Jurnal
ILMU KEPOLISIAN
ISSN : 2620-5025
E-ISSN : 2621-8410

Vol. 18, No. 2, 2024

Cyber Fraud with Profile Cloning Mode in The Perspectives of Cyberculture and Space Transition Theory

Submitted 22 January 2024, Revised 22 July 2024, Accepted 22 July 2024, Published 14 August 2024

Wily Yulistiyo[1]*, Firman Fadillah[2], Andi Gibran[3]

[1]West Java Regional Police, Bandung, Indonesia
[2]School of Strategic and Global Studies, Universitas Indonesia, Jakarta Pusat, Indonesia
[3]Metropolitan College, Boston University, Boston, USA
Corresponding email: *yulistiyowily@gmail.com

DOI: https://doi.org/10.35879/jik.v18i2.437

Abstract

This study aims to investigate whether there are still any society who do not understand cyber culture on social media which then has the potential to become victims of cyber fraud crimes. In the digitalization era 4.0, people tend to use technology to do various activities and meet their needs, including online transactions for goods and services using various digital platforms and social media. The high activity on the Internet is also accompanied by opportunities for crimes by utilizing the internet media. One of the cases that is increasingly occurring in the digitalization era is cyber fraud with profile cloning mode. The author is interested in studying cyber fraud in Wajo Police because the mode used was profile cloning, which used the profile of a law enforcer to make fictitious buying and selling. This study used a qualitative approach and a case study method to conduct an in-depth analysis of cyber fraud cases with profile cloning mode. The results of the study show that there are still people who do not understand cyberculture on social media, so they have the potential to be victims of cyber fraud crimes. Moreover, the results of the study also show that perpetrators commit cyber fraud with profile cloning mode due to the pressure in real life and the ease of cloning accounts on social media. Thus, such circumstances provoke perpetrators to shift their evil deeds to cyberspace.

Keywords: Cyber Crime, Cyber Fraud, Profile Cloning

INTRODUCTION

Cyber technology-based crimes are increasing along with the development of technology in the digitalization era 4.0 in Indonesia. The use of communication and information technology is increasingly becoming a trend in society in line with the increasing development of human life and is able to issue ideas that can help many people (Syarief et al., 2016). Among the ideas that emerged from the development of communication and information technology is the transaction of goods and services using Internet media to make the transaction process easier and more efficient (Setiawan, 2018). With this convenience and efficiency, online buying and selling are currently widely used, especially by urban communities and the young generation. The tendency of Indonesians to make online goods and services transactions with the persuasion of lower prices has caused many victims

of fraud (Sari et al., 2022). Moreover, various modes have begun to develop, such as inviting collaboration on behalf of a well-known company, online store sales with lower prices, offering assurance or investment, fictitious promotion, winning the lottery, and so on. These modes will continue to develop because the perpetrators will continue to find ways various to deceive victims.

The rapid development of digital media in Indonesia has created challenges in the form of increasing rates of legal violations (Siboro & Hadiningrum, 2024). Like a double-edged sword, besides providing positive contributions, technology development also has a bad or negative impact. The appropriate use of information technology will provide advancement for society's quality of life and the advancement of human civilization (Munti & Syaifuddin, 2020). On the other hand, information technology also provides opportunities for more complex crimes using internet networks (Hamid, 2023). The level of cybercrime in Indonesia is second place in the world. In a work meeting with the Ministry of Communication and Information of the Republic of Indonesia, Rudiantara Akhmad stated that Indonesia is in second place in cybercrime after Ukraine. Cyber crimes increased significantly in 2022 compared to the same period in 2021. The number of cyber crimes has increased 14 times, with 612 cases in 2021 and 8,831 cases in 2022. Data from e-MP Robinopsnal (Electronic Investigation Management of the Bureau of Development and Operation) of the Criminal Investigation Agency show that police have taken action against 8,831 cyber crime cases from January 1 to December 22, 2022. All work units at the Criminal Investigation Agency and regional police in Indonesia have taken massive action against cybercrime cases. Polda Metro Jaya (Greater Jakarta Metropolitan Regional Police) is the work unit with the highest number of prosecutions for cybercrime cases, which is 3,709 cases. Meanwhile, in the same period in 2021, the number of prosecutions was 612 cases around Indonesia; only 26 work units took prosecutions (Pusiknas Polri, 2022).

The high number of cyber crimes in Indonesia is also influenced by the limited knowledge about the use of information technology in society. A study by Supardi Hamid and Rodon Pedrason (2023) concluded that knowledge about communication and information technology is important in society, so it can provide positive things and avoid criminal deviations through social media. Looking at the high number of cyber crimes in Indonesia shows that the level of knowledge about communication and information technology in Indonesian society still must be improved so the community can avoid becoming victims of cyber fraud or even committing crimes using cyber media (Handoko, 2021).

