



Criminal Law Enforcement in Overcoming Crimes Arising from the Existence of Fake Account From a Criminological Perspective

Rosalia Dika Agustanti¹, Bambang Waluyo², Slamet Tri Wahyudi³, Abdul Kholiq⁴,
Nashwa Hatta Aqila⁵

^{1,2,3,4,5} Faculty of Law, University of Pembangunan Nasional Veteran Jakarta, Jakarta -
Indonesia
rosaliadika@upnvj.ac.id

Abstract. One of the new issues in human existence brought about by the rapid advancement of technology is cybercrime, which communicates with its victims through fictitious accounts. This article aims to investigate the strategies used by law enforcement to apprehend criminals who utilize fictitious accounts to carry out their heinous deeds. Although there are clear regulations governing information and electronic transactions, the execution of the law has not been fully utilized because of challenges in obtaining evidence or errors made by law enforcement in interpreting evidence. This kind of research takes a statutory approach while using normative legal approaches. Although the results indicate that not all fictitious accounts are used for illegal activity, this will facilitate criminal activity since it is difficult to identify the true identity of an individual using a fictitious account. This affects a person's capacity for responsibility. If so, criminology can be used to understand what makes someone commit a crime which ultimately provides a concept of proof, so that law enforcement against crimes with these false accounts can be handled properly.

Keywords: Criminal Act, Fake Account, Criminology.

1 Introduction

Internet social network users that want Fake accounts are commonly used to perpetrate crimes such as sending spam, committing fraud, or abusing the system. A single bad actor has the ability to create dozens or even thousands of fake accounts in order to scale their operations and find as many new members as a series of crimes. But any fraudulent account someone has could appear legitimate at first glance, for instance, if it has a legitimate-sounding name or a reliable profile picture. People from all over the world today rely on online social networks to search for resources and information, create new relationships, and share ideas, thoughts, and experiences. But the same qualities that ordinary people find useful also make social networks vulnerable to misuse in different kinds. For instance, a platform with a sizable audience is a prime target for spammers and con artists, and the target may be more likely to fall for a scam due to the platform's reputation [1].

Popular apps for sharing a range of content, such as text, images, and videos, are online social networks. Nonetheless, one of the challenges facing the modern online social

networking system is the issue of fraudulent accounts. Attackers utilize fictitious accounts to disseminate false information and harmful URLs, viruses, or malware [2]. In addition to providing incentives for certain people to create false profiles, the presence of false accounts might lower the value that legitimate users derive from online social networks. For instance, Users could damage the network's reputation if they begin to doubt the accuracy of profile information. Additionally, advertisers can wonder about the costs they incur to reach a specific user base if a sizable fraction of the users are fraudulent., which might negatively affect a network's ad income.

Millions of people use social networking sites like Facebook and Twitter every day, and their interactions with these networks have tremendous impact on their lives. Due to its popularity on social media, there are a number of issues that have arisen, such as the potential for users to be exposed to false information through phony accounts, which could lead to the spread of harmful content. This circumstance may cause significant harm to society in the actual world [3].

According to the survey, there are 500 million female-owned Facebook profiles, yet there are only about 300 million women worldwide. Thus, we can estimate the quantity of unnecessary data and fictitious accounts that are being generated. And how can we recognize phony social media accounts? Identification by post, tweet, and status is not possible in full. We must delve further into the idea and look into the accounts [4]. Furthermore, users can follow celebrities and fan pages locally or worldwide on the well-known Instagram platform. Because Instagram is more widely used for producing material and fake news than Facebook, the number of phony accounts on Instagram is growing daily.

The majority of people in the world now use online social networks because they spend a lot of time using these platforms to engage with others and exchange information, from adults to children to the elderly. On the one hand, this social network offers the benefits of direct communication, information exchange, building a big audience, etc. However, there are also numerous ways in which people misuse it. Social networking companies lose money as a result of users who primarily use false identities to take advantage of weaknesses in their business practices, such as appealing target accounts that are used to click on harmful links or commit other cybercrimes [5].

Numerous elements, including social, cultural, economic, and others, contribute to crime. These Indonesian elements demonstrate a detrimental impact. The number of people who commit crimes only aims to make ends meet. Hardianto, Djanggih and Nurul Qamar, "Application of Criminological Theories in Cyber Crime," *Pandecta Research Law Journal* 13, no. 1 (2018): 10–23. Because they include citizens as users, crimes resulting from the establishment of phony accounts constitute a threat to state security. In order to make up for this, the government needs to focus on both how to prevent crime and its manner of operation [7]. Every progress basically has an effect in the form of positive and bad sides, which are like two sides of a coin that are connected and inseparable [8]. Based on this background, to concentrate on the examination of the paper's theme, which the author outlines in two problem formulations, specifically as follows: What are the factors that cause someone to create a fake account? and How does criminal law enforcement in tackling crimes arising from fake accounts in a criminological perspective?

