the Criminal Code concerning Fraud. This article does not specifically regulateonline fraud, but regulates fraud as a whole (in its main form). Article 378 of the Criminal Codeconcerning Fraud regulates acts intended to benefit oneself or others by using a false name or dignity, by deception or by lying to hand over something of value to him.

In the ITE Law, it can be seen that there is only one main criminal article and criminalthreats given to the perpetrators but it has not explained how to protect the victim, what kind of protection can the victim get after the case is over with material and immaterial losses suffered by the victim. Compensation for victims who have been harmed is a legal protection for victims where victims can get certainty, victims are not only protected by legal witnesses but how to achieve the victims' rights afterwards.

Based on the description above, the researcher proposes the following problem formulation: 1) What is the legal protection for victims of fraud in the digital era? 2) What arethe obstacles and solutions in legal protection for victims of fraud in the digital era?

METHOD

The research method used in this study is a normative juridical method, as a logical consequence of the nature of sui generis jurisprudence, using secondary data, namely primarylegal materials and secondary legal materials. Primary legal materials are binding legalmaterials, so in this study primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), the Criminal Code, secondary legal material, namely data obtained from library research and documentation, which is the result of research and processing of other people, which is already available in theform of literature or documentation.

RESULT AND DISCUSSION

A. Legal Protection for Victims of Fraud in the Digital Age

Indonesia is a constitutional state, where in regulating society a system is needed so that social inequality does not occur between communities, and the system itself is called the legal system.[4]A law enforcement is believed to be able to regulate all actions in society, eitherin general or specifically.[5]The presence of technology at this time makes people increasingly keep abreast of developments. Including the development of a crime, namely crime through electronic means. The development of an era will trigger the development of a crime, none other than the majority of crimes that occur in criminal acts. Criminal law is basically public law, in which criminal acts occur because individuals or groups violate a rule of law for their own or group interests.

The main factor in the occurrence of criminal acts of fraud is falsification of evidence which is ultimately said to be authentic evidence so that the aggrieved party believes. If we return to Article 378 of the Criminal Code concerning Fraud, there are elements of fulfilling aperson who is said to be a party who will be legally charged in criminal acts of electronic means. So there are also elements of online fraud that are not fulfilled in the provisions of Article 378 of the Criminal Code concerning Fraud, namely: 1) The main media elements usedin carrying out online fraud crimes are not fulfilled, namely electronic media that are not yet known in the Criminal Code and the Criminal Procedure Code. ; 2) Different methods of fraudbetween conventional fraud and online fraud;

Article 378 of the Criminal Code, Whoever with the intent to benefit himself or others against his rights, uses a false name or false character or uses deception or arrangement of lyingwords, moves other people to surrender an object or enters into a debt agreement or negates a receivable, because of having committed fraud, is punishable by imprisonment for a maximumof four years.

Regarding the crime of fraud in Article 378 of the Criminal Code as follows:

1) This crime is called the crime of fraud. Fraud is his job:
    a. Persuading people to give away goods, create debts or write off receivables.
    b. The purpose of the persuasion is to benefit oneself or others by violating rights.
    c. Coax him into it by using:
    d. Fake name or fake state
    e. Clever sense (trick) or
    f. Lies essay
2) Persuading, namely exercising influence by cunning over people, so that person according to him does something when he knows the real situation.
3) Regarding the goods there is no mention of a restriction, that the goods must belong tosomeone else, so persuading people to hand over the goods themselves,

can also be considered fraud, as long as other elements are met.

4) As is the case with theft, if fraud is committed within a family circle, the regulations referred to in Article 367 Jo 394 apply.

Apart from being regulated in the Criminal Code, fraud is also specifically regulated inLaw Number 19 of 2016 if the perpetrator uses additional media known as Cyber Crime, namely in this law has discussed matters related to electronic information. , electronic transactions, and also regulates things that are prohibited related to "cyberspace" along with criminal threats. The ITE Law, the article that regulates criminal acts of fraud, especially on the internet, is regulated in Article 28 paragraph (1), which reads as follows: (1) "Anyone whodeliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions" the criminal threat that can be imposed on the perpetrator isimprisonment for a maximum of 6 (six) years and/or a fine of up to Rp. 1 billion.

b. Obstacles And Solutions In Legal Protection Against Victims Of Fraud In The Digital Age

Providing legal protection to victims of fraud is not easy. Especially with online fraud crimes in today's digital era. The large number of crimes that are currently being committed using technology or through digital platforms that have developed to date is one reason why inthis day and age law and technology are related.

Law Number 11 of 2008 concerning Information and Electronic Transactions. However, Law Number 11 of 2008 does not specifically regulate criminal acts of fraud, but related to consumer losses in electronic transactions, there is a provision in Article 28 paragraph

(1) of Law Number 11 of 2008 concerning Information and Electronic Transactions, hereinafterreferred to as with the ITE Law states: "Every person intentionally, and without right spreads false and misleading news that results in consumer losses in Electronic Transactions." Violations of Article 28 paragraph (1) of the ITE Law are subject to a maximum imprisonmentof six years and/or a maximum fine of Rp. 1 billion, according to the provisions of Article 45 paragraph (2) of the ITE Law.

