INDONESIAN JOURNAL OF MULTIDISCIPLINARY SCIENCE

P-ISSN: 2808-5957
E-ISSN: 2808-6724
ijoms.internationaljournallabs.com

A LEGAL ANALYSIS ON ONLINE FRAUD USING FAKE IDENTITY

Juneidi Hasibuan[1], Syafrudin Syam[2]
Faculty of Syaria and Law, Universitas Islam Negeri Sumatera Utara, Deli Serdang, North Sumatera, Indonesia
[1] juneidihsb@gmail.com [2] syafruddinsyam@uinsu.ac.id

ARTICLE INFO

Published: July 27th, 2023

Keywords: *online fraud, fake identities, legal accountability, law enforcement, societal protection*

This work is licensed under CC BY-SA 4.0

ABSTRACT

This study aims to analyze the legal accountability for online fraud using fake identities, also known as catfishing. The phenomenon of catfishing has become increasingly prevalent with the advancement of information technology, particularly in the use of social media and online dating applications. The practice of online fraud using fake identities has detrimental emotional, psychological, and financial impacts on victims.The research method used is document analysis and literature review. Through document analysis, the researcher analyzes relevant texts and legal documents such as laws, regulations, court decisions, and government policies related to online fraud and fake identities. Meanwhile, through literature review, the researcher searches for and reviews relevant literature on the legal aspects of online fraud and fake identities.The research findings indicate that catfishing can be a violation of the law depending on the country and jurisdiction in place. Some countries have adopted laws that regulate online fraud and the misuse of fake identities. However, identifying catfish perpetrators and enforcing related laws often proves to be challenging as they employ various means to conceal their true identities in the virtual world. The legal accountability for online fraud using fake identities needs to be acknowledged and strengthened. In this regard, law enforcement and prosecution of catfish perpetrators are crucial to protect society from online fraud practices. Additionally, prevention and protection efforts involving education and public awareness regarding the risks and preventive measures against catfishing should also be enhanced.

INTRODUCTION

Various aspects of life, including the application of law, have been influenced by advances in information technology. The widespread use of electronic media, from mobile phones to increasingly sophisticated computers, is a hallmark of the growth of information technology. Many individuals are currently accustomed to using electronic media, which includes methods for collecting, preparing, storing, processing, announcing, analyzing, and/or transmitting information (Puspitasari, 2018).

With the development of technology and information today, many people abuse technology, especially on social media. it often happens that people take advantage of social media to gain profit by deceiving many people using fake identities or other people (catfish). The catfish phenomenon is one of the serious problems faced by many people. Scammers create new identities on social media accounts and other online applications using fake information. Using images that have been obtained or altered from someone else's information without the consent of the original owner of the stolen data is the most common type of identity theft. Catfishing activities are often carried out by perpetrators in online dating applications, even though it can occur in various virtual world applications (Putri & Hamzah, 2022).

Catfish itself is not only limited to the use of social media, but can also be found in online dating applications, discussion forums and various other forms of virtual interaction. In most cases, the catfish's main goals are personal gain, manipulating others, and creating false relationships. This phenomenon occurs more frequently and attracts the attention of the wider community because it has a negative impact both emotionally and psychologically for the victim. If someone gets caught in a web of lies and deceit orchestrated by the catfish, they may experience broken trust, emotional trauma, and even financial loss. In addition, catfish also raises complex legal issues. Identification of catfish perpetrators and associated law enforcement is often tricky, as they use various means to hide their true identities online.

In this case, the researchers were interested in analyzing how legal responsibility for online fraudulent acts using fake identities becomes very relevant. Here, the researchers discussed various aspects related to catfish, including the motivation behind the practice, the techniques used by catfish, the psychological impact on victims, the legal aspects involved, and preventive and protective measures. It is hoped that a better understanding of catfish will help people to be more careful and take appropriate steps in dealing with problems created by online scammers using fake identities. In addition, this legal analysis can also provide guidance for law enforcement in dealing with catfish cases and developing effective policies to protect the public from the harms associated with this.