2. Research Methods

The Normative Yuridis (legal research) method is employed, which combines a case-based and legal approach [9].

3. Results and Discussion

3.1 Factors Causing Someone to Create a Fake Account

Social media platforms on the internet are changing how people interact with one another and exchange political, business, and personal information. Similar to cyberspace on the Internet, users can now rely solely on their mobile phones and other devices that enable the capabilities required by this online social media program instead of physically meeting in person. Because there are so many online social media platforms, malevolent entities are drawn to them and attempt to take advantage of their flaws and vulnerabilities. Many online social media platforms have tens of millions or even hundreds of millions of members, which results in billions of pieces of content containing personal information that might be misused. Through online contacts with the victim's acquaintances, fake profiles can be used to cultivate relationships with them in order to eventually obtain the victim's personal information [10].

It is well known that crimes can occur on online social networks, where offenders will create numerous fictitious profiles and utilize them to commit a variety of crimes [11]. These days, a person's power frequently hinges on how many followers they have on their own social media accounts. In light of this, the prevalence of phony accounts is among the most pertinent issues and has the ability to significantly affect a wide range of personal and professional endeavors. Social media sites should be wary of fake followers because they have the potential to distort ideas about influence and popularity, which can have a significant impact on society, politics, and the economy [12].

In today's world, social media networks on the internet are crucial. It not only fundamentally alters communication, but it also opens up new avenues for possible attacks like identity theft and fraudulent information, among others. Recently, phony accounts on social media have caused issues for several social media platforms. Online social networking companies suffer from an overabundance of advertisements, the dissemination of incorrect information, etc., as a result of the high number of bogus account creation [13].

According to new research, individuals unintentionally reveal an astounding quantity of personal information on online social networks. Furthermore, according to recent estimates, there are tens of millions of bogus user profiles on the network, endangering the security and privacy of users [14]. In contrast to a cloned account, which is created by the user from the original account when the user profile is copied, a false account does not create new accounts from scratch. Typically, the purpose of cloning an account is to obtain the victim's or his friends' information; nevertheless, the fictitious account can be used for many purposes, such as spamming, advertising, scamming, and so forth.

There are several reasons why someone could make a fake account, including the need to have many accounts in order to log into different communities or to utilize the account for other hobbies. The three primary motivations for making fictitious accounts are as follows: (1) to boost one's popularity or degree of trustworthiness; (2) to disseminate spam to real users; and (3) because the service provider only permits one account to be connected to a single email address or phone number, users create multiple accounts using different email addresses or phone numbers to get around this restriction. Fake accounts only have a small number of connections since they lack reliable connections, are not the graph's center node, and lack any distinctive data or history [15].

Furthermore, users claim that the reason they utilize fictitious accounts is to feel more liberated when utilizing online social media. However, many of the users also claim that they use fictitious identities only for the purpose of stalking. It seems that using these kinds of accounts is a trend that makes sense and ought to be followed, particularly for teens. As long as they are used appropriately and don't cause harm to others, the existence of phony accounts is not an issue [16].

Therefore, it is crucial to understand from criminological considerations what motivates someone to make a false account and use it to conduct a crime, ultimately leading to the commission of a criminal act. The study of crimes stemming from false accounts makes use of a number of criminological theories. This is predicated on theoretical analyses of how well the ideas in these theories mesh with the traits of crime, the traits of offenders, and the responses of the general public to cybercrime in Indonesia [17].

3.2 Criminal law enforcement in tackling crimes arising from fake accounts in a criminological perspective

These days, internet is involved in a lot of social events that take place. For instance, because of the Covid-19 pandemic, everyone relies on the internet for everything. In the same way, using a smartphone is sufficient for communication. Unrestricted internet usage appears to have forgotten that Indonesia is a state governed by laws; various measures are unquestionably needed to restrict freedom in cyberspace.

Law enforcement officers' readiness to uphold existing arrangements is unquestionably necessary. Indonesian criminal law enforcement has several distinct and multifaceted features. There are frequently exceptions to the criminal code, as seen by the numerous criminal cases, including cybercrime, where law enforcement is tasked with apprehending criminals. This means that someone who shouldn't be guilty could end up as a suspect, and someone who should be guilty by the law is released from bondage [18].