W. Steve Albrecht and Chad D Albert explained that cyber fraud is a crime committed within an internet network-based system to deceive or manipulate information to gain as much profit as possible (Karyono, 2013: 3). From the concept of cyber fraud explained, there are several elements for an act to be categorized as cyber fraud, where the act must use internet network, commit deception, and aim to gain a profit (Prabhaswara, 2023). Cyber frauds that occur along with the

development of information and communication technology tend to continue transforming from time to time from cyber frauds with simple modes to using complex and complicated modes. All of these actions are committed only to avoid suspicion from potential victims of cyber fraud. One of the various modes of cyber fraud that commonly occur currently is cyber fraud mode by profile cloning.

Profile cloning is one of the modes of cyber fraud, where the perpetrators attempt to steal or fake their identity on the Internet or social media to commit fraud or other crimes (Esfandari, 2019). The perpetrators usually will use names, photos, or other identities from someone cloned on an internet or social media account to make it look like the real one. After successfully having a fake social media account, perpetrators commit fraud or other crimes on behalf of someone whose identity was previously cloned. Generally, the identities cloned are social media accounts of public figures, law enforcement officers, online sellers, and banking institution accounts. These profiles are often cloned because they are more convincing to potential victims when committing cyber fraud (Bernoza et al., 2020).

In social media that developed in Indonesia, public figures, such as political figures or artists, tend to have many followers or account visitors. In recent years, even ordinary people who have the ability to create content (content creators) on social media have also become the center of attention on social media. People who are not public figures but have appearances that attract public attention usually become the center of attention on social media with a large number of followers. The existence of accounts with many followers, both public and non-public figures, attracts the attention of goods and services owners to promote their goods and services to the public through these accounts. These account owners will be endorsed with certain agreements or contracts to increase sales, especially to followers of certain accounts, according to their market characteristics. This way of advertising goods and services is considered more effective than advertising them on other electronic media, such as television and radio, because nowadays, almost everyone looks at their gadget all the time. Meanwhile, watching television or listening to the radio might only be done at certain times, and the audience is not as large as on social media.

The phenomenon of accounts with large followers is one factor that leads to cyber fraud with profile cloning mode (Bhariatta et al., 2019). From the perspective of cyber fraud perpetrators, if they clone a social media account of a public figure, the possibility of gaining profits will be greater, mainly if potential victims are not careful in differentiating which accounts are real and which accounts are fake. There are many cases where fake accounts clone public figure accounts. Then, they successfully cheat by selling fictitious goods or fictitious lotteries. In several cases, the perpetrators of cyber fraud are able to manipulate fake messages to deceive potential victims (Sabilah, 2023). For example, when perpetrators pretend to buy an item, they send fake transfer receipts as they have paid by transfer. The sellers who receive the transfer receipt then send the item to the perpetrators. Usually, the new victims will realize that the transfer made is fictitious when they

will recap sales at the end of the month or the end of the week. When victims realize there is a difference, they will check transaction data one by one. Then, the victims realized that the transfer receipt sent was fake.

From the explanation above, it can be seen that the nature of criminals is to continue to try to commit crimes in cyberspace, both through cyber fraud and hacking. When one mode is successfully revealed, the criminals will innovate to find other modes, even the most complicated and complex mode, to gain profits (Mudjiyanto & Roring, 2024). In the future, old modes that have been forgotten by the public will possibly be used again by cyber fraud perpetrators. Not only cloning accounts, criminals can even hack or log in to a real account illegally, only by sending an application file wrapped like a wedding invitation or other invitations (Sahabuddin & Andrizki, 2024). Therefore, people in the digital era must increase their awareness so as not to avoid becoming victims of social media crimes.

Previous research has explored several facets of cyber fraud, such as the technological techniques employed by criminals, the psychological and social consequences for victims, and the wider implications for digital security policy. Unfortunately, we have not come across a thorough investigation about the particular occurrence of a case where clonings profiles is used in order to commit fraudulent activities. Therefore, we will address this gap by conducting a comprehensive analysis of this unique modus operandi used in cyber fraud cases. We aim to thoroughly examine the strategies employed by cyber fraudsters in profile cloning schemes, utilizing relevant theories and concepts from the fields of criminology, cybersecurity, and social psychology.

The case analyzed in this study is cyber fraud committed by Mr. Abdullah, a resident of Wajo Regency, South Sulawesi, who cloned the Facebook account of a policewoman named "Kiki Widya S." Through the cloned account, the perpetrator succeeded in deceiving victims by selling motorbike auctioned from crime cases at low prices. This case is one of the cyber fraud cases that use profile cloning of law enforcement officers' social media accounts in Indonesia so that in-depth analysis can be carried out. Based on the background, this study aims to analyze how cyber fraud crimes can occur, mainly using profile cloning mode. By using relevant theories and concepts, this study is expected to analyze how cyber fraud perpetrators commit their crimes and how the internet or social media users can be victims of cyber fraud using the profile cloning mode.

