Legal Consequences for Perpetrators of Online Fraud Crimes on Electronic Social Media.

Andien Mutiara Zahra Faculty of Law, Universitas Muslim Indonesia, Indonesia
Mulyati Pawennai Faculty of Law, Universitas Muslim Indonesia, Indonesia
Muhammad Faisal Faculty of Law, Universitas Muslim Indonesia, Indonesia

This study aims to find out and analyze the legal consequences for perpetrators of online fraud through electronic social media. To find out and analyze legal efforts for victims of online fraud on social media. This study uses an empirical legal research method by focusing on analyzing primary data and secondary data using qualitative data analysis techniques. The results of this study indicate that the legal consequences for perpetrators of online fraud through electronic social media. The application of legal sanctions for perpetrators of online investment fraud has not been expressly regulated in a special law that can provide criminal penalties for perpetrators but is regulated in the Criminal Code Article 372 with a maximum imprisonment of four years or a maximum fine of nine hundred rupiah, and Article 378 with a maximum imprisonment of 4 (four) years. Efforts to provide countermeasures in providing criminal policies are carried out with the criminalization aspect of criminal law, namely by forming special laws to regulate things that are prohibited in this case. Legal action is a solution provided by law to victims whose rights to justice are not fulfilled, as well as providing relief and peace of mind for the criminal acts that befell them. Online Fraud Actions involve the following steps such as Legal Efforts through Litigation, and Legal Efforts through Non-Litigation. This Research Recommendation Should be the Urgency of Making Regulations or Legal Arrangements for Investment or Commonly Called Online Capital Investment Specifically in Order to Provide Criminal Aggravation and Strengthen Criminal Sanctions for Online Fraud Perpetrators for the Purpose of the Law, namely Legal Certainty, Justice and Benefit. The State in Protecting Online Practices Should Make Regulations That Specifically and Firmly Regulate the Aspects of Investment Practices or Online Capital Investment in Order to Achieve Legal Certainty.

INTRODUCTION

Internet fraud also invites debate and difficulty for law enforcement in handling it, in contrast to fraud as regulated in Article 378 of the Criminal Code which reads: Whoever with the intention of benefiting himself or another person unlawfully, by using a name or a composition of false words, moves someone to hand over an object, to enter into a debt agreement or to cancel a receivable, because he has committed fraud, is punished with a maximum prison sentence of four years. [1]

Talking about the limitations or weaknesses of criminal law governing cybercrime, Law Number 11 of 2008 concerning Information and Electronic Transactions was formed, because the Criminal Code and Criminal Procedure Code can no longer reach or anticipate crimes that are developing today. Of course, in the implementation of the Law on Information and Electronic Transactions, law enforcement officers face new things in the way of proof.

The development of the modus operandi of fraud crimes shows a widespread and increasingly sophisticated scale. Not only is fraud varied, various kinds of social media applications are mushrooming in society. Its use is not only adults, but children can also access social media. All activities ranging from teaching and learning activities, office work, shopping for daily needs via

the internet/online. Related to this fraud, many irresponsible individuals take advantage of the situation so that it causes fraud. [2] One example is a computerized telephone that appears on a gadget as if it were from the gadget owner's area, but in reality it comes from another area or even another country. So it is increasingly difficult to catch and prosecute criminals.

Fraudulent acts always exist and tend to increase and develop in society along with economic progress, even though fraudulent acts are seen from any angle as being very reprehensible because they can give rise to feelings of mutual distrust and as a result damage the social order of life. [2]

The Criminal Code (KUHP) itself in Article 378 emphasizes that a person who commits a crime of fraud is threatened with criminal sanctions. Thus, it is still considered ineffective in enforcing it against violators, because in enforcing criminal law, it is not enough to only regulate an act in a law, but also requires law enforcement as the implementer of the provisions of the law and institutions authorized to handle a crime such as the police, prosecutors, courts. Fraud cases have recently been growing and often occur even though this crime has been regulated in the Criminal Code, in addition to being regulated in the Criminal Code, fraud is also regulated in the Electronic Information and Transactions Law to deal with fraud in cyberspace that the increasing number of frauds in today's era that occurs in society, especially fraud using social media such as Facebook, Twitter, Whatsapp, Instagram, and other media that are misused by humans to generate profits by justifying all means. [3] This fraud has long been disturbing the community, many people have become victims of this fraud and many perpetrators have been caught.