Therefore, additional methods that are observable from a criminological standpoint are required in order to ascertain the perpetrator's guilt. There are four (four) things that motivate criminals to commit crimes, and criminology is the science that analyzes crime in action [19]. First, economic factors supported by the large number of "subjective *nahrungsschwerung*" or making the crime rate increase. There is no longer any excuse, namely because of the economic squeeze in addition to soaring prices of necessities and lack of income. So that this economic factor becomes the main

motivation for someone to commit a crime. Second, social environmental factors where usually the perpetrator consists of several people who are related to each other, the environment has a great influence on the life and behavior of individuals in it. So it is not uncommon to find that there are still many group members together committing crimes. Third, the place factor that is synonymous with the opportunity to commit crimes if it is done in a dark, quiet place and far from community settlements. Because if there are potential victims there, when the conditions of the place do not support the commission of a crime, then the perpetrator will think again so that he can discourage his intention to commit a crime. Fourth, imitating crimes in other areas that usually get a role from the media, where the media displays various types of crimes of a national nature. Of course this for some people becomes a new idea in committing crimes.

When criminology first emerged, it was thought to be a discipline that examined all aspects of crime, including offenders, how society views them, and the status of victims of crime .M. Kemal Darmawan, *Criminology Theory* (South Tangerang: PT. Gramedia, 2020). Researching crime entails examining the causes of crime and why some people commit crimes while others do not. Another key element in understanding why crimes might happen in society and be committed by certain individuals is the social responses that society has to crime and criminals [20].

Because crime disturbs individuals and negatively affects their life, nobody wants it. Thus, criminal law enforcement is one means of combating crime of any kind in order to prevent it from happening as much as feasible [21].

If this legislation's enforcement is based on the criminal code's principle of legality—which states that no act may be penalized other than in accordance with current laws' criminal provisions and not the act itself—then the law may be enforced [22]. Criminal law is applied in public life based on the date, time, and location of the offense. The binding principle of legality as expressly stated by law states that an act cannot be prosecuted or punished if it satisfies the legal formula but was performed before the provisions of the law were enacted [23].

The Electronic Transactions and Information Law (ITE Law) was revised by Law Number 19 of 2016 to address changes to Law Number 11 of 2008 covering Electronic Information and Transactions,” has, of course, explicit regulations pertaining to this fraudulent account [24]. Fake identities, complete with names and profile pictures that don't correspond with the real person, are employed in some of the modes.

According to Section 1 of the ITE Law states which “electronic information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail (electronic mail), telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed that have meaning or can be understood by capable people understand it.” Furthermore, as per Article 1 paragraph 4 of the ITE Law, “electronic documents are any electronic information created, transmitted, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a computer or electronic system, including but not limited to writing, sound, images, maps, designs, photos, or the like, letters, signs, numbers, access codes, symbols, or perforations that have meaning or meaning or can be understood by a person capable of understanding them.”

Criminals who utilize fictitious identities and bogus accounts to commit crimes, including those who employ photos—which are contained in electronic documents and information as defined by the ITE Law. When it comes to the picture file that was utilized to create a phony account, the picture that is shown is electronic data, however the electronic document in the file is in jpg or another format [25].

The ITE Law's Article 35 also stipulates that "everyone intentionally manipulates, creates, changes, eliminates, or destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they were authentic data, without rights or against the law." The objective of the restrictions outlined in Article 35 of the ITE Law is to maintain the credibility of electronic information and documents, especially when it comes to electronic transactions. The reliability of electronic data or documents is shown by their authenticity. At the very least, the source and substance of an electronic document or information must be considered when assessing its validity. Two requirements must be met for an electronic information or document to be deemed authentic: (1) the source must originate from a person or party with the legal capacity to issue the information in question; and (2) the content must match the source's intended meaning [26].

The following ITE Law, paragraph 51(1), provides for the charging of criminal threats against the actions of an individual who uses an identity that differs from the original: "any person who satisfies the requirements listed in Article 35 may be sentenced to a maximum of 12 (twelve) years in prison and/or a maximum fine of IDR 12,000,000,000.00 (twelve billion rupiah)." To be sure, the law has made law enforcement operations easier, but it is not a set of rules; judges must consider the results of evidentiary procedures when determining a defendant's guilt or innocence.

4 Conclusion

Because individuals are able There are fake accounts that can be used to create an endless number of accounts on online social media networks.. Typically, in order to create an account, you need to provide your phone number or email address, which you can only use once. But in order to accommodate the 'trend' and the demands of certain users, a few then search for other ways to maintain several identities; setting up a new email address and purchasing a new phone number is the simplest way to accomplish this. However, some individuals also exploit this as an opportunity to further criminal activity. On the other hand, utilizing false identities, images of other people, and names makes them clearly detectable. The reason is because in the digital sphere, one cannot hide. However, as technology advances, criminals may still be able to hide online and carry out their illegal activities if law enforcement officials aren't any more "good" than the criminals themselves. Therefore, it is crucial that law enforcement officers establish guidelines and restrictions pertaining to social media accounts online in order to stop this.