METHOD

In this study, the author employes the qualitative approach. According to Bogdan and Taylor, qualitative is associated with research procedures that result in descriptive data in the form of written or spoken words from people or observed behavior (Moleong, 2020). A qualitative study is used because there is a problem that must be explored. In this study, cyber fraud cases using profile cloning mode must be explored in depth and analyzed using relevant theories and concepts. The research

method used was the case study method, where the focus of the case study method is on the specification of the case in an incident, either involving individuals, groups, or a portrait of life (Creswell, 1998).

The case study method was used in this study because, when analyzing a case, the author can focus on an in-depth study and analyze a cyber fraud case with profile cloning mode in Wajo regency, South Sulawesi. The case study allowed the author to investigate cyber fraud so that the author could investigate problems more focused with clear scope boundaries. Therefore, the author obtained a comprehensive description of a cyber fraud case with profile cloning mode to be further studied using cyberculture and space transition theory.

RESULTS AND DISCUSSION

Results

Cyber Fraud Case in Wajo

A case that became the object of the study was a cyber fraud case with profile cloning mode in the jurisdiction of the Wajo Police, South Sulawesi. On March 18, 2021, the Criminal Investigation Unit of Wajo Police, through the Specific Crimes Unit (Tipidter), raided a house in Kec. Maniangpajo, Wajo Regency. The raid began with information from the public reporting a house suspected of being a place where cyber fraud perpetrators (in the Bugis community known as Pasobis) committed crimes. People were suspicious because many people often gathered and committed close activities in the house for a long time. In the raid, a man named Mr. Abdullah (22 years old, resident of Lakadaung, Kecamatan Maniangpajo, Wajo Regency, South Sulawesi), who was committing cyber fraud activity using several laptops and mobile devices, was arrested. After carrying out an investigation, facts were obtained that the person was a cyber fraud perpetrator with profile cloning mode who claimed to be a law enforcement officer to make fictitious buying and selling transactions.

After this arrest, a cyber fraud case in 2020 was finally revealed. The chronology of the cyber fraud case began in December 2020, when a victim, Mr. Olfan Mundok (36 years old, resident of Malinow, Kotamobagu, North Sulawesi), was using the social media application Facebook. Then, he saw a post from a Facebook account named "Kiki Widya S," based on the profile, was a policewoman at National Police Headquarters, Jakarta. This policewoman account sold several used motor vehicles, mainly motorbikes, at a very low price and under the market price. The post mentioned that the vehicles sold were the auction of the proceeds of crime, so the price was really low. The victim was increasingly convinced due to many comments reviewing that they had a transaction with the perpetrator and the vehicle purchased was in good condition. However, the comments were fictitious and were made by the perpetrator using different accounts. The victim is finally interested and bought 1 (one) unit of motorbike. After negotiation via chatting in Facebook Messenger and WhatsApp, it

was agreed that the victim would buy 1 (one) unit of Yamaha N-Max for 8 (eight) million rupiahs. The victim then paid a down payment via transfer to the account provided by the perpetrator. The perpetrator also asked the victim to pay a vehicle transfer fee and shipping cost of 6 (six) million rupiahs. After the down payment, vehicle transfer fee, and shipping cost were transferred by the victim, the perpetrator could not be contacted, both via WhatsApp and Facebook account. The item purchased was 1 (one) unit of motorbike that never arrived at the victim's address in Kotamobagu, North Sulawesi.

From the description above, it can be seen how cyber fraud case with profile cloning mode, where the perpetrator created a fake account in a Facebook application using the profile of a policewoman named "Kiki Widya S." It can be known that the policewoman does have social media account and has a relatively large number of followers, thus making her one of the policewomen whose profile is often faked by cyber fraud perpetrators. The profile of a policewoman also provoked the perpetrator to clone the profile to commit cyber fraud that sold the auctioned motor vehicles from crimes handled by the police.

Space Transition Theory

This theory is developed by Karuppannan Jaishankar (2008) to observe crimes in cyberspace. Space Transition Theory attempts to explain how someone commits cyber crimes. Moreover, this theory also explains natural human behavior, taking conformity and non-conformity behavior in real life and cyberspace. Transition, in this theory, means the shift of a person from one world to another. In other words, this theory sees that an individual can have different behavior when they move to another space, for example, from physical space to cyberspace or vice versa. An individual who behaves well in a social environment (physical space) will not always behave well in cyberspace. Several factors can influence an individual to do the opposite in cyberspace.

This theory has become a reference for various studies that examine crimes in cyberspace. Cyberspace has become a new locus for criminal activities, making this an interesting topic of discussion for study in various sciences. Criminal activity has increasingly occurred in recent years, making cyberspace a new space for criminals. Various kinds of conventional crimes in real life are currently starting to transition to cyberspace; one of the most frequent is fraud. Fraud that previously occurred in physical space has currently transitioned to cyberspace. This is one of the impacts of the development of communication technology, the Internet, and new media (Sari et al., 2022).

