CONTENT: JOURNAL OF COMMUNICATION STUDIES

Journal homepage: https://cjcs.usu.ac.id

Online Identity and Cybercrime: Unmasking Threats in the Digital Age

Rahma Hayati Harahap*[1], Muhammad Adfhol Zikri[1]

[1]*Sociology, Universitas Sumatera Utara, Medan, 20155, Indonesia*

*Corresponding Author: rahmashiny12@usu.ac.id

ARTICLE INFO

Article history:

Received 29 April 2024

Revised 26 May 2025

Accepted 28 May 2025

Available online 31 May 2025

E-ISSN: 3032-4440

How to cite:

Harahap, R. H. & Zikri, M. A. (2025). Online Identity and Cybercrime: Unmasking Threats in the Digital Age. *CONTENT: Journal of Communication Studies*, 3(1), 11-16. https://doi.org/10.32734/cjcs.v3i01.16297

ABSTRACT

Currently, the development of technology is increasingly massive, the development of technology has presently entered generation 5.0 and is heading towards 6.0. The development of technology at this time cannot be stopped due to the human will to develop continuously. Internet technology users in Indonesia reach more than 221 million people, and 139 million people use social media. This research aims to describe the negative impact of using internet technology in cyberspace, especially on social media, namely online crime or cybercrime involving personal online identity data that is misused. This research uses a qualitative approach that uses a literature study as its data collection. Which is sourced from existing journals, news, and blogs. And from this research we can see that crime in cyberspace itself has become increasingly massive, especially crimes that target a person's personal data or crimes by targeting a person's online identity such as catfishing, doxing, cyberbullying, and online-based fraud. This research can be an illustration that there are many crimes that occur in cyberspace and this research is expected to be a lesson for all parties to be more vigilant.

Keyword: *Cybercrime, Cyberspace, Online Identity*

ABSTRAK

Saat ini perkembangan teknologi semakin masif, perkembangan teknologi saat ini sudah memasuki generasi 5.0 dan sedang menuju ke arah 6.0. Perkembangan teknologi saat ini tidak dapat dihentikan karena kehendak manusia untuk terus berkembang. Pengguna teknologi internet di Indonesia mencapai lebih dari 221 juta orang dan 139 juta orang menggunakan media sosial. Penelitian ini ingin mendeskripsikan dampak negatif penggunaan teknologi internet di dunia maya, khususnya pada media sosial, yaitu kejahatan online atau cybercrime yang melibatkan data identitas online pribadi yang disalahgunakan. Penelitian ini menggunakan pendekatan kualitatif yang menggunakan studi pustaka sebagai pengumpulan datanya. Yang bersumber dari jurnal, berita, dan blog yang ada. Dan dari penelitian ini kita dapat melihat bahwa kejahatan di dunia maya sendiri menjadi semakin masif, terutama kejahatan yang menargetkan data pribadi seseorang atau kejahatan dengan menargetkan identitas online seseorang seperti catfishing, doxing, cyberbullying, dan penipuan berbasis online. Penelitian ini dapat menjadi gambaran bahwa banyak kejahatan yang terjadi di dunia maya dan penelitian ini diharapkan dapat menjadi pelajaran bagi semua pihak untuk lebih waspada.

Kata Kunci: Dunia Maya, Identitas Online, Kejahatan Dunia Maya

1. Introduction

Technology has developed rapidly, especially in information technology, and technology has increased massively. Currently, the spread of information and communication technology is very difficult to follow, because information is spread not only from one point, but from various points around the world. At this time, the development of technology has entered the development of 5.0; in this case, it has developed very rapidly and will continue towards the development of 6.0 (Fitriani & Pakpahan, 2020).

In line with the development of existing technology, especially information and communication technology, the number of users is increasing. It can be said that users of information technology are essentially internet users. According to data from the Indonesian Internet Service Providers Association (APJII) in 2024, the number of internet users in Indonesia reached 221,563,479 people, representing 79.5 percent of the country's 2023 population of 278,696,200. And from the number of internet users in Indonesia, social media users in the country reached over 139 million in January 2024 (APJII, 2024).

In the use of the internet, the container can be called *Cyberspace.* Cyberspace is a place or container used in the development of technology in the world. In other words, cyberspace is a place for the development of technology, information, communication, online interaction, and various activities that are online. Cyberspace includes social media. Social media itself, according to Van Dijk, is a platform that has the benefit of accommodating users in developing their creativity, and social media, according to Van Dijk, also has a function as a relationship strengthener in online social ties (Saputri, 2020).