From the theory above, Allah SWT says in Surah Al-Baqarah verse 10 which reads: [4] It means. In their hearts is a disease, so Allah increased their disease and they received a painful punishment because they used to lie.

This is because in their hearts there are diseases, such as envy and envy towards those who believe, doubts about the teachings of Islam, wrong beliefs, and so on, then Allah makes the disease worse with a great victory for those who believe. This victory really hurt them because of the envy, envy and arrogance that existed within them. Their doubts became even more intense. And, as a result, apart from suffering in the world, they will suffer a painful punishment, because they lied by showing faith even though their hearts were disbelieved. [4]

This online arisan fraud has been so rampant, including in the city of Makassar, one of the cases of online arisan fraud in the city of Makassar, in the case of online arisan fraud investigators have named 3 (three) managers of online arisan and fraudulent investments as suspects. Each of the initiators of the arisan with the initials LSD and his girlfriend AR who acted as the owner of the holding account. The funds that were deposited first went into AR's account if the victim wanted to join as a member.

The suspects created a social gathering group. From the initial investigation, it was said, the suspects conspired to manage this online social gathering. They divided 300 members into a WhatsApp group, this suspect held one admin related to investment (social gathering), the group was divided into various types of social gathering where the social gathering prizes were different. For one of the previous admins, he held three social gatherings. One social gathering per 20 days, one social gathering for 10 days and an iPhone or cellphone social gathering, through that group each admin conveyed information about this social gathering, including if one of the members received the social gathering. The social gathering money will be transferred to the perpetrator's account, until now the police at the Makassar Police are still opening the door to reporting for victims who feel disadvantaged due to fraud under the guise of online social gathering and fraudulent investment in Makassar. From the results of the investigation, there were ten victims who had reported to the Makassar Police.

This online fraud has caused a lot of harm to the community, based on the problems above, the author is interested in discussing the application of criminal sanctions for online arisan fraud in

Makassar City. For this reason, the author conducted a study in the form of legal writing entitled "Legal Consequences for Perpetrators of Criminal Acts of Fraud Through Arisan Mode on Electronic Social Media.

The formulation of the problem of this study is What are the legal consequences for perpetrators of online fraud through electronic social media? What are the legal remedies for victims of online fraud on social media?

The purpose of this study is to determine and analyze the legal consequences for perpetrators of online fraud through electronic social media. To determine and analyze legal efforts for victims of online fraud on social media.

The benefits of this research are, as a contribution to law faculty students in general and for the author himself for the development of legal science, the results of the research can be used as reference material, sources of information and contributions of thought that are expected to be useful for students and as literature for readers and as input for researchers in conducting research in the same field , especially from other sides of this research.

METHOD

In terms of the focus of the study, the legal research conducted is included in the type of empirical research. Empirical Legal Research is a legal research that attempts to see the law in a real sense or can be said to see, examine how the law works in society [5] . The approach used to answer the formulation of the problem in legal research uses several approaches. These approaches include the statutory approach, the conceptual approach and the historical approach . What can be used as an object in research with a normative doctrinal approach is data in the form of primary materials and secondary legal materials and tertiary legal materials. This research was conducted through a literature study (library search), a literature study or normative research only by reading or analyzing written materials. The legal material collection technique that will be used in this research is through interviews and library research, namely the legal material collection technique by searching, recording, inventorying, studying books, literature, laws and regulations, previous research results, and documentation related to the problem being studied.

DISCUSSION

Legal Settlement Process for Violations of the Police Professional Code of Ethics

One type of crime that commonly occurs in society is fraud, which is now increasingly complex and diverse in form along with the increasing level of intelligence in carrying out fraudulent acts. Fraud is included in the category of crimes against other people's wealth and is generally regulated in Book II Chapter XXV of the Criminal Code.