To analyze empirical problems with space transition theory, an analysis of case facts using the postulates that build this theory is required. The postulates of this theory are as follows:

1. A person with evil behavior who is depressed in real life tends to commit crimes in cyberspace.

2. The flexibility of identity, anonymous disassociation, and limited deterrent factors in cyberspace provoke perpetrators to commit crimes in cyberspace.
3. Evil behavior of someone in real life can shift to cyberspace, and vice versa; evil behavior in cyberspace can also shift to real life.
4. Intermittent attempts of criminals in cyberspace accompanied with the natural nature of space and time in cyberspace, give opportunities for criminals to escape.
5. Criminals who do not know each other tend to meet in cyberspace and then commit crimes in real life.
6. The association of criminals in real life tends to unite perpetrators to commit criminal acts together in cyberspace.
7. Someone from a closed society has a greater tendency to commit crimes in cyberspace than someone from an open society.
8. Conflicts between norms and values from real life and cyberspace can cause crimes in cyberspace.

Several postulates in space transition theory will be closely associated with cyber fraud, which is currently widespread on social media. Thus, cyber fraud will become a suitable analysis tool for analyzing how someone can commit cyber fraud on the Internet.

The Concept of Cyber Culture

Cyberculture is a study of culture in cyberspace (Bell in Suseno, 2019). Since the Internet was founded, human activities have slowly shifted from real life to utilizing the Internet to do their activities. The use of the Internet, which allows humans not to interact with each other directly, certainly forms new patterns of human behavior in cyberspace (Rafiq, 2020). Thus, cyberculture can briefly be explained as certain habits or values developed in cyberspace so they become a culture in cyberspace. In other words, cyberculture emerges from the use of computer networks for communication, entertainment, and business (Rachman, 2017).

When seen from history, cyberculture initially developed to exchange ideas and promote ideas related to the development of information and communication technology (Kautsarina, 2018). In its development in the contemporary era, cyberculture has increasingly influenced human life, including cultural dynamics and social relations. Therefore, it is important to understand and study cyberculture in the digital era to adapt to developing cultural dynamics, especially in cyberspace or the Internet. An adequate understanding of cyberculture will help someone to do activities in cyberspace and prevent them from undesirable things, such as being a victim of a crime or experiencing losses when doing activities in cyberspace (Azzani et al., 2023).

In this study, the concept of cyberculture explained how cyber fraud in Wajo Regency, South Sulawesi, from the cultural aspects that are currently developing on social media. The characteristics of the perpetrator and victim, as well as the case description described in this study, were enough to analyze how the victim understands the culture developing on social media.

Discussion

The development of the use of information technology in each line of human life has entered an era where the Internet is used for various political, economic, social, and cultural activities (Indrawan, 2019). In the economic aspect, the Internet is used to carry out various activities, which previously could only be carried out by direct interaction in real life; for example, buying and selling goods in shopping centers has shifted to buying and selling using the Internet in cyberspace. These activities continue to develop until various online platforms for buying and selling goods and services are created in cyberspace.

Buying and selling activities in cyberspace are currently becoming an alternative to effective and efficient trading (Susanto & Pangesti, 2021). Prospective buyers can see various products without going to the sellers' places. The prospective buyer can also compare the price of a product quickly because there is a certain algorithm that can filter and sort certain products according to certain prices or categories. This algorithm will really help consumers find products according to their desired criteria.

Currently, several buying and selling platforms in cyberspace are increasing and developing, such as Tokopedia, Lazada, Shopee, and Blibli. Online buying and selling platforms compete to dominate online buying and selling markets with various attractive features and promos. Moreover, there are buying and selling platforms that specifically become a forum for buying and selling used goods, such as OLX and the Marketplace feature in the Facebook application that sells various used goods, from vehicles to electronics. In its development, social media applications have also been used for buying and selling activities. Social media accounts, such as Instagram, TikTok, Facebook, and Twitter, with many followers, are often used to make online buying and selling activities or as promotional media that effectively reach social media users.

From the explanation above, in principle, communication using the Internet via any media can be used to make economic activities. The use of internet media for economic activities really helps effectiveness because social media can reach all levels of society (Harahap & Adeni, 2020). In this digital era, almost all people have digital devices and social media accounts, encouraging people to have economic activities via social media. Moreover, the use of Internet media also increases efficiency. Sellers and buyers no longer have to go to shopping places to make transactions; sellers no longer have to rent a shophouse and other conveniences that can increase the efficiency of time and cost.

In the context of a case study in this study, the author intends to analyze what and how cyberculture in cyber fraud in Wajo Police, South Sulawesi, to obtain a comprehensive understanding regarding how the perpetrator commits cyber fraud and how the victims can be deceived to make online buying and selling transaction in this case. According to the explanation of the incident explained at the beginning of this study, it can be analyzed how the study of cyberculture in this case can be explained as follows:

Facebook application, one of Indonesia's most mainstream social media applications, has been widely used by its users to make online trading activities. Over time, opportunities for crime arise from online buying and selling activities. This can be understood because of the ease of creating a Facebook account that allows for fake accounts (for example, through profile cloning), so criminals can fake their identity on social media. Therefore, criminals can commit various illegal acts, including cyber fraud.