Currently, the virtual world is widely used to carry out various activities, such as the use of social media intended for branding ourselves, or other activities. Online identity itself is a form of self-description in virtual media. According to Jacob Van Kokswijk, what is displayed in cyberspace is a picture of a person's self, a person can change what they want to be like in cyberspace, and according to Jacob himself the level of trust displayed in cyberspace is very low because social media users can change according to what they want.

The online identity built by a person on social media certainly shows positive things. By building a positive online identity, a person can be recognized for positive things. But at this time, many crimes have sprung up in cyberspace, commonly referred to as Cybercrime. Cybercrime itself is a crime committed in virtual media. Cybercrime itself arises because of a sense of wanting to get personal gain without paying attention to the losses suffered by others. Based on data from AwanPintar.id, Indonesia experienced a total of 2,499,486,085 cyberattacks as of early 2024. Therefore, this research will reveal various online crimes or cybercrime in the form of crimes utilizing other people's online identities without the user's permission (Fitriani & Pakpahan, 2020). The online identity built by a person on social media certainly shows positive things. By building a positive online identity, a person can be recognized for positive things. But at this time many crimes have sprung up in cyberspace, commonly referred to as Cybercrime. Cybercrime itself is a crime committed in virtual media. Cybercrime itself arises because of a sense of wanting to get personal gain without paying attention to the losses suffered by others.

Online Identity

Online identity is an identity that is built in cyberspace. In depicting one's self-image in cyberspace, it does not have to be the same as the identity that exists in the real world. Many people use their online identity as their main identity, because online identity is an identity that is easy to form and manipulate the truth (Aprilia, 2024). Online identity itself becomes a second identity of a person, and in this case, the identity in the real world remains the first identity. Many reasons make someone build their online identity in cyberspace. At this time, a person's life is more in the virtual world than in the real world. And in life in cyberspace, a person can create his own identity in the media with what he wants. There are several reasons that individuals use in building their online identity in cyberspace, the first being a form of self-expression, personal branding, connection and networking, and educational and learning needs (Saputri, 2020).

Social Media

Social media is an application based on the internet and on the ideological basis of technological development. According to Liedfray, dkk (2022), Social media is an online media, where users can easily participate, share, and create content including social networks, blogs, forums and virtual worlds. In other words, social media as a medium that can disseminate information and can form public opinion in it. According to Michael Haenlin and Andreas Kaplan, there are 6 types of social media platforms, namely (1) Blogs and Microblogs, which are social media applications that spread short and large blogs. (2) Social Networking Communities, serves as a link between one individual and another. (3) Collaborative Projects, social media as a collaborative medium that is intended for all. (4) Content Communities, social media can accommodate various communities in it. (5) Virtual Social Worlds, social media connects a person with another person in the world without barriers. (6) Virtual Game world, in this case social media is also used to play games (Setiadi, 2016).

The characteristics of social media include: (1) Network, in this case connecting one computer with another computer. (2) Information, massive information dissemination. (3) Archive, functions as a storage of information. (4) Social Simulation, in social media, interacting and doing virtual activities. (5) Interaction, connecting with other social media users. (6) Content, which functions to influence listeners in social media (Setiadi, 2016).

Cybercrime

Cybercrime is a crime committed by individuals or groups in cyberspace who use technology as a way to commit their crimes. Andi Hamzah revealed that cybercrime is a crime committed using a computer, which means that using a computer to commit a crime is illegal (Fitriani & Pakpahan, 2020). Cybercrime itself has its characteristics according to Freddy Haris (Mansur & Gultom, 2009), damaging computer operations, preventing and inhibiting connections or access to computers, Unauthorized access, Unauthorized alteration or destruction of data. And Online Crime has various other types of crimes, including Identity crime. Identity crimes are crimes committed by disseminating a person's identity without permission and for personal purposes. There are several online identity crimes, namely, catfishing, doxing, cyberbullying, online fraud, and several other online identity crimes (Marita, 2019)

Cyberspace

The word cyberspace itself was first popularized by William Gibson in a novel book made with titled Burning Chrome in 1982. Cyberspace itself, according to Dysson, is a bioelectronic ecosystem in various places that has a network of telephones, fiber optics, electromagnetic waves, and coaxial cables (Arifin, 2021). The characteristics of cyberspace itself are, being in cyberspace or operating through virtual media, cyberspace is always changing rapidly along with technological developments, cyberspace has no restrictions in it such as connecting one person to another, in cyberspace a person can do what he likes such as manipulating the identity used in cyberspace, and various information in cyberspace can be owned by everyone in the sense that the information is public.