METHODS

In discussing research methods for legal analysis of online fraud using fake identities (catfish), using the method, namely document analysis and literature review. The researchers search for literature, primarily scientific journals and books, to gain data. The data then were analyzed using documentation technique.

RESULTS AND DISCUSSION

Understanding of Online Fraudulent Actions Using Fake Identities

Catfish is a term used to describe the actions of someone who creates a fake profile or pretends to be a different person online, with the aim of deceiving or manipulating others. In the context of social media and online networks, catfishing is generally done by using fake photos, fabricated personal information, and fabricated stories to create fake identities that attract the attention of others. Catfishing is a "romance scam" and a form of fraud that occurs when someone falsifies their identity by creating a fake profile on social media and with the aim of tricking the victim (Wijayanto, 2021).

A new problem is in the form of crimes that often occur in the community through online media. This also has a very negative impact on society, such as the rise of new crimes in cyberspace (Zahra et al., 2022). Unlawful acts that refer to criminal activities in cyberspace by utilizing technological and telecommunication developments in the form of computer intermediaries or computer networks are also called Cybercrime (Hutasoit, 2018).

Catfish acts are often carried out with a specific motive, such as seeking attention, creating a false romantic relationship, gaining financial advantage, or causing harm and hardship to the victim. Typically, catfishers use online platforms such as social networks, dating apps, discussion forums, or chat rooms to impersonate and interact with others.

The actions of catfishing instigators can lead to illegal activities. People with fake profiles can engage in criminal activity through intellectual property infringement, defamation, or impersonation for the use of likeness of another person, or fraud. Almost anything that person does can have legal consequences when he or she harms someone else. There are no specific laws against catfishing yet, and this makes it more difficult to catch cybercriminals involved in the crime. In most cases, the victim can bring the catfisher to court by providing evidence of fraud or emotional distress and other issues (Rawat et al., 2021).

Of the various fraud cases that exist, catfishing is the number one fraud motive with 51% of victims being targeted by perpetrators. This form of catfishing fraud lasts a long time, for perpetrators it is a large investment of time and effort which can be undertaken for many motives. There was no main reason behind the actions of the perpetrators of catfishing, the reasons were various, such as simply feeling bored and lonely, the intention to extort money, to seek revenge or emotional exploitation and mental torment.

In some cases, catfish may also violate the law, depending on the country and applicable jurisdiction. Several countries have adopted laws governing online fraud and the misuse of fake identities.

Today there are several regulations that are used as a reference for cybercrime cases as already stated in the ITE Law. Regarding this matter, the public hopes that this regulation can provide protection to every user of technology and information facilities in Indonesia. Therefore, this condition is crucial based on the significant increase in the number of internet technology users.

Law Enforcement Against Online Fraudulent Actions Using Fake Identities

According to Abdulkadir (2006) "law enforcement can be formulated as an effort to implement the law as it should, supervise its implementation so that no violations occur, and if a violation occurs, restore the violated law so that it is enforced again."

Meanwhile, Jimly Asshidiqie (2006) divides law enforcement into two meanings, namely in a narrow sense it is "an action against any violation or deviation from laws and regulations through the criminal justice process which involves the role of apparatus such as police, prosecutors, lawyers and judicial bodies. As long as in a broad sense are activities that are carried out and apply the law and take legal action against any violation of the law committed by legal subjects either through judicial procedures or through arbitration procedures and other dispute resolution mechanisms (alternative dispute or conflict resolution)

From these two opinions or statements it can be concluded that law enforcement is an effort to improve order and legal certainty in society. This can be done by regulating the functions, duties and authorities of the institutions tasked with enforcing the law according to the

proportions of their respective scopes, and based on a good system of cooperation and support for achieving a goal. Thus, the law draws a line between what is in accordance with the law and what is contrary to it compared to what is legal (which is interpreted normatively as it should be), against the law this is actually more of a concern for law enforcement itself. Therefore, it can be concluded that law enforcement (especially criminal law) is a reaction to acts against the law" (Sudarto, 1995).

