Law Enforcement Against Fraudulent Acts Committed in Cyberspace

Dianto Gunawan Tamba[1], Indah Sya Vitri[2]. Felix Adrian Sembiring[3], Yolanda Anatasya Sembiring[4]
[1.2 3] Faculty of Law, Department of Law, Universitas Prima Indonesia.
Email: indahsyavitri93@gmail.com

These developments have created new business opportunities that enable individuals to conduct legal transactions involving online sales/e-commerce. However, these developments also have negative aspects/problems that are detrimental to consumers, namely criminal acts of fraud committed by irresponsible parties, particularly sellers, as well as inadequate law enforcement, including problems with evidence. This needs to be discussed because of the problem of evidence, namely electronic data that is easy to falsify, the lack of readiness of law enforcement, and in order to reduce online fraud. The author's suggestion is that there should be stricter law enforcement and evidence from law enforcement officials, and the community should also play a role in reducing the use of the internet that is harmful to society. Cultural factors within a community are also important.
Keywords: Law Enforcement; Cyberspace; Technology

Corresponding Author:
Yolanda Anatasya Sembiring
Faculty of Law, Department of Law, Universitas Prima Indonesia.
E-mail: anastasyayolanda125@gmail.com

1. Introduction

The need for computer network technology is increasing and developing worldwide. Besides providing information, the internet is also a major and rapidly growing part of the commercial community, spanning national borders. Through this network, global market activity can be monitored 24/7.[1]Through the internet, also known as cyberspace, anything can be done. The positive aspects of this virtual world certainly add to the trend of global technological development, fueling all forms of human creativity. However, negative impacts are also unavoidable. When pornography is rampant on the internet, society is left with little to do. Along with the development of internet technology, it has given rise to crimes known as cybercrime, or crimes committed through internet networks. Several cybercrime cases have emerged in Indonesia, such as credit card theft, website hacking, intercepting other people's data transmissions, such as email, and manipulating data by setting unwanted commands into computer programmers. Therefore, computer crimes can involve both formal and material crimes.This is very detrimental to society in its actions. The need for computer network technology is increasing.

And information technology has succeeded in building a new habit in a global society that influences changes in the pattern of people's living needs in the social and economic fields, which usually transact, do business or socialize by meeting physically or conventionally to transact, do business or socialize electronically, namely meeting each other in the virtual world, because it is believed that this can make transactions easier, save more time, costs and is not limited by space and time.

And it is not impossible that in the development of the internet there is a positive side that can help the community, students and school children and all officials and all, along with the development of the internet today. And with the positive aspects of technological development, of course, adding to the trend of global technological development with all forms of human creativity. Fraud through online media is growing in Indonesia for several reasons, namely internal and educational factors in the context of a society that does not understand the law and is lazy in following news or information, and is not familiar with technology so that factors of hedonistic or consumerist environmental conditions are easy to access technology and influence.

The Internet is one of the operated funds of computers or communication tools that cause one of the social changes, and will be very in society, one of which is a change in behavior in social relations, and has an impact on the emergence of new norms, but development. And its use in the hands of people who like to commit crimes and are irresponsible which can cause negative and very influential on many people. In efforts and overcoming crime with criminal law from criminal politics, it must also be an integral part of social politics, namely the policy of achieving social welfare and community protection.

Formulation of the problem

How effective is law enforcement against fraud crimes committed in cyberspace based on Law No. 1 of 2024 concerning the Second Amendment to the ITE Law and the Criminal Code?

What are the inhibiting factors faced by law enforcement (particularly the police) in identifying, investigating, and apprehending perpetrators of online fraud, especially those involving cross-border jurisdictions or anonymous identities? What are the legal protections for victims of online fraud and the mechanisms for reimbursing financial losses, given that funds cannot always be recovered?

Research purposes

The purpose of this study is to determine and analyze how law enforcement against cyber fraud occurs, the obstacles faced by law enforcement officials, and the efforts that can be made to improve legal protection for the public. This study aims to provide a comprehensive understanding of law enforcement against cyber fraud, both from a normative perspective and in practice in Indonesia. The objectives of this study are as follows, To examine in depth the characteristics of fraud crimes in cyberspace, including the modus operandi used by perpetrators, such as fraud through social media, marketplaces, email, digital banking, and instant messaging applications, as well as the differences with conventional fraud crimes. To analyze the legal regulations governing fraud crimes in cyberspace, especially the provisions in the Criminal Code (KUHP), Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments, as well as other relevant laws and regulations. To examine the application of elements of fraud crimes in law enforcement practices, including proving the elements of intent, unlawful acts, victim losses, and the use of electronic evidence in the process of investigation, prosecution, and examination in court. To analyze the role and authority of law enforcement officials, especially the police, prosecutors, and courts, in handling fraud cases in cyberspace, as well as the extent of effectiveness of coordination between these institutions. To identify obstacles and challenges in law enforcement, both juridical obstacles,technical and non-technical factors, such as limited human resources, rapid technological advances, cross-regional and international (borderless crime), and low public legal awareness. To examine legal protection for victims of cyber fraud, including victims' rights to recovery of losses, restitution, and available complaint mechanisms.