Article 378 of the Criminal Code explains fraud in general, while in Chapter XXV of Book II of the Criminal Code, there are variations of fraud against property which are described in several articles with different names as special forms of fraud. The following are several types of fraud crimes that exist:

“Primary Fraud (Article 378 of the Criminal Code)

Minor Fraud (Article 379 of the Criminal Code)

Fraud in Buying and Selling (Article 379a of the Criminal Code, Article 383 of the Criminal Code,

and Article 386 of the Criminal Code)

Fraud in Scientific Works and Others (Article 380 of the Criminal Code)

. Fraud in Insurance (Article 381 of the Criminal Code and Article 382 of the Criminal Code) f. Fraudulent Competition (Article 382bis of the Criminal Code)

Stellionaat (Article 385 of the Criminal Code)

Fraud in Contracting (Article 387 of the Criminal Code)

Fraud Against Yard Boundaries (Article 389 of the Criminal Code).

Broadcasting of False News (Article 392 of the Criminal Code) k. Fraud by providing a false description of securities (Article 391 of the Criminal Code)

Fraud by preparing false balance sheets (Article 392 of the Criminal Code).”

Article 378 of the Criminal Code stipulates the following: "Anyone who with the intention of benefiting himself or another person against their rights, either by using a false name, either by means of trickery and deceit or by fabricating falsehoods, persuades someone to give something, create debt or extinguish debts, shall be punished for fraud, with a maximum prison sentence of four years." The essence of the crime of fraud involves a number of elements listed below. [6]

Based on Article 184 of the Criminal Procedure Code, electronic information is not included in valid evidence. However, if we start from Article 5 paragraph (2) of the ITE Law and its Explanation, electronic information is categorized as "an expansion of valid evidence". Electronic information (dhi. Cell Data Record) obtained from the provider, then the employee of the provider will be examined as an expert who explains the Cell Data Record as electronic information. Related to electronic information in the form of cloning results of cellphones from Cellebrite UFED 4PC can be printed into written evidence which in the perspective of the ITE Law is called "electronic data".

The electronic data obtained must also be explained by a digital forensic expert to become valid evidence based on Article 184 of the Criminal Procedure Code and Article 5 paragraph (2) of the ITE Law and its Explanation. [7] The expert who explains the digital evidence must make a report on the analysis he/she conducted. This report is attached as written evidence based on Article 184 of the Criminal Procedure Code. In addition, the report of the digital forensic expert can also be used in court, if the case has entered the prosecution stage in court. In the case where the evidence used is digital evidence, a forensic expert is needed to present it before the panel of judges. [8] Activities carried out by investigators to reveal their findings to the authorities or in court. Usually the presentation of data is carried out by a forensic expert to explain things that are difficult for the general public to understand, so that the data can help the investigation process to find the suspect.

According to the Director of Special Criminal Investigation of the South Sulawesi Regional Police, Dedi Supriadi, said that: The Criminal Code as the main legal basis for criminal punishment in Indonesia has regulated the rules prohibiting criminal acts of fraud as stated in Article 378 of the Criminal Code. The element of fraud in Article 378 of the Criminal Code is still conventional fraud, namely fraud that generally occurs and is intended for all things in the real world. The use of Article 378 of the Criminal Code is less appropriate if used to ensnare online fraud in cyberspace using electronic media as a means to commit the crime, due to limitations in evidence that is limited by the Criminal Procedure Code and jurisdictional issues in handling cybercrime cases.

Data from the Directorate of Special Criminal Investigation of the South Sulawesi Regional Police

Online Fraud Cases	
Year	Amount
2020	172
2021	220
2022	270
2023	310

Cyber Crime Directorate of Special Criminal Investigation of the South Sulawesi Regional Police. Since 2020 to 2023 there has been a significant increase in the number of Police reports regarding Online Fraud Crimes reported by the public, namely in 2020 there were 172 cases per year that were handled, then in 2021 there was an increase of 220 cases per year, then in 2022 there was another increase to 270 cases per year, and the most experienced spike was in 2023, namely there were 310 cases up to October 2023. The increase in Online Fraud cases cannot be denied because people's electronic transaction activities using the internet as a medium have a very large influence. [9]