2. Method

The method used in this research is qualitative research, qualitative research is a study that uses an approach to examine social or human phenomena that can describe the entire object of research in detail and can be used as a reference in subsequent research. As according to other experts Denzin and Lincoln, said that qualitative research is research aimed at life to find out about phenomena that occur in natural life (Adlini et al., 2022). Data collection is done through literature studies. Literature study is a study that focuses on reviewing existing literature materials to be developed in a study, and this case, by looking for theories that are in line with the research. The literature study has 4 stages in it, including reading or collecting research materials, organizing time, and preparing various supporting tools for research.

3. Results and Discussion

Various cybercrimes occur today, especially crimes in the form of misusing or stealing someone's online identity for personal gain. The following are forms of identity crime in cyberspace.

3.1. Catfishing

In the view of Rachmah Ida M Comms, Professor of FISIP Universitas Airlangga, catfishing is a behaviour that hides its identity and uses the identity of others to trick victims. According to Rachmah, catfishing can be divided into 2 types, the first is unintentional, which is when someone uses someone else's identity because he feels insecure using his own identity, and the second is intentional, in this case catfishing is done intentionally, namely to trick someone and does not intend to show his identity in public (Nariswari, 2022). One of the cases that made a splash in Indonesia is Catfishing carried out by one of the Twitter social media accounts, namely Tinder Swindler. The perpetrator uses the identity of another person to trick the targeted victims. Tinder Swindler uses the identity of another person, namely James Sinaga, who works as a businessman who owns various factories and electronic stores.

One of the eccentric things displayed to seduce his victims is by flexing or displaying luxury on social media. With this flexing behaviour, Tinder itself tries to convince its victims to transfer money to it with the intention that it is in urgent need of money as soon as possible. After transferring some money, the perpetrator disappeared and could not be contacted. Of course, this causes losses for the catfishing victim. Several characteristics are identical to catfishing perpetrators, namely: (1) It is too easy to say they like the victim; catfishing perpetrators often use words of seduction to lure their victims and immediately express their feelings for the victim. (2) Usually, catfishing perpetrators do not want to meet the victim face to face, and catfishing perpetrators use the identity of other established people in seducing their victims. (3) The portrayal of catfishing actors on social media usually displays things that smell of luxury and with perfect physical and material conditions, the purpose of displaying such things is to convince victims that catfishing actors are truly perfect people. (4) Catfishes use other people's identities and are usually very difficult to identify on the internet. (5) And what is most synonymous with catfishing is that they will try to ask the victim for money on the grounds of urgency, and when the transfer has been made, they will disappear like air (Nariswari, 2022). From the examples of catfishing cases above, it can be prevented so that catfishing does not target us by paying attention to personal data on social media, social media privacy is maintained or checked regularly, being aware of new people known on social media, not accepting friendships with unknown people.

Doxing

Doxing is the activity of spreading personal information to a large audience or public. Doxing itself according to Honan comes from dropping documents or dropping boxes, meaning that doxing is a revenge activity carried out for hackers who spread individual identities to a large audience or public. According to David M Douglas himself divides doxing into several types, namely: (1) Targeting doxing, this doxing is a form of disseminating information carried out by perpetrators with targets that have been considered from the start. (2) Delegitimization Doxing, is an act of sharing information with the public that has the bad purpose of destroying the character, credibility, and reputation that has been built by someone and can ultimately destroy someone's career. (3) Deanonymizing Doxing, this doxing is a target in the form of random or random people (Putri, 2023).