Furthermore, in terms of criminal law, it should be noted that this branch of law basically regulates the use of law and consists of regulations that define behavior that is prohibited and accompanied by penalties. To clarify that criminal law enforcement is an effort to maintain or actually function legal standards as a guideline for behavior in traffic or legal contact in social and state life, criminal law is part of law enforcement actions that regulate society. Criminal law enforcement can be interpreted as a broad subject and can also be interpreted as law enforcement activities that cover all subjects, depending on the subject's point of view.

There are two interpretations which of course can be taken into consideration in accordance with the criminal law theory of fraud, namely according to linguistic meaning and according to legal understanding. According to the language, the basic word for deception is "deceit" which means "a dishonest act or word (lying, fake, etc.) with the intent to mislead, outsmart, or seek profit; deceived" (Muladi, 2009). As for the legal sense, the definition of fraud is included in the definition of a crime in the Criminal Code, but the definition of fraud in the Criminal Code does not mean that it is understood; rather it only identifies the components of an act so that it can be said to be fraud and the perpetrators can be punished.

Article 378 of the Criminal Code states that "Whoever with the intent to benefit himself or another person against his rights, uses a false name or false character or uses deception or arrangement of false words, moves another person to hand over an object or enters into a debt agreement or negate a receivable, because one has committed fraud, is punished with a maximum imprisonment of four years."

Based on Article 378 of the Criminal Code, the researcher argues that in the crime of fraud (in the main form) there are various elements such as moving people to give goods or objects for personal gain even though it is against the law. Persuading the victim by using a fake identity such as name, position, dignity with a series of lies and clever tricks.

Acts of fraud are currently developing very quickly because it is difficult to prove if law enforcement officials only follow the articles of the Criminal Code. In the modern cyber environment, fraud can be carried out using a variety of techniques, from easy to complex. For example, fraud can be carried out in simple ways by spreading false information or impersonating someone else and then admitting it online, whereas complex ways can be shown in the actions of actors cooperating or conspiring. In this situation, the Criminal Code's prohibition against criminal acts of fraud will limit the imposition of sanctions or punishments for these crimes.

The same thing was conveyed by Maskun (2017), who said that "First, the criminals committed fraud against the computer system. Second, the series of actions of the perpetrators of

criminal acts is difficult to categorize into the methods regulated in the Criminal Code because as previously stated the methods regulated in the Criminal Code are aimed at people, not computer systems."

To strengthen this law, this can be linked to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and includes several articles, namely:

1. Article 28 paragraph (1): "Every person intentionally and without rights performs: access to all or part of the computer system; access to all or part of the electronic data contained in the computer system; destroys, changes, adds, subtracts, makes incorrect functions or eliminates the performance of all or part of the computer system or electronic data contained in the computer system, resulting in losses for other people or possibly causing harm to other people, shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp. 1,000,000,000.00 (one billion Rupiah)."
2. Article 30: "Every person who deliberately and without rights uses other people's electronic information and/or electronic documents in whole or in part which is contrary to laws and regulations, shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine Rp. 1,000,000,000.00 (one billion Rupiah)."
3. Article 51 paragraph (1): "Every person who intentionally and without rights uses electronic systems and/or electronic networks: carries out activities that violate the provisions of laws and regulations; provides, transmits, announces, or disseminates information intended to create hatred or hostilities of certain individuals and/or groups of people based on ethnicity, religion, race and inter-group (SARA) which can cause material and/or immaterial harm to certain people or groups of people; give, transmit, announce or disseminate information aimed at prohibited interests; commit insults and/or defamation; commit fraud; or f. commit other criminal acts, shall be punished with imprisonment for a maximum (six) years and/or a fine of a maximum Rp. 1,000,000,000.00 (one billion Rupiahs)."

Of the three articles, there is an element of prohibiting anyone intentionally and without rights from illegally accessing a computer system that can cause harm to others. Actions such as unauthorized access, damage, alteration, or loss of the performance of computer systems or electronic data contained in them. Establish prohibitions against hijacking other people's electronic identities. Establish criminal sanctions for perpetrators of electronic fraud.

As for Article 378 of the Criminal Code, it stipulates that a person who deliberately uses a trick, fake name, or fake letter to deceive other people with the aim of making the other person give goods, money, or securities that can cause losses in terms of property, then it can be subject to a maximum imprisonment of four years or a maximum fine of nine hundred Rupiahs.