The legal dysfunction can be overcome in several ways, one of which is by applying the principle or legal doctrine of lex specialis derogat legi generalis. Article 28 paragraph (1) of the ITE Law has more specific elemental characteristics compared to Article 378 of the Criminal Code in the context of criminalization of online fraud crimes, it can be said that Article 28 paragraph (1) of the ITE Law is lex specialis derogat legi generalis of Article 378 of the Criminal Code. In addition to having more specific elemental characteristics in the context of criminalization of online fraud crimes, Article 28 paragraph (1) of the ITE Law has fulfilled several principles in the principle of lex specialis derogat legi generalis, namely: [10]

The provisions found in general legal rules remain valid, except those specifically regulated in the special legal rules.

The provisions of lex specialis must be equal to the provisions of lex generalis (law with law).

The provisions of lex specialis must be in the same legal environment (regime) as lex generalis.

Why are online fraud cases rampant, because people tend to easily believe information in cyberspace such as offers of cheap goods, business investments, or job vacancies. [9] People are too gullible, even though they don't know who is playing a role behind the scenes. Gullible so that their minds are easily manipulated to believe in a truth, even though it is not necessarily true. This ability to manipulate data and thoughts is what is used by fraudsters to commit crimes. Check and recheck before making a transaction, first make sure the data is correct, the certainty of the data, make sure there is a person behind the screen who operates the electronic device.

According to the Director of Special Criminal Investigation of the South Sulawesi Regional Police, Dedi Supriadi, he said that:

"In terms of disclosing Online Arisan Fraud, Investigators are very careful in tracking because perpetrators tend to easily remove evidence in the form of electronic devices used for work, for example, mobile phones, laptops, or deleting accounts used to cheat. Because in conducting investigations, investigators focus more on pursuing the electronic devices used, not the perpetrators whose identity is not yet known, later after the perpetrators who operate the device can be caught, then it can be concluded who the suspect is."

Someone who intentionally commits fraudulent arisan bodong 6 years and a maximum fine of one billion rupiah. So, anyone who lies and misleads others in electronic transactions can be prosecuted to be held accountable for their actions with a prison sentence of 6 years and a maximum fine of

one billion rupiah.

According to the Director of Special Criminal Investigation of the South Sulawesi Regional Police, Dedi Supriadi,

"Criminal sanctions for crimes that are the same as conventional fraud are regulated both in the old Criminal Code which is still in effect at the time this article was published and the 2022 RKUHP which has received joint approval from the President and the DPR ("RKUHP") which will come into effect 3 years from the date of enactment, namely in 2025. The ITE Law and its amendments do not explicitly regulate online fraud. The following is the text of Article 28 paragraph (1) of the ITE Law, namely that anyone who intentionally and without the right to spread false and misleading news that results in consumer losses in electronic transactions shall be subject to a maximum imprisonment of 6 years and/or a maximum fine of IDR 1 billion.

In addition, the scheme of inviting members and asking members to find new members is an activity with a Ponzi scheme. This activity has been clearly prohibited in Article 9 of Law No. 7 of 2014. This article states that distribution business actors are prohibited from implementing a pyramid scheme system in distributing goods. According to Article 3 of Law No. 7 of 2014, goods are any object, whether tangible or intangible, whether movable or immovable, whether consumable or non-consumable, and can be traded, used, utilized, or utilized by consumers or business actors. Arisan activities are activities that trade money and members can be promised bonuses. This means that arisan is an activity that has goods, namely money. This prohibition is also emphasized in Article 21 letter k of the Regulation of the Minister of Trade Number 70 of 2019 concerning Direct Distribution of Goods ("Permendag 70/2019") that companies that already have a trade business license are prohibited from carrying out activities by forming a marketing network using a pyramid scheme. This means that it is clear that investment services or arisan with a Ponzi scheme are services that do not meet the standards recognized in Indonesia. So, if there are individuals who admit to failing to pay or being negligent after using a fake Ponzi scheme, then they must still be held criminally responsible. [11]

Article 378 of the current Criminal Code (KUHP) regulates the crime of fraud. The article states that a person who with the intention of unlawfully benefiting himself or another person, by using a false name, by trickery, or by a series of lies, induces another person to give something to him, or to give a loan or to cancel a debt, can be punished. Four years' imprisonment is the maximum penalty for this offense.