One of the doxing cases in Indonesia itself was in 2022, at that time there was a demonstration in front of the DPR-RI building carried out by the All-Indonesian Executive Board (BEM-SI) and at the same time Ade Armando, a lecturer at the University of Indonesia, was in the same place and the end, Ade Armando was persecuted by students who caused Ade Armando's battered body. The police also acted quickly by securing several perpetrators of the persecution of Ade Armando. At the same time on social media, photos of the alleged perpetrators of the persecution of Ade Armando and the identity of the alleged perpetrators were spread. This is one of the violations of existing doxing behaviour, where social media users spread photos and personal data of suspected actors, but not necessarily the truth. According to Miftah Fadli as a researcher at the Institute for Community Studies and Advocacy said that doxing on social media cannot be justified. According to Miftah, the steps should provide the data to the police. The perpetrators of doxing can be charged with Article 28, paragraph 2 of the ITE Law, which can cause the perpetrators of doxing to be sentenced to 6 years and a fine of 1 billion (Taher, 2022).

Cyberbullying

Cyberbullying is bullying behaviour carried out in cyberspace. In AR Rasyid's view, cyberbullying is a form of crime in the form of bullying others in cyberspace, in the form of ridicule, saying harsh words to people (Febrianti & Setiyowati, 2023). In this case, cyberbullying does not only occur on social media, but can also occur in online games. Cyberbullying in the gaming world is divided into 3 parts, namely: (1) Harassment, which is an activity that attacks an individual in chat by saying inappropriate words and intending to harass the victim. (2) Flaming, in itself, emphasizes the use of vulgar words. (3) Grieving, an activity that seeks to provoke the opponent to do annoying activities in the game.

There are many examples of cyberbullying in online games. This time, I tried to explain cyberbullying in the Mobile Legends game world. Mobile Legends is currently a mobile game that can be played by various groups, both young and old. This mobile legend game itself has been around since 2016, and until now. And the game uses a 5 vs 5 system that is randomly selected. The mobile legends game itself consists of various features, one of which is the chat feature and voice feature. Usually, the chat feature is used to provide information to teammates. But lately many mobile legends players have complained that there has been a lot of bullying against players or mobile legends players. Many harsh words and intimidation are involved it such as using indecent words or using harsh words that cause unhealthy mobile legends games. And currently, mobile legends often bullying occurs to the perpetrator or the mobile legend player (Febrianti & Setiyowati, 2023). Many impacts are caused by cyberbullying behaviour, including mental damage experienced by online game players, which can cause someone to be depressed and even lead to suicide, and negative impacts on the surrounding community with bullying.

Online Scam

Online fraud is a fraudulent activity carried out through internet services and software to take as much profit as possible from victims, and can cause loss of identity because it has been stolen to carry out other online fraud activities. The criminal offense of online fraud is Article 378 of the Criminal Code. But the article does not emphasize online-based fraud (Prasetyo, 2014). And in recent times, there has been a phenomenon of online fraud based on wedding invitations. The spread of wedding invitations on WhatsApp social media, a mode to send a document that says wedding invitation, but the person who sent the wedding invitation is an unknown person. If we open the document sent, the data on our cell phone will be easily accessed by the fraudster, but if we do not open the document, our data is safe from hacking.

Fraud using wedding invitations has claimed many victims, many victims who open the wedding invitation document and end up with their data being hacked, and important information on their cell phone will be easily accessed by the perpetrator. Especially to access the victim's account number to steal the money from the victim's ATM (Nurdiyyani et al., 2024). With the many scams in the form of spreading wedding invitations from unknown people, we, as social media users, are more careful in maintaining our own identity amid the rise of similar fraud cases. Some things that can be done to prevent similar fraud from recurring are by making laws or laws that discuss online fraud and along with criminal sanctions, the second can be done by increasing public sensitivity to online fraud cases, there are many cases, especially parents who are not literate on the internet and are very easy to trick, the third can be done by taking action to socialize to the public that online fraud is currently rife and the public can maintain their privacy better in cyberspace.

4. Conclusion

Based on the data presented above, many crimes exist in cyberspace, including crimes related to identity. It cannot be denied that, along with the development of technology today, a person or individual can carry out an activity that smells of crime. Crimes in cyberspace are easier to commit, as only a computer and being at home can commit crimes in cyberspace, including crimes that target a person's online identity. There are many forms of identity crime, such as catfishing, doxing, cyberbullying, and online fraud. Catfishing itself emphasizes how an individual commits a crime in the form of becoming someone else to outwit the victim and reap benefits for himself. And it is not only catfishing that can cause harm to other internet users, but doxing activities carried out by an individual can cause great harm; in this case, the perpetrators spread private information owned by individuals to damage their reputation, labor, and defame their name in the public space. Doxing activities occur due to an individual's dislike for the victim, and many other things cause doxing behavior.