Cyber fraud using social media, such as Facebook, has been occurring in various modes for a long time. Many cyber fraud cases have been revealed, and law enforcement officers have been putting in the effort to solve them. In fact, the phenomenon of cyber fraud continues to occur and cannot be removed from cyberspace. In order to understand this, it can be seen in real life where crimes also cannot just be removed even though law enforcement continues to run because criminals will also develop to find new ways and modes of committing criminal acts. Likewise, in cyberspace, when a cyber fraud mode is no longer effective in deceiving victims, the perpetrators continue to innovate, creating new modes to deceive subsequent victims. From this point, the author intends to show how cyber fraud on social media, especially on Facebook applications, has become a cyberculture because it is considered commonplace on social media. Even though various efforts have been made to remove the phenomena of cyber fraud from Facebook, both carried out by law enforcement officers through law enforcement efforts and by Facebook developers through internal regulations in the application, in fact, until this time, this phenomena still occur.

Regarding buying and selling activities on Facebook, most users understand that many fake accounts commit cyber fraud on this social media platform, not only on Facebook but also on almost all social media platforms, such as Instagram. Therefore, Facebook users will generally be really careful when making buying and selling activities using this application so they do not become cyber fraud victims. There are several ways commonly carried out by Facebook users before making online buying and selling transactions. One of them is asking relatives or friends if anyone has made buying and selling activities with Facebook accounts to avoid making transactions with fake accounts. If relatives or friends have previously successfully made transactions with an account, it can be confirmed that the account does not commit fraud. Another way is by profiling Facebook accounts that will sell or buy goods by searching via their social media accounts. Fake accounts usually have a short history, which is different from real accounts that usually have been around for a long time

and have a long history of activities on social media. Another method is being aware of suspicious things in the buying and selling process.

The suspicious things in the buying and selling process with fake accounts should be threat with suspicion if, first the price is very cheap and unreasonable, far below the market price. The perpetrators usually argue that the low price is because the items sold are from auctions or refurbished goods. Using fake product photos or ones that have been edited using specific applications. Second, this usually can be seen when the product photos look perfect or unrealistic. Third, the account name is usually similar to a popular brand's name; for example, only one letter is different from the original brand name. For example, the account @adidasindonesiaofficial is to be @addidasindonesiaofficial. Also, if the activity history on social media is not much, we also need to thread it with suspicion. This is because the perpetrator of cyber fraud often changes social media accounts. This is committed to avoid tracing victims who have been successfully deceived. Then, if a product post has a comment feature or review, there will be many similar and repeated comments and reviews. It seems like many people review it even though the fake account itself also commits this using other social media accounts. Moreover, reviews written by fake accounts are usually short, consisting of only several words, but many. Lastly, the name in the bank account is different from the name on the social media account. The difference between the name in the bank account and the name on the social media account is not always committed by a fake account, but this can be one of the verification methods to check the authenticity of a buying and selling account.

From the explanation above, the authors intends to explain that it has become a cyberculture on Facebook to carry out various checking steps before making buying and selling transactions to avoid cyber fraud. The victim, Mr. Olfan Mundok, did not carry out this step, so he was deceived into making buying and selling transactions of the vehicle. Furthermore, the Facebook application also has a menu called Marketplace, which functions to facilitate the buying and selling activities of Facebook users. This point also becomes cyberculture on Facebook, where if users want to engage in buying and selling activities, they will use the Marketplace on Facebook. This culture was not understood by the victim, Mr. Olfan Mundok, so he only saw a post that appeared on the "Home Page" and did not search for the product on the Marketplace on the Facebook application.

Based on the analysis above, an explanation can be obtained as to why Mr. Olfan Mundok could be deceived and become a cyber fraud victim with a profile cloning mode. By paying attention to the profile of the victim, who graduated from secondary school and worked as a farmer, it can be analyzed that the victim very likely does not understand several cybercultures on the Facebook application. The limited understanding makes the victim not take the checking steps to the "Kiki Widya S" account, whether it was true that it was a policewoman who served at National Police Headquarters or a fake account. The victim was also not suspicious of the lower price offered by the

perpetrator, which was far from the normal price. Victims at least must ask why an item is being sold at a price far under the market price because someone usually sells goods to make a profit.