In the Electronic Information and Transactions Law, the agreement provides general limitations. As explained in Article 1 number 17 of the ITE Law, electronic systems can be used by various parties who need to enter into agreements. [12] However, the electronic system in question includes a series of procedures and electronic devices used to distribute, transmit, announce, display, store, analyze, process, and collect electronic information. Electronic information is a collection of various forms of data that are processed and have a meaning that can be understood by people who understand them, such as symbols, access codes, letters, numbers, telecopy, telegram, telex, EDI, email, designs, writings, maps, photos, images, and sounds, as explained in the sentence above. A brief explanation of the validity of electronic agreements or contracts is given in the ITE Law. In addition, in accordance with Article 18 paragraph (1) of the ITE Law, both parties have a strong relationship with the Electronic Contract made through Electronic Transactions. Therefore, it is very important for the parties involved in the agreement to understand and comply with the terms and conditions stated in the electronic contract or agreement. Therefore, the relevant articles must be examined thoroughly. In order to be protected by law, an agreement must meet all the requirements set out in the Civil Code. In order to be considered valid, an agreement must also comply with the applicable legal framework governing electronic transactions. According to Article 5 paragraph (I) of the ITE Law, valid evidence is considered valid if it includes printouts, electronic documents, and electronic information, and meets the formal and material requirements outlined in the ITE Law. Electronic information includes various forms of electronic data, including voice,

writing, images, and photos, as outlined in the general provisions of the ITE Law. Some types of electronic evidence are as follows: [13]

Legitimate electronic evidence includes Online fraud, also known as electronic transaction fraud, is a crime that involves the use of computers, devices, and internet networks to carry out fraudulent activities.

Electronic transactions have many features, one of which is borderless. Despite capital constraints, online businesses can operate in multiple countries and attract a wide consumer base.

Transaction anonymity means that transactions can be conducted without the exchange of personal information between the seller and the buyer. Digital and non-digital goods/products: This category covers a wide range of goods. Digital products, such as software that can be downloaded online, fall into this category, while non-digital goods include a variety of physical goods, such as electronics, clothing, vehicles, etc. "Intangible goods" or "intangible goods" refer to products that cannot be physically purchased, such as files, software, or ideas, which are typically sold online.

Law No. 11 of 2008 regulates electronic transactions and information. In the ITE Law, there is no specific clause that regulates fraud committed through electronic media. However, in situations like this, Article 378 of the Criminal Code can be used. If someone intentionally seeks personal or other people's gain by forcing others to provide goods or eliminate receivables, they can be sentenced to up to four years in prison. Although the ITE Law does not specifically address electronic media fraud, there is growing concern about consumer losses caused by electronic transactions. [14] Article 28 paragraph 1 of the ITE Law indicates that someone who spreads false information can be held responsible for the financial losses of others. Article 45A paragraph 1 of Law No. 19 of 2016 stipulates sanctions for those who violate Article 28 paragraph 1 of the ITE Law. In accordance with Article 28 paragraph 1 of the ITE Law, people who intentionally spread false news can be sentenced to up to 6 years in prison and a fine of up to 1 billion rupiah.

Article 378 of the Criminal Code and Article 28 paragraph 1 of the ITE Law are different. Article 378 regulates fraud, while Article 28 paragraph 1 regulates fake news that can harm consumers when they make electronic media transactions. Arisan activities have used this tool to expand their membership base and increase the amount of money involved due to the rapid advancement of information technology. Using social media for any purpose, including participating in online arisan, is permissible. To maintain the welfare of all parties involved, such activities must be carried out with integrity, transparency, and accountability, as well as ensuring compliance with agreements and legal requirements.