Cyberbullying committed against people in cyberspace can cause various mental problems or fear in them, and at this time cyberbullying is mostly done in online games, especially mobile legends. The beginning of cyberbullying behavior is due to the innate toxicity of a game user and in its release can be directed to other game users by saying harsh words, and what is worse, can bring Tribe, Race, and Religion which is a sensitive thing in Indonesia itself. And the last is online fraud, there are many cases of online fraud that exist, as I took the example above of the spread of fictitious wedding invitations, where the wedding invitation letter is not true and is only a forum for fraudsters to trick victims. Many cases of fictitious marriages have their data stolen, and most importantly, to take the victim's ATM information data to drain the victim's savings. This is a loss for social media user pigs who experience identity theft crimes. And in increasing awareness of online identity theft cases, we can do various things to prevent it such as checking our social media security so that it does not spread, checking our social media regularly and if it has happened and happened to us, do not hesitate to report the action to the authorities.

References

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*, *6*(1), 974–980. https://doi.org/10.33487/edumaspul.v6i1.3394

APJII. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. APJII.

Aprilia, T. (2024). *Apa itu Identitas Digital? Komponen dan Cara Mengelolanya*. Mekarisign.Com.

Arifin, Z. (2021). *Keamanan dan Ancaman pada Cyberspace* (1st ed.).

Febrianti, R. W., & Setiyowati, E. (2023). Dampak Toxic Game Terhadap Cyber Bullying. *JIK JURNAL ILMU KESEHATAN*, *7*(1), 70. https://doi.org/10.33757/jik.v7i1.652

Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di dunia maya atau cyberspace. *Jurnal Cakrawala*, *20*.

Liedfray, T., Waani, F. J., & Lasut, J. J. (2022). Peran Media Sosial Dalam Mempererat Interaksi Antar Keluarga Di Desa Esandom Kecamatan Tombatu Timur Kabupaten Minahasa Tenggara. *JURNAL ILMIAH SOCIETY*, *2*(1).

Marita, L. S. (2015). Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia. *Cakrawala: Jurnal Humaniora Universitas Bina Sarana Informatika*, *15*(2). https://doi.org/https://doi.org/10.31294/jc.v15i2.4901

Mansur, Arif, D. M., & Gultom, E. (2009). *Cyber law : aspek hukum teknologi informasi*. Refika Aditama.

Nariswari, S. L. (2022). *Tinder Swindler Indonesia Viral, Awas Jebakan Catfishing*. Parapuan.Com.

Newsunair. (2022). *Mengenal Catfishing di Media Sosial dan Cara Menghindarinya*. News.Unair.Ac.Id.

Nurdiyyani, Mappaselleng, A. K. K., & Hardani, A. H. Y. (2024). Pertanggungjawaban Hukum Terhadap Pelaku Tindak Pidana Penipuan Online dengan Modus Undangan Pernikahan. *LEX SUPREMA: Jurnal Hukum Fakultas Hukum Universitas Balikpapan*, *6*(1).

Prasetyo, R. D. (2014). *Pertanggungjawaban Pidana Pelaku Tindak Pidana dalam Hukum Pidana Positif di Indonesia*. Universitas Brawijaya.

Putri, C. N. (2023). *Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial*. Universitas Lampung.

Saputri, V. S. (2020). *Kontruksi Identitas Diri Virtual Melalui Instagram (Studi pada Mahasiswa Jurusan Ilmu Komunikasi Angkatan 15 Universitas Muhammadiyah Surakarta)*. Universitas Muhammadiyah Surakarta.

Setiadi, A. (2016). Pemanfaatan Media Sosial untuk Efektifitas Komunikasi. *Cakrawala: Jurnal Humaniora Universitas Bina Sarana Informatika*, *16*(2). https://doi.org/https://doi.org/10.31294/jc.v16i2.1283

Taher, A. P. (2022). *Kasus Ade Armando & Doxing Data Terduga Pelaku Tak Bisa Ditolerir*. Tirto.Id.

Team, D. (2022). *Apa itu Penipuan Online dan Bagaimana Menghindarinya?* DawaWeb.Com.

Watie, E. D. S. (2016). Komunikasi dan Media Sosial (Communications and Social Media). *Jurnal The Messenger*, *3*(2), 69. https://doi.org/10.26623/themessenger.v3i2.270