Referring to the analysis above, it can seen that there are still many Indonesian people who are unfamiliar with things commonly occurring on social media. The government should be responsible for providing massive education and socialization to the public to prevent crimes in cyberspace. Crimes, such as cyber fraud, have occurred for a long time, but people still become victims of these crimes due to various factors, including the minimum education (Wahyudi et al., 2022). The government, through the related ministries and institutions, should actively identify actual cyber crimes and crimes that have the potential to occur in the future to take preventive steps so people no longer become victims. Moreover, it has also been explained that space transition theory can analyze how someone can commit cyber crimes. In order to explain a phenomenon, this theory has several postulates that can be used as an analysis. Thus, the author analyzed fraud cases committed by Mr. Abdullah in Wajo, South Sulawesi, using the space transition theory as follows:

First, it can be explained that a person with evil behavior depressed in real life tends to commit crimes in cyberspace. This is in line with the profile of Mr. Abdullah, who is known to not have a permanent job or is unemployed. As an adult at 22 years old, when the case occurred, the person certainly should live independently and be able to meet his own needs. The person is even old enough to get married. Therefore, the perpetrator has a tendency to be depressed in real life, which can provoke him to commit crimes in cyberspace through cyber fraud with profile cloning mode. Thus, the condition of the perpetrator who is under pressure in real life transfers his crimes in real life in accordance with this postulate.

Second, it is stated that flexibility of identity in cyberspace provokes the perpetrator to commit crimes in cyberspace. This is in accordance with the fact that cyber fraud with the perpetrator, Mr. Abdullah, used profile cloning mode in his act. The perpetrator utilizes the ease in manipulating identity on social media and uses it to commit cyber fraud. To create a social media account, such as a Facebook account, the account creator only fills in personal data without factual validation to ensure the identity of the account owner. In the Facebook application, someone can have more than one account because the basis of a Facebook social media account is an email account, not the population identity number. In order to create an email account, there is no factual verification to ensure the validity of the identity registered to create an email account. Therefore, in the Facebook application, it is possible for someone to create a Facebook account that can be misused to commit various crimes in cyberspace, such as cyber fraud.

Third, the natural nature of space and time in cyberspace gives opportunities for criminals to escape. This is in accordance with the cyber fraud in Wajo Polic if paying attention to the description of the case, where the cyber fraud committed by Mr. Abdullah to the victim, Mr. Olfan Mundok, occurred in December 2020. Several months later, the perpetrator was arrested in March 2021 for

committing the action against other potential victims. If the perpetrator utilized several months before being arrested to escape, there is the possibility that the perpetrator would not get arrested by the law enforcement officers. In this case, the perpetrator did not do it because he felt that the law enforcement officers could not detect his action, even though the perpetrator had the opportunity to escape.

Fourth, it is stated that the association of criminals in real life tends to unite perpetrators to commit criminal acts in cyberspace. As explained in the description, the raid carried out by the Criminal Investigation Unit of Wajo Police began with information from the public, which stated that the house becoming a crime scene became a basecamp or gathering place for cyber fraud (pasobis) perpetrators in Kecamatan Maniangpajo, Wajo Regency. This means that there are many other perpetrators who usually act in this house, even though when the arrest, only Mr. Abdullah was committing cyber fraud in the house. This can be proven by the many laptops and mobile devices that were obtained during the arrest. This fact strengthens the suspicion that usually there are usually many cyber fraud perpetrators operating in this house. This shows that Mr. Abdullah, with his friends, is most likely a network or syndicate in real life who commits criminal acts in cyberspace, as one of the postulates in space transition theory.

Fifth, it is stated that someone from a closed society has a greater tendency to commit crimes in cyberspace compared to someone from an open society. Cyber fraud perpetrators in South Sulawesi (Pasobis) will usually look for quiet places or avoid crowded environments. This is important so the perpetrator's activities are not suspected by the local community. When committing the act, the perpetrator usually will stay at home for days without leaving the house or interacting with the environment because cyber fraud activities require the perpetrator to always stand in front of his/her digital devices, waiting for victims to respond to the fraud actions. Thus, this postulate is in line with the characteristics of cyber fraud perpetrators, where a person from a closed community tends to commit crimes in cyberspace compared to a person from an open community environment.

The correspondence between postulates in space transition theory and facts in the cyber fraud case with profile cloning mode in the jurisdiction of the Wajo Police, South Sulawesi, can answer why a person can commit cyber fraud crime, including due to pressures in real life that provoke the perpetrator to commit crimes in cyberspace, flexibility of identity in cyberspace, the natural nature of space and time on social media, environmental and friendship factors, and characteristics of the perpetrators who tend to be closed or in closed environment. These factors have comprehensively explained why a person commits cyber fraud.

According to the analysis of cyber fraud cases with profile cloning mode that still occurs in Indonesia, a description showed that the government has not been able to prevent and overcome cyber crimes effectively. The government should be able to prevent crimes in cyberspace through the implementation of strict regulations on social media. For example, when creating a new account on

social media, verification, such as face recognition, should be carried out to prevent fake accounts (Afrizal et al., 2022). The government can also strictly separate social media platforms and e-commerce platforms. Besides the government, social media developers, such as Facebook, also should support the efforts to prevent crimes in cyberspace. Social media developers should not only pursue profits by allowing many fake accounts to be active on social media, but they should also be responsible for ensuring the safety and convenience of social media users by supporting stricter policies for account creation.