Action for Victims of Online Fraud on Social Media

Criminal law is based on the basis or rules adopted by a country. So in fact criminal law is divided into two, namely formal criminal law and material criminal law. [15] Talking about material law. Criminal law that is included in material is a rule that is related to a prohibited event, where in this case the existence of rules regarding the imposition of criminal law and criminal procedures for perpetrators or convicts is a legal provision that can be used as a reference for the law enforcement process. While law enforcement can be concluded as a legal effort as it should be. Namely, it can monitor an event so that a violation does not occur and if the violation occurs, it must be immediately restored, that is what we can conclude with the law enforcement process.

According to the Director of Special Criminal Investigation of the South Sulawesi Regional Police, Dedi Supriadi, stated that efforts to provide countermeasures in providing criminal policies are carried out with the criminalization aspect of criminal law, namely by forming special laws to regulate things that are prohibited in this case. Legal action is a solution provided by law to victims whose rights to justice are not fulfilled, and to provide relief and peace of mind for the criminal acts that befell them. Online Fraud Actions involve the following steps, such as Legal Efforts through

Litigation, and Legal Efforts through Non-Litigation

According to the Director of Special Criminal Investigation of the South Sulawesi Regional Police, Dedi Supriadi stated that:

"One of them as a guideline for evidence is the provisions in Article 184 of the Criminal Procedure Code, where the evidence referred to is witness testimony, expert testimony, letters, instructions, and defendant's testimony. In addition, investigators can use cybercrime investigators using evidence, namely Electronic Information and/or Electronic Documents and/or their printouts. However, electronic information and/or electronic documents are declared valid if they use an electronic system in accordance with the provisions stipulated in the ITE Law.

There are several ways to report online fraud that you can do: [16]

Contact the relevant bank

The first way to report online fraud is to contact the relevant bank. If it has already happened, it is better for the victim to immediately contact the relevant bank to prevent the fraudster from making transactions or accessing more of the victim's account data. This first way to report online fraud is expected to immediately block access to your account so that the funds stored in it remain safe.

Report fraud to the Financial Services Authority (OJK)

In addition to the relevant bank, the next way to report online fraud is to contact the OJK. This is because the OJK has a special institution for complaints and reports related to this case called the Investment Alert Task Force (SWI). In addition to receiving complaints from victims, they can block and take further action against the perpetrators of this online fraud.

Report fraud via Lapor.go.id

The next way to report online fraud is to contact lapor.go.id. LAPOR is the People's Online Aspiration and Complaint Service. This service is a centralized public service complaint management system in one container. Of course, this container can follow up on the perpetrators of this fraud.

Making a report to the Indonesian Telecommunications Regulatory Body (BRTI)

The next way to report online fraud is to contact BRTI. This institution is a forum owned by the Ministry of Communication and Information Technology to be a place for the public to report misuse of telecommunications services, either calls or messages that are indicated as fraud.

Make a complaint to the police station

The most concrete way to report online fraud is to report it to the nearest police station. The goal is that this case can then be processed and acted upon by the authorities. Make sure you include detailed evidence and information so that the legal process will run and become the most deterrent way to report online fraud for the perpetrators.

Legal protection refers to legal efforts. In which there is protection regarding the rights of individuals to be able to prevent any losses that may be caused to them. There is another definition that explains "Legal protection is an action to provide rights to freedom and respect for the individual himself, as well as protection of the dignity and honor of the individual.

The amendment of the 2008 ITE Law to the 2016 ITE Law provides a new regulation for issues regarding social media that are popular in society. This aims to provide guidelines for cybercrime,

[17] but there are still some loopholes even though there are problems with the amendment of the 2008 ITE Law. ITE 2016 has not completely changed the violations in the ITE Law, such as not updating the provisions on electronic transactions. This can be seen when the law does not have a specific understanding of the form of sales carried out electronically, but only "electronic transactions" which have a very broad meaning, namely actions in which the perpetrator uses electronic means, computer networks and other electronic means.