In the context of catfish, if the perpetrator of catfish commits fraud by using trickery, misrepresentation of identity, or fake documents to deceive the victim and obtain financial gain or valuable assets from the victim, then article 378 of the Criminal Code can be used as a legal basis to take action against the perpetrator. This can be strengthened by Law no. 28 of 2008 ITE Article 28 paragraph 1, Article 30 and Article 58 paragraph 1.

Law Number 28 of 2008 ITE Article 28 paragraph 1, Article 30, and Article 58 paragraph 1 which regulates Information and Electronic Transactions can be used to convict perpetrators of online fraud. Article 378 of the Criminal Code regarding criminal acts of fraud cannot be used to hold perpetrators of online fraud accountable because there are many obstacles in enforcing criminal sanctions against perpetrators of crimes, such as barriers to evidence where evidence is limited by the Criminal Procedure Code. Only legal subjects (naturlijk persoon) are recognized by Article 378 of the Criminal Code, and it is difficult to decide which jurisdiction should be used to convict those responsible for online fraud, including transnational crimes and cybercrimes, where one of the characteristics cannot be restricted by boundaries of the sovereign territory of a country.

With these deficiencies in the Criminal Code, Law Number 28 of 2008 ITE Article 28 paragraph 1, Article 30, and Article 58 paragraph 1 concerning Information and Electronic Transactions, although it does not specifically regulate provisions regarding criminal acts of fraud, but in a context that different can still be used. burden perpetrators to be held accountable for their actions in terms of criminal acts of online fraud, in electronic transaction activities, or it can be said to be buying and selling online considering the actual context of the existence of the ITE law is as consumer protection. When the crime of online fraud is charged with Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law, the two articles in the two laws set aside and exclude each other.

Article 378 of the Criminal Code is a lex generalis for criminal acts of fraud, while Article 28 paragraph (1) of the ITE Law only applies to criminal acts of online fraud, which means only buying and selling activities online. In other words, Article 28 paragraph (1) of the ITE Law is a lex specialis of Article 378 of the Criminal Code which is a lex generalis for the crime of fraud, although both of them also have ambiguity in meaning.

The use of Article 28 paragraph (1) of the ITE Law is considered very appropriate to be charged directly to the perpetrators considering the elements and modes of online fraud which are increasingly sophisticated and keep up with the times, so there is no fear of the perpetrators escaping from punishment for their actions (Puspitasari, 2018).

Islamic Law Review of Online Fraudulent Acts Using Fake Identities

There is no clear policy governing the use of false identities in fraud in the rules of Islamic law, but there are examples of cases where the main actors can be used as a basis and evidence that crimes of fraud using counterfeiting have occurred when reading history. When Umar bin Khatab was in power, there was a case involving Mu'an bin Zaidah, who committed fraud by using a fake Baitul Mal stamp. The Baitul Mal officers then came to him to collect the fake stamps left at night and took them. Umar bin Khatab heard about the case and punished Mu'an with one hundred strokes and imprisoned him, then he was scolded and then beaten a hundred times and then exiled (Efendi, 2021).

According to this example, scams involving this type of forgery existed throughout the lifetime of the Prophet Muhammad and his followers. In connection with this deception, in a hadith the Prophet once said *"Who deceives us, then he is not part of us."* (Sahih Muslim).

This hadith emphasizes the rejection of fraudulent acts and emphasizes that people who are involved in such acts are not considered part of the Muslim community who are honest and loyal to Islamic teachings. In Islam, the principles of honesty, fairness and self-protection apply in all aspects of life, including online interactions. The values taught by Islam can be applied to maintain integrity and avoid fraud in cyberspace.