CONCLUSION

According to the explanation above, the author draws several conclusions obtained from the analysis of cyber fraud with profile cloning mode in Wajo Police using space transition theory and the concept of cyberculture. From the discussion of the concept of cyberculture, the conclusion is obtained that cyber fraud with the victim, Mr. Olfan Mundok, can occur because the victim does not understand several cybercultures in making buying and selling transactions using social media, mainly the Facebook application. The victim might not understand that many fake accounts in the Facebook application act to deceive Facebook users. Thus, the victim was not suspicious or even interested in the certain product offered in the Facebook application. The victim might also not understand that if someone would like to make transactions on social media, they should carry out checking steps to ensure that they do not have transactions with fake accounts committing fraud. Thus, the victim immediately decided to transfer money without knowing whether the policewoman's or seller's account was real or fake.

Furthermore, from the analysis using space transition theory, it can be concluded that cyber fraud with perpetrator Mr. Abdullah is in accordance with several postulates in space transition theory. First, there is a correspondence between postulate 1 and the profile of the perpetrator, Mr. Abdullah, who is unemployed and tends to be depressed in real life due to the demands of life's necessities, so he committed crimes in cyberspace through cyber fraud with profile cloning mode. Postulate 2 is in accordance with the fact that the perpetrator utilizes the ease of manipulating identity on social media and uses it to commit cyber fraud. Postulate 2 is in accordance with the fraud case because the perpetrator, Mr. Abdullah, had the opportunity to escape due to cyber fraud crimes in December 2020, and the perpetrator was arrested in March 2021. Postulate 5 is in accordance with information from society that Mr. Abdullah is usually not alone in the house and has a group that commits crimes in cyberspace. The last, postulate 6, is in accordance with the characteristics of the perpetrator, Mr. Abdullah, which tends to be closed, so he has a tendency to commit crimes in cyberspace.

Based on the analysis of the cyber fraud case, it can be concluded that the government is still unable to prevent crimes in cyberspace, such as cyber fraud. The lack of community education and

permissive regulation of social media contribute to the existence of cybercrimes. Criminals can easily create fake accounts, which will then be used to commit crimes. The community is also not provided with appropriate knowledge to avoid crime in cyberspace.

SUGGESTION

Cyber fraud continues to occur in the middle of the increasingly advanced development of information and communication technology. Various cyber fraud modes continue to change and develop, so the community should be aware of not being a victim when having activities on social media. Therefore, the author suggests that the next researcher conduct a study related to the analysis of cyber fraud with various modes that are developing. This is important so that the government understands the characteristics and methods of handling cyber fraud cases that continue to occur. By understanding the details and characteristics of cyber fraud, the government and academics will also have adequate capacity to provide education to society to avoid cyber fraud with profile cloning mode.

Moreover, strengthening regulations on social media is required to prevent account cloning or the creation of social media accounts that do not match the user's personal data. Face recognition technology has been widely used in banking and government applications. Social media, mainly Facebook, should also implement regulations related to account creation verification, such as using face recognition technology. Therefore, fraud with profile cloning mode can be prevented or reduced due to more valid regulations for social media account creation.

REFERENCES

Afrizal, T., Paramita, A., & Sulaiman, H. (2022). Sosialisasi keamanan transaksi belanja online pada remaja karang taruna. *Jurnal Pengabdian Kepada Masyarakat Bangun Cipta, Rasa, & Karsa*, *1*(4), 98-104.

Azzani, I. K., Purwantoro, S. A., & Almubaroq, H. Z. (2023). Urgensi peningkatan kesadaran masyarakat tentang kasus penipuan online berkedok kerja paruh waktu sebagai ancaman negara. NUSANTARA: *Jurnal Ilmu Pengetahuan Sosial*, *10*(7), 3556-3568.

Bernoza, A., Fadlan, F., & Nurkhotijah, S. (2020). Analisis yuridis tindak pidana penipuan berbasis jual beli online di Kota Batam (Studi penelitian Polresta Barelang). *Zona Hukum: Jurnal Hukum*, *14*(3), 1-11.

Bhariatta, E. C., Rufaidah, I. N., & Adnina, M. R. (2019). Jual beli followers, likes, viewers di Instagram perspektif hukum ekonomi syariah. *El-Qist: Journal of Islamic Economics and Business (JIEB)*, *9*(1), 32-45.

Creswell, J. W. (1998). Qualitative inquiry and research design: Choosing among five traditions. SAGE Publications.

Esfandari, D. A., & Ridhayani, R. (2019). Analisis deskriptif profile cloning pada akun Instagram @Feydown waspada love scam. *Jurnal Prosiding ISBI Bandung*, *1*(1), 17-23.