In addition, the trend of reform regarding the Criminal Code which in this case cannot target the perpetrator is not clearly visible in the 2016 ITE Law, because when a crime occurs and results in some losses for the victim, the 2016 ITE Law is also not clearly displayed, there are no regulations regarding definite fines when cybercrime occurs, such as in the crime of fraud that based on the 2016 ITE Law is regulated in Article 28, namely: "individuals who in this case are found to be spreading false information without rights or misleading information causing losses for consumers in electronic transactions according to the provisions stipulated in Article 45A paragraph (1) the perpetrator can be sentenced to imprisonment for 6 years and a fine of Rp. 1,000,000,000.00, also regulated in Article 28 paragraph (1), including the following elements, among others: [18]

Acts that are done consciously/intentionally

This action can be said to be contrary to the law

Spread of false information

Context of fake news

The occurrence of losses for other parties.

Regarding fraud where the perpetrator uses electronic media to carry out his actions, the 2016 ITE Law in this case regulates criminal provisions in the form of imprisonment or fines, but does not provide regulations regarding compensation for victims of fraudulent crimes. In fact, every year, cases of fraud in online trading transactions are increasing. With the provisions of fraud in the 2016 ITE Law, victims are increasingly suffering losses because there is no compensation for their losses. In addition, in online sales agreements, victims are the ones who bear the most losses because in the process consumers first pay a certain amount of money before the goods are sent, this certainly provides a great opportunity for perpetrators to carry out their fraudulent actions, the need for consumer protection is very much needed, this is considering the very weak position of consumers in online transactions.

The procedure for transactions carried out online often causes many losses for the victims. The forms of these losses include damaged products, negligence and the community experiencing losses in the form of lost goods or non-delivery of goods even though the victim in this case has paid the amount of money promised or agreed upon. The law as a guarantor in providing protection for consumers by using its power, namely by requiring business actors to fulfill their obligations after receiving the rights they should receive. In practice, there is a concept that states that consumers must bear all risks arising from the choices they make, namely the purchase of products in the form of goods and/or services provided by business entities. This weakens the position of consumers in terms of legal protection. [2]

According to Baoak, legal protection for victims of online fraud involves both procedural and substantive aspects. Here is an explanation of the two aspects:

Substantive Protection

Substantive legal protection begins with the definition of the crime of fraud through social media in criminal law or other laws. This definition includes the essential elements of fraud through social

media that can form a legal basis for prosecuting the perpetrator, including:

Sanctions and penalties that can be imposed on perpetrators of online fraud. This includes the types of penalties that can be imposed, such as fines or prison sentences, which are specified in law.

The right to compensation gives victims the right to receive compensation from perpetrators of fraud via social media. This right gives victims the right to receive compensation for the material losses they experience as a result of fraud.

Consumer protection Substantial consumer protection laws can provide a legal basis for involving business actors in fraudulent practices through social media and provide special rights to consumers.

Procedural Protection

This legal system and law enforcement process in procedural protection involves a legal system and law enforcement process that ensures that handling of online fraud cases is carried out fairly and effectively, including investigation, prosecution and trial procedures.

Victims' rights in the legal process Victims of online fraud have certain rights in the legal process, such as the right to give testimony, the right to be represented by a lawyer, and the right to receive information about the progress of their case.

Information security and privacy in procedural protection involves the security of information and the privacy of victims. Handling of personal information and victim data must be done carefully to prevent further misuse.

Access to the legal system can ensure that victims have equal access to the legal system, including access to legal aid services and easily accessible reporting mechanisms.

CONCLUSION

Legal Consequences for Perpetrators of Online Fraud Crimes Through Electronic Social Media The application of legal sanctions for perpetrators of online investment fraud has not been expressly regulated in a special law that can provide aggravating criminal penalties for perpetrators but is regulated in the Criminal Code Article 372 with a maximum imprisonment of four years or a maximum fine of nine hundred rupiah, and Article 378 with a maximum imprisonment of 4 (four) years. Efforts to provide countermeasures in providing criminal policies are carried out with the criminalization aspect of criminal law, namely by forming special laws to regulate things that are prohibited in this case. Legal action is a solution provided by law to victims whose rights to justice are not fulfilled, and provides relief and peace of mind for the criminal acts that befell them. Online Fraud Actions involve the following steps, such as Legal Efforts Through Litigation, and Legal Efforts Through Non-Litigation. The urgency of making regulations or legal arrangements for investment or commonly called online capital investment specifically so that it can provide criminal penalties and strengthen criminal sanctions for online fraud perpetrators for the purpose of the law, namely legal certainty, justice and benefits. The state should, in protecting online practices, make regulations that specifically and firmly regulate aspects of investment practices or online capital investment in order to achieve legal certainty.