In Islamic law, it is strictly forbidden to lie, let alone lie that endangers the interests of others. Cheating is a shameful, evil act that interferes with the rights of others, harms others, and is contrary to the objectives of Islamic law. Fraudsters cannot be left alone to prevent this behavior from spreading further. To provide a deterrent effect and become a lesson for others, the perpetrator must receive a punishment commensurate with his actions. In the Qur'an, Allah SWT strictly prohibits the act of consuming other people's property in vain, as stated in the Al-Qur'an Surah al Nisa verse 29:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ مِنْكُمْ ۚ وَلَا تَقْتُلُوا أَنْفُسَكُمْ ۚ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا

"*O you who believe, do not eat one another's wealth in a false way, except by the way of business that takes place with love among you. And do not kill yourselves; Indeed, Allah is the Most Merciful to you."*

From this verse, it can be explained that in Islam it is strictly forbidden for us to consume wealth obtained in an improper way, such as deceiving someone to benefit us, it is unlawful to eat property obtained in an improper manner, such as the fraud earlier. In the verse it is also explained that there are exceptions, namely if we do business properly and well and it is also explained that Allah loves honest people very much.

Online transactions are prohibited for many reasons, including the fact that some of the goods or services involved are illegal, violate contracts, have fraudulent aspects, or harm people rather than benefit them. Online trading is acceptable in Islam as long as it does not involve elements of usury, tyranny, monopoly and fraud (Jannah, 2020).

Factors inhibiting law enforcement against online fraud using fake identities

Difficulties in Tracking Fake Identity (Asriyani & Dwiyanti, 2022)

Use of False Identities Catfish perpetrators often use false identities that are difficult to trace. They can use photos taken from the internet or steal other people's photos, making it difficult to know who is actually behind the fake profile. This fake ID can include names, addresses, phone numbers and other personal information designed to deceive victims. Use of Untracked Accounts Catfishers may also use anonymous accounts or accounts with limited

information, making it difficult to trace their digital footprint. They may use virtual private network (VPN) services or other online identity masking tools, which make it difficult to discover the perpetrator's physical location or real identity.

Ignorance and Suspicion of Victims

Embarrassment or Reluctance to Report: Victims of online catfish scams may feel embarrassed or reluctant to report the act. They also may not realize they have been a victim or do not have sufficient evidence to report it. Some victims may also fear that their report will not be acted upon or that they will be subject to further intimidation by the perpetrator, Stigma and Shame: Victims of online catfish scams often face stigma or feelings of shame for having been deceived. They may worry about the impact on their reputation or diminished self-confidence. This can prevent them from taking legal action or reporting the incident to the authorities. The social stigma associated with being a victim of online fraud can also make victims hesitate to seek help or share their experiences with others, thereby hampering the accountability of catfish perpetrators (Rahmanto, 2019).

Legal Limitations and Regulatory Discrepancies

Lack of Relevant Laws: Some jurisdictions may not yet have sufficiently clear or appropriate laws to address online catfish fraud. Existing laws may not be adequate in dealing with the challenges and fast developments of digital technology. The unavailability of specific and firm regulations related to online catfish fraud can hinder the process of law enforcement and accountability for perpetrators. Legal Differences in Different Countries: Regulatory discrepancies between countries can be an obstacle in prosecuting perpetrators and imposing adequate sanctions against them. If the perpetrator is in a country with inadequate or lax laws regarding online catfish fraud, prosecution can be difficult or even impossible.

Sophisticated Disguise Technologies and Methods

Use of Digital Tools and Techniques: Catfish perpetrators sometimes use sophisticated technology and disguise methods to trick victims and investigators. They can use tools such as photo manipulation software, IP hiding techniques or even artificial intelligence to create fake profiles that are difficult to detect. The technical expertise required to track and identify perpetrators who use this method can be a hindrance to authorities who do not have sufficient resources or expertise.

It is important to address these inhibiting factors in order to increase liability for online catfish scams. Collaborative efforts between governments, law enforcement agencies, online platforms and the general public are needed to develop and implement policies, regulations and approaches that are more effective in dealing with the catfish phenomenon and provide protection for victims.

CONCLUSION

Online fraud using fake identities, commonly known as catfishing, is an act in which a person creates a fake profile or poses as someone else online with the aim of deceiving or manipulating other people. Catfish perpetrators' motivations can range from seeking attention to creating a fake romantic relationship to seeking financial gain.

Law enforcement against online fraud using fake identities involves efforts to improve order and legal certainty in society. In the context of criminal law, online fraud can be categorized as an unlawful act that can be subject to criminal sanctions.