Accounts that are deemed to be fraudulent must be withdrawn by the Information Technology and Communication Ministry since their existence is often unsettling and

damaging. Furthermore, to enable law enforcement personnel to work toward suitable and maximal enforcement in compliance with relevant laws and regulations.

References

1. Xiao, C., Freeman, D.M., Hwa, T.: Detecting clusters of fake accounts in online social networks. In: *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*. pp. 91–101 (2015).
2. Wanda, P., Jie, H.J.: DeepProfile: Finding fake profile in online social network using dynamic CNN. *J. Inf. Secur. Appl.* 52, 102465 (2020).
3. Erşahin, B., Aktaş, Ö., Kılınç, D., Akyol, C.: Twitter fake account detection. In: *2017 International Conference on Computer Science and Engineering (UBMK)*. pp. 388–392. IEEE (2017).
4. Raturi, R.: Machine learning implementation for identifying fake accounts in social network. *Int. J. Pure Appl. Math.* 118, 4785–4797 (2018).
5. Joshi, S., Nagariya, H.G., Dhanotiya, N., Jain, S.: Identifying fake profile in online social network: An overview and survey. In: *International Conference on Machine Learning, Image Processing, Network Security and Data Sciences*. pp. 17–28. Springer (2020).
6. Hardianto, D., Nurul, Q.: Application of Criminological Theories in Cyber Crime. *Pandecta Res. Law J.* 13, (2018).
7. Ketaren, E.: Cybercrime, Cyber Space, dan Cyber Law. *J. Times.* 5, 35–42 (2016).
8. Lisanawati, G.: Pendidikan tentang pencegahan kekerasan terhadap perempuan dalam dimensi kejahatan siber. *Pandecta J. Penelit. Ilmu Huk.* 9, 1–15 (2014).
9. Peter Mahmud Marzuki: *Penelitian Hukum*, Edisi. Kencana, Jakarta (2022).
10. Conti, M., Poovendran, R., Secchiero, M.: Fakebook: Detecting fake profiles in on-line social networks. In: *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. pp. 1071–1078. IEEE (2012).
11. Jia, J., Wang, B., Gong, N.Z.: Random walk based fake account detection in online social networks. In: *2017 47th annual IEEE/IFIP international conference on dependable systems and networks (DSN)*. pp. 273–284. IEEE (2017).
12. Caruccio, L., Desiato, D., Polese, G.: Fake account identification in social networks. In: *2018 IEEE international conference on big data (big data)*. pp. 5078–5085. IEEE (2018).
13. Chen, Y.-C., Wu, S.F.: FakeBuster: a robust fake account detection by activity analysis. In: *2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*. pp. 108–110. IEEE (2018).
14. Fire, M., Kagan, D., Elyashar, A., Elovici, Y.: Friend or foe? Fake profile identification in online social networks. *Soc. Netw. Anal. Min.* 4, 1–23 (2014).
15. Kareem, R., Bhaya, W.: Fake Profiles Types of Online Social Networks: A Survey. *Int. J. Eng. Technol.* 7, 919–925 (2018).
16. Setiawati, T., Vilya, D.A.: Background Of Anonymous Account Users Among Students. *KOMUNIKATA* 57. 3, (2022).
17. Djanggih, H., Qamar, N.: Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Res. Law J.* 13, 10–23 (2018).
18. Ediwarman, E.: The Paradox of Criminal Law Enforcement in Criminological Perspective in Indonesia. *Indones. J. Criminol.* 8, (2012).
19. Millah, I.A.: Penanggulangan kejahatan di masa pandemi Covid-19 (dalam perspektif kriminologi dan Viktimologi). *J. Komun. Huk.* 6, 497–513 (2020).
20. M. Kemal Darmawan: *Teori Kriminologi*. PT. Gramedia, Tangerang Selatan (2020).

21. Muliadi, S.: Aspek kriminologis dalam penanggulangan kejahatan. *Fiat Justisia J. Ilmu Huk.* 6, (2012).
22. P.A.F. Lamintang: *Dasar-Dasar Hukum Pidana Indonesia* (dasar-dasar untuk mempelajari hukum pidana yang berlaku di Indonesia). Sinar Baru, Bandung (1984).
23. Situngkir, D.A.: Asas Legalitas Dalam Hukum Pidana Nasional Dan Hukum Pidana Internasional. *Soumatera Law Rev.* 1, 22–42 (2018).
24. Agustani, R.D., Setiawan, A.N.: Tindak Pidana Penipuan Pada Transaksi E-Commerce Di Masa Pandemi Covid-19. *Era Hukum-Jurnal Ilm. Ilmu Huk.* 19, (2021).
25. Abi Jam'an Kurnia: *Hukumnya Membuat Fake Account di Media Sosial*.
26. Sitompul, J.: *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. PT. Tatanusa, Jakarta (2012).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