References

1. Z. O. Dheny Rusdiyanto, Dwi Raka Siwi, Galuh Fitriana, Astria Fitri, “Penipuan Menggunakan Media Internet berupa Jual Beli Online,” Iqtishaduna J. Ilm. Mhs. Jur. Huk.

Ekon. Syariah, vol. 5, pp. 277–285, 2024.
2. K. T. Situmorang, “Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Transaksi Jual Beli Media Online,” pp. 1–23, 2019.
3. M. A. Facebook, “Analis Yuridis Penipuan Online Melalui Aplikasi Facebook,” 2023.
4. Zubairi, “Pola Kepribadian Manusia Perspektif Al-Qur"an,” JIQTA J. Ilmu Al- Qur’an dan Tafsir, vol. 2, no. 1, pp. 29–44, 2023.
5. F. S. R. Nurul Qamar, Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal, vol. 11, no. 1. 2020. [Online]. Available: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI
6. T. Y. Rahmanto, “Penegakan Hukum Terhadap Tindakan Pidana Penipuan Nernasis Tranksasi Elektronik,” Jure, vol. 19, no. 30, pp. 31–52, 2019.
7. I. P. K. Adhi, “Rekaman Elektronik Personal Chat Pada Sosial Medial Sebagai Alat Bukti,” Univ. Airlangga, vol. 1, no. 3, 2018, doi: 10.20473/mi.v1i3.9829.
8. N. P. R. Y. Made Sugi Hartono, “Penggunaan Bukti Elektronik Dalam Peradilan Pidana,” Fak. Huk. Dan Ilmu Sos. Univ. Pendidik. Ganesha, vol. 6, no. 1, pp. 281–302, 2020.
9. J. Wahyudin, R. Renggong, and A. H. Hamid, “DAERAH SULAWESI SELATAN Analysis of Online Criminal Fraud in the South Sulawesi Regional Police,” Indones. J. Leg. Law e-ISSN, vol. 6, no. 2, pp. 273–280, 2024, doi: 10.35965/ijlf.v6i2.4474.
10. S. Agustina, “Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana,” Fak. Huk. Univ. Andalas Kampus Limau Manis Padang, pp. 503–510, 2008.
11. B. Janet and T. Murwadji, “Praktik Skema Piramida dalam Sistem Distribusi Barang,” vol. 14, pp. 135–152, 2020.
12. J. R. Gansalangi, “Penegakan Hukum Pidana Dalam Kasus Tindak Pidna Penipuan Melalui Arisan Online,” Court Rev. J. Penelit. Huk., vol. 5, no. 01, pp. 75–85, 2025.
13. D. Asimah, “Menjawab Kendala Pembuktian Dalam Penerapan Alat Bukti Elektronik,” Puslitbang Huk. Dan Peradil., vol. 3, pp. 97–110, 2020.
14. H. Sumadi, F. Hukum, and U. Subang, “Kendala dalam menanggulangi tindak pidana penipuan transaksi elektronik di indonesia,” J. Wawan Huk., vol. 33, no. 2, 2015.
15. A. Ilyas, Asas-asas hukum pidana. Rangkang Education Yogyakarta & PuKAP-Indonesia, 2012.
16. J. Aaron, R. Simanungkalit, R. Hertadi, and U. Pakuan, “Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya,” Akad. J. Mhs. Humanis, vol. 4, no. 2, pp. 281–294, 2024.
17. A. Suharto, “Upaya Perlindungan Terhadap Tindak Pidana Online Perspektif Undang-Undang,” IBLAM Law Rev., no. September, 2024.
18. S. Kakoe, M. R. I, and A. Madjid, “Perlindungan Hukum Korban Penipuan transaksi Jual Beli Melalui Ganti Rugi Sebagai Pidana Tambahan,” J. Leg., vol. 13, pp. 118–131.