Hamid, S., & Pedrason, R. (2023). Edukasi penanggulangan kejahatan penipuan online di masyarakat desa Gunung Putri Kabupaten Bogor. *Wikuacitya: Jurnal Pengabdian Kepada Masyarakat*, *2*(1), 202-209.

Hamid, S. (2023). Peningkatan deteksi-aksi berbasis data, informasi, dan kejadian aktual untuk pemetaan situasi kamtibmas melalui pemolisian prediktif dalam rangka pemeliharaan kamtibmas. *Jurnal Ilmu Kepolisian*, *17*(2), 25.

Handoko, H. P. (2021). Perlindungan hukum terhadap pengguna smartphone dari penipuan iklan. *Jurnal Ilmu Kepolisian*, *15*(1), 15.

Harahap, M. A., & Adeni, S. (2020). Tren penggunaan media sosial selama pandemi di Indonesia. *Professional: Jurnal Komunikasi Dan Administrasi Publik*, *7*(2), 13-23.

Indrawan, J. (2019). Cyberpolitics sebagai perspektif baru memahami politik di era siber. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *10*(1), 1-16.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), Crimes of the Internet (pp. 283-301). Prentice Hall.

Karyono. (2013). Forensic fraud. CV. Andi.

Kautsarina, K. (2018). Perkembangan riset etnografi di era siber: Tinjauan metode etnografi pada dark web. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi*, *8*(2), 145-158.

Moleong, L. J. (2020). Metodologi penelitian kualitatif. Remaja Rosdakarya.

Mudjiyanto, B., & Roring, F. P. (2024). Tendensi politik kejahatan dunia maya. *JIKA (Jurnal Ilmu Komunikasi Andalan)*, *7*(2), 26-51.

Munti, N. Y. S., & Syaifuddin, D. A. (2020). Analisa dampak perkembangan teknologi informasi dan komunikasi dalam bidang pendidikan. *Jurnal Pendidikan Tambusai*, *4*(2), 1975-1805.

Prabhaswara, S. (2023). Analisis yuridis terhadap tindak pidana penipuan di dalam penggunaan media sosial. *Jurnal Bevinding*, *1*(03), 62-80.

Pusiknas Polri. (2022). Kejahatan siber di Indonesia naik berkali-kali lipat. Pusiknas Polri. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat#:~:text=Bahkan%20jumlah%20tindak%20kejahatan%20siber,Januari%20hingga%2022%20Desember%202022

Putri, F. A. (2022). Studi tentang penipuan melalui media online pada masa pandemi (Tesis). UIN Walisongo.

Rachman, R. F. (2017). Menelaah riuh budaya masyarakat di dunia maya. *Jurnal Studi Komunikasi*, *1*(2), 206-222.

Rafiq, A. (2020). Dampak media sosial terhadap perubahan sosial suatu masyarakat. *Global Komunika: Jurnal Ilmu Sosial Dan Ilmu Politik*, *3*(1), 18-29.

Sabilah, H. (2023). Penipuan digital: Antara penipuan dan privasi data dalam hukum pidana Islam. Sharia and Law Proceedings, *1*(1), 101-116.

Sahabuddin, S., & Andrizki, L. D. (2024). Tindak pidana pembobolan rekening via online berkedok link (Suatu kajian terhadap perundang-undangan informasi dan transaksi elektronik). *Jurnal Wajah Hukum*, *8*(1), 461-467.

Sari, E. P., Febrianti, D. A., & Fauziah, R. H. (2022). Fenomena penipuan transaksi jual beli online melalui media baru berdasarkan kajian space transition theory. *Deviance Jurnal Kriminologi*, *6*(2), 153-168.

Setiawan, D. (2018). Dampak perkembangan teknologi informasi dan komunikasi terhadap budaya. *Jurnal Simbolika Research and Learning in Communication Study*, *4*(1), 62-72.

Siboro, S., & Hadiningrum, S. (2024). Tantangan penegakan hukum perdata di era digital. *Public Service and Governance Journal*, *5*(2), 52-59.

Susanto, R., & Pangesti, I. (2021). Analisis faktor-faktor yang mempengaruhi masyarakat kampung Cilangkap Kota Depok dalam pengambilan keputusan pembelian di online shop. *JABE (Journal of Applied Business and Economic)*, *8*(2), 182-189.

Suseno, B. (2019). Konsep Facebook policing sebagai pencegahan kejahatan sekunder profile cloning crime. (Disertasi). Sekolah Tinggi Ilmu Kepolisian, Jakarta.

Syarief, E., Shahrullah, R., Fitrianingrum, A., & Agustina. (2016). Legal approaches to online arbitration: Opportunities and challenges in Indonesia. *Jurnal Mimbar Hukum*, *28*(2), 314-321.

Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). Akibat hukum bagi pelaku tindak pidana penipuan online melalui modus arisan online di media sosial elektronik. *Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana*, *4*(2), 326-336.