According to Barda Nawawi Arief, this evaluation or review needs to be carried out, because there is a close link between legislative policy formulation and law enforcement policyand crime eradication/control policies (criminal policy). Weaknesses in criminal law formulation policies will affect criminal law enforcement policies and crime prevention policies.

Law enforcers in Indonesia are currently experiencing difficulties in dealing with the spread of cybercrime. This is motivated by the fact that at least law enforcement officials understand the ins and outs of information technology (internet), limited facilities and infrastructure, and the lack of public awareness of law in efforts to deal with information technology crimes. In addition, law enforcement officials in the regions are not ready to anticipate the rise of this crime because there are still many law enforcement officers who are technologically illiterate. Limitations of special cybercrime tools owned

by the Police in districtareas up to the sub-district level to support investigator facilities in uncovering criminal acts ofelectronic transaction fraud. The limitations of modern tools in the regions cause it to take quitea long time to uncover crimes of electronic transaction fraud and the tools needed also requirea large amount of money. Nobody can deny that technology can be a tool for change in society.Such is the importance of the function of technology, that it seems that today's society is very dependent on technology, both for positive and negative things. The limitations of modern toolsin the regions cause it to take quite a long time to uncover crimes of electronic transaction fraudand the tools needed also require a large amount of money. Nobody can deny that technology can be a tool for change in society. Such is the importance of the function of technology, that it seems that today's society is very dependent on technology, both for positive and negative things. The limitations of modern tools in the regions cause a long time to uncover crimes of electronic transaction fraud and the tools needed also require a large amount of money. Nobody can deny that technology can be a tool for change in society. Such is the importance of the function of technology, that it seems that today's society is very dependent on technology, bothfor positive and negative things.

Increasing internet penetration opens up many gaps for the emergence of various cybercrimes.How to avoid online or online scams? The following are prevention efforts againstonline fraud, namely:

1. The public can use services that can be used to check the status or level of trustfrom account numbers or telephone numbers such as the CekRekening.id service or the GetContact application;
2. Be alert if someone requests an OTP code via email, chat application, telephoneor SMS from those who claim to be an official institution;
3. Be alert to fake or phishing sites and scams by using the call forwarding feature;
4. Don't be easily tempted by the low price of a product;
5. Read reviews and testimonials from other buyers of a sales platform;
6. Always save proof of payment transactions;
7. Checking the identity of the seller, by:
    a. Check the followers of the account in question, does it make sense between thenumber of followers with likes and comments on each post,
    b. Check whether the comment column for the account is turned off or not. If it isturned off, the public should be suspicious,
    c. Check the number of items sold. If only a few items are detected for sale, thenit should be considered in making a transaction;
8. Pay attention to the payment method, it is recommended to avoid paying directly to the seller's bank account for any reason. To be safer, you can transactdirectly through the payment methods available on e-commerce.

In the field of regulation, Indonesia already has comprehensive arrangements with the ITE, PK and Trade Laws, and Government Regulation no. 82 of 2012 concerning Implementation of Financial Systems and Transactions. In terms of infrastructure, an agency that oversees data traffic has been established, namely Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet and Infrastructure/ Coordination Center) which has the main task of conducting socialization with related parties regarding IT security (IT security), perform monitoring, detection, and early warning of network threats from within and outside the country.

CONCLUSION

Legal protection and a sense of security for all legal actions in the form of electronic transactions, one of which is the issuance of Law Number 11 of 2008 concerning Information and Electronic Transactions. legal protection given to victims of online fraud, namely Preventive Law protection and Repressive Law. Preventive in the form of protection provided by the government with the aim of preventing violations beforethey occur. Repressive is the final protection in the form of sanctions such as fines, imprisonment, and additional penalties given when a dispute has occurred or an offensehas been committed.

Obstacles in legal protection for victims of fraud in the digital era, namelythere are stillvery few law enforcement officials who understand the ins and outs of information technology (internet), limited facilities and infrastructure, and a lack of public legal awareness in efforts to deal with information technology crimes. Solutionin legal protection against victims of fraud in the digital era namelyestablished an agency that oversees data traffic, namely Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet and Infrastructure/ Coordination Center) which has the main task of conducting socialization with related parties regarding IT security (IT security), monitoring, detecting , and early warning of network threats from within and outside the country.

REFERENCES

Barda Nawawi Arief, 2007, Law Enforcement Issues and Criminal Law Policy inCrime Control, Jakarta.

Maskun. 2013, Cyber Crime Cybercrime. Jakarta: Kencana.

Maskun and Wiwik Meilarati, 2017, Legal Aspects of Internet-Based Fraud, Bandung: CVKeni Media.

Prasetyo, RD (2014). Criminal Accountability of Online Fraud Offenders

In Positive Criminal Law in Indonesia (Doctoral dissertation, Brawijaya University).

Rahmad, N. 2019. Legal Studies of Online Fraud Crimes. JournalSharia Economic Law, 3(2), 103-117.

Sinaga, EP, & Alhakim, A. (2022). Juridical Review of Legal Protection for

Users of Illegal Online Loan Services in Indonesia. UNES Law Review, 4(3), 283-296.

Simamora, J. 2014. Interpretation of the meaning of the rule of law in the perspective of the constitution

Republic of Indonesia 1945. Journal of Legal Dynamics, 14(3), 547-561.

Widodo. 2013, Criminal Law in Information Technology. Yogyakarta: Aswara Persindo