Factors hindering law enforcement against online fraud using fake identities include: Difficulty in tracing fake identities used by catfish perpetrators. Use of anonymous accounts or with limited information that is difficult to track digitally. Constraints arising from territorial boundaries and jurisdictions that cut across different countries. Difficulties in cooperation between countries in law enforcement and exchange of information related to online fraud. Shame, reluctance to report, stigma, and feelings of shame experienced by victims of online catfish scams. Relevant legal limitations and regulatory incompatibility with the rapid development of digital technology.

In dealing with online fraud using fake identities, efforts are needed that involve collaboration between authorities, institutions and the public to raise awareness about the risks of online fraud, protect victims, and develop an adequate legal framework to deal with these crimes.

To avoid online scams the authors suggest several things namely Keep personal information confidential and avoid sharing it carelessly Beware of suspicious links and emails Verify sender identity before providing personal information Update your software and security regularly Use strong and different passwords to every online account, Be careful when shopping online and check return policies, Check billing and account statements regularly for suspicious activity, Increase your knowledge about online scams, Share information and experiences with others and Report fraud to authorities.

REFERENCE

Abdulkadir, M. (2006). *Etika profesi hukum*. PT. Citra Aditya Bakti.

Asriyani, A., & Dwiyanti, A. (2022). Efektivitas kepolisian dalam melakukan penyelidikan tindak pidana penipuan online melalui media elektronik internet. *Jurnal Litigasi Amsir*, 140–145.

Asshidiqie, J. (2006). Hukum tata negara dan pilar-pilar demokrasi, serpihan pemikiran hukum. *Media Dan HAM. Jakarta: Konstitusi Press Dan PT. Syaamil Cipta Media*.

Efendi, S. (2021). Sanksi kejahatan penipuan dengan identitas palsu dalam KUHP Indonesia dan fiqh jinayah. *Al-Ahkam: Jurnal Syariah Dan Peradilan Islam, 1*(2).

Hutasoit, K. (2018). Tinjauan yuridis terhadap tindak pidana penipuan secara online dalam perspektif hukum pidana di Indonesia (Studi putusan Pengadilan Negeri Banda Aceh No.22/Pid.B/2017/PN-BNA). *Jurnal Hukum Fakultas Hukum Universitas Sumatera Utara*.

Jannah, A. M. (2020). Penegakan hukum pidana terhadap tindak pidana penipuan bisnis online di Polda Metro Jaya menurut hukum positif dan hukum Islam. In *Repository.Uinjkt.Ac.Id*.

Maskun, S. H. (2017). *Aspek Hukum Penipuan Berbasis Internet* (Vol. 1). Keni Media.

Muladi. (2009). *Hak asasi manusia*. PT Refika Aditama.

Puspitasari, I. (2018). Pertanggungjawaban pidana pelaku tindak pidana penipuan online dalam hukum positif di Indonesia. *Hukum Dan Masyarakat Madani*, *8*(1). https://doi.org/10.26623/humani.v8i1.908

Putri, C. E., & Hamzah, R. E. (2022). Analisis fenomena penipuas identitas diri (Catfishing) pada literasi digital pengguna media sosial. *KOMUNIKATA57*, *3*(2).

Rahmanto, T. Y. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1). https://doi.org/10.30641/dejure.2019.v19.31-52

Rawat, R., Mahor, V., Chirgaiya, S., & Rathore, A. S. (2021). Applications of social network analysis to managing the investigation of suspicious activities in social media platforms. In *Advances in Cybersecurity Management*. https://doi.org/10.1007/978-3-030-71381-2_15

Sudarto, A. H. (1995). *Islam berbagai perspektif (Islam from various perspectives)*. LPMII.

Wijayanto, A. R. (2021). Love scams and its legal protection for victims. *Law Research Review Quarterly*, *7*(2), 211–224.

Zahra, R. A., Gunawan, R. S. P., & Fauzianti, N. A. (2022). Catfishing dan implikasinya terhadap romance scam oleh Simon Leviev dalam dokumenter Netflix 'Tinder Swindler' menurut perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana. *Padjadjaran Law Review*, *10*(1).