Benefits of research

Theoretical Benefits

Theoretically, this research is expected to contribute to the development of legal science, particularly criminal law and cyber law, by enriching studies on law enforcement against cyber fraud. The results of this study can serve as academic reference material for researchers, students, and academics in understanding the characteristics, regulations, and legal application of information technology-based fraud crimes.

Practical Benefits

For Law Enforcement Officers

This research is expected to provide input for law enforcement officials, such as the police, prosecutors, and judges, in increasing the effectiveness of handling and enforcing the law against fraud crimes in cyberspace, especially in the aspect of proof and application of electronic evidence.

For Policy Makers (Government and Legislators)

The results of this study are expected to be used as consideration in formulating or improving policies and laws and regulations related to cyber fraud crimes to be more responsive to developments in information technology.

For the Community

This research is expected to increase public awareness and legal understanding regarding forms of fraud in cyberspace and preventive measures, so that people can be more careful in carrying out digital activities.

For Victims of Cyber Fraud

This research is expected to provide information regarding legal protection and legal remedies that can be taken by victims to obtain justice and recovery for the losses they have experienced.

2. Method

This research is a normative legal study, which is conducted by reviewing library materials or secondary data related to law enforcement against cyber fraud. This research focuses on the study of legal norms, legal principles, and regulations governing fraud and their application. Using an empirical approach, this research can be supplemented with empirical legal research, which is research that examines the application of the law in practice through field data, such as interviews with law enforcement officials or related parties.

The approaches used in this research are the statutory approach, the conceptual approach, and the case approach. The statutory approach is used to examine and review the laws and regulations related to the crime of fraud in cyberspace, particularly the provisions in the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016. The conceptual approach is used to understand the concepts, principles, and legal doctrines related to the crime of fraud, cybercrime, and the enforcement of criminal law based on the opinions of legal experts. Meanwhile, the case approach is used to examine court decisions related to the crime of fraud in cyberspace to determine the application of the law by judges in judicial practice.

The legal sources used in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations related to fraud and cybercrime, as well as legally binding court decisions. Secondary legal materials include legal textbooks, scientific journals, legal articles, and previous research relevant to the research topic. Tertiary legal materials include legal dictionaries, the Great Indonesian Dictionary, and legal encyclopedias, which are used to clarify legal terms and concepts.

Legal material was collected through a literature study, which involved collecting, reading, and reviewing laws and regulations, legal literature, and documents related to the research problem. The collected legal material was then analyzed qualitatively by outlining and interpreting relevant legal provisions and then linking them to the research problem.

The legal material analysis technique is carried out using the deductive method, namely drawing conclusions from general legal provisions to specific conclusions in order to answer problems regarding law enforcement against criminal acts of fraud committed in cyberspace.

3. Results and Discussion

Characteristics and Development of Fraud Crimes in Cyberspace

Advances in information and communication technology have transformed fraud patterns from conventional to digital. Cyberfraud has unique characteristics, including being conducted over the internet, utilizing electronic devices, and utilizing electronic systems as the primary means. These characteristics mean that cyberfraud has a wide reach, can be carried out quickly, and has the potential to cause a large number of victims.

Online fraud modus operandi continues to evolve with the increasing use of social media, marketplaces, and digital financial services. Perpetrators often use fake identities, anonymous accounts, and social engineering to gain victims' trust. Furthermore, perpetrators exploit weaknesses in digital security systems and low levels of digital literacy to carry out their actions. This situation demonstrates that online fraud is not only a legal issue, but also a social and technological one.

Elements of the Crime of Fraud from a Criminal Law Perspective

In Indonesian criminal law, fraud is primarily regulated by Article 378 of the Criminal Code, which includes elements of intent to unlawfully benefit oneself or another person, the use of deception or a series of lies, and causing harm to another party. These elements also apply to fraud committed online, although the means used differ from those used in conventional fraud.

In the context of online fraud, the element of deception can include the dissemination of false information through electronic media, manipulation of website appearance, or disguise of the perpetrator's identity. Meanwhile, the element of loss is not limited to material losses but can also include immaterial losses, such as misuse of the victim's personal data. Therefore, the application of Article 378 of the Criminal Code to fraud inThe virtual world is still relevant, although it requires adaptive interpretation to technological developments.

Regulation of Fraud in Cyberspace in the ITE Law

Apart from the Criminal Code, fraud in cyberspace is also regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016. Article 28 paragraph (1) of the ITE Law expressly prohibits any person from intentionally and without the right to spread false and misleading news that results in consumer losses in electronic transactions.

These provisions demonstrate the recognition of fraud as a form of cybercrime. However, the provisions in the ITE Law are still limited, as they focus more on consumer protection in electronic transactions, so not all forms of online fraud can be effectively addressed. Therefore, in law enforcement practice, a combination of the Criminal Code and the ITE Law is often used to prosecute perpetrators.

Law Enforcement Process against Cyber Fraud

Law enforcement against cyber fraud crimes is carried out through stages of inquiry, investigation, prosecution, and trial. The police, particularly the cybercrime unit, play a central role in uncovering and

handling online fraud cases. During the investigation phase, law enforcement officers must collect and analyze electronic evidence, such as digital transaction records, online conversations, and system log data.Electronic evidence is recognized as valid evidence in the Indonesian legal system. However, the process of collecting and testing it requires specialized technical expertise to maintain the authenticity and integrity of the data. Without adequate digital forensic technology, proving cyber fraud will be difficult in court.

Obstacles to Law Enforcement in Practice

Despite a clear legal basis, law enforcement against cyber fraud still faces various obstacles. One major obstacle is the difficulty in identifying and tracking perpetrators, who often use fake identities, virtual private networks (VPNs), and servers located overseas. This situation often leads to transnational cyber fraud crimes, necessitating international cooperation.

Furthermore, limited human resources and supporting infrastructure in the information technology sector are also inhibiting factors. Not all law enforcement officers have adequate skills and training to handle cybercrime. Furthermore, low public legal awareness leads many victims to be reluctant to report or delay reporting fraud, complicating the law enforcement process.

Preventive and Repressive Efforts in Combating Fraud in Cyberspace

Combating cyber fraud cannot rely solely on repressive measures through criminal law enforcement. Preventive measures also play a crucial role, including increasing public digital literacy, strengthening electronic transaction security systems, and monitoring digital platforms. Educating the public about online fraud methods can reduce the potential for these crimes to occur.

On the other hand, repressive measures are still necessary to provide a deterrent effect to perpetrators. Firm and consistent law enforcement against cyber fraudsters is expected to create a sense of justice and legal certainty. With a balanced combination of preventive and repressive measures, combating cyber fraud can be more effective and sustainable.

4. Conclusion

Based on the discussion regarding law enforcement against cyber fraud, it can be concluded that the development of information technology has brought significant legal consequences, particularly in the increasing modes and scale of electronic-based fraud. Cyber fraud not only causes economic losses for victims but also has an impact on declining public trust in electronic transaction systems and the development of the digital economy in general. Normatively, the legal system in Indonesia has provided a sufficient legal basis for prosecuting perpetrators of cyber fraud, both through the provisions of Article 378 of the Criminal Code (KUHP) and the provisions of the Electronic Information and Transactions Law (UU ITE). The existence of these regulations demonstrates the state's commitment to providing legal protection to the public from cybercrime. However, these legal regulations are still general and have not fully accommodated the complexity of fraud crimes that continue to grow along with advances in digital technology. In law enforcement practice, law enforcement officials face various obstacles, particularly in the aspect of proving electronic-based crimes. Digital evidence that is easily deleted, manipulated, or disguised presents a particular challenge in the investigation process and evidence in court. Furthermore, the use of fake identities, anonymous accounts, and servers located outside Indonesian jurisdiction makes tracking and prosecuting perpetrators increasingly difficult. Human resources are also a significant obstacle in law enforcement against cyber fraud. Limited technical capabilities and knowledge of information technology among law enforcement officials can impact the effectiveness of handling cybercrime cases. Furthermore, low levels of digital literacy and public legal awareness contribute to the

high rate of online fraud, as many victims lack an understanding of the risks of electronic transactions and do not promptly report fraud. Furthermore, the transnational, and even inter-national, nature of cyber fraud requires closer cooperation between national law enforcement officials and international institutions. Without effective coordination and cooperation, law enforcement efforts against cybercrime will struggle to achieve optimal results. Therefore, law enforcement against cyber fraud cannot rely solely on a repressive approach through criminal prosecution but must also be balanced with preventive and educational efforts. Strengthening regulations, increasing the capacity of law enforcement officials, and developing law enforcement technology infrastructure,and improving the public's digital literacy are strategic steps that need to be implemented sustainably. Through this comprehensive approach, it is hoped that law enforcement against cyber fraud will be more effective and provide a sense of justice, legal certainty, and optimal legal protection for the public..

5. Reference

Ali, Mahrus. Fundamentals of Criminal Law. Jakarta: Sinar Grafika, 2015.

Arief, Barda Nawawi. Criminal Law Policy: Developments in the Drafting of the New Criminal Code. Jakarta: Kencana, 2018.

Atmasasmita, Romli. Contemporary Criminal Justice System. Jakarta: Kencana, 2017.

Hamzah, Andi. Indonesian Criminal Law. Jakarta: Sinar Grafika, 2017.

Makarim, Edmon. Introduction to Telematics Law: A Compilation of Studies. Jakarta: RajaGrafindo Persada, 2014.

Maskun. Cyber Crime: An Introduction. Jakarta: Kencana, 2013.

Soesilo, R. The Criminal Code (KUHP) and its Complete Article-by-Article Commentaries. Bogor: Politeia, 2016.

Wahid, Abdul, and Mohammad Labib. Cyber Crime. Bandung: Refika Aditama, 2010.