



Uploading Private Chat Screenshots on Social Media: How the Law Respond it?

Ni Nyoman Juwita Arsawati¹, Dewi Bunga², Putu Eva Ditayani Antari³, I
Made Wahyu Chandra Satriana⁴

¹Faculty of Law Universitas Pendidikan Nasional, E-mail: juwitaarsawati@undiknas.ac.id

²Faculty of Dharma Duta Universitas Hindu Negeri I Gusti Bagus Sugriwa Denpasar,

E-mail: dewibunga@uhnsugriwa.ac.id

³Faculty of Law Universitas Pendidikan Nasional, E-mail: evaditayaniantari@undiknas.ac.id

⁴Faculty of Law Universitas Dwijendra, E-mail: wahana.chandra@gmail.com

Article Info

Received: 3rd March 2023

Accepted: 23rd July 2023

Published: 29th July 2023

Keywords:

Privacy; Private chat;
Screenshots; Upload

Corresponding Author:

Ni Nyoman Juwita Arsawati,

E-mail :

juwitaarsawati@undiknas.ac.id

DOI:

10.24843/JMHU.2023.v12.i0

2.p05

Abstract

Personal chat is a personal communication conducted in two directions and concerns privacy in communication. The latest behavior of social media users shows considerable virtual openness. The social media users upload screenshots of their personal chat to their social media accounts and even send them to gossip accounts in social media. In this study, there are three issues discussed namely privacy rights in personal chats uploaded on social media, potential crime of uploading personal chats, and state legal responses to the spread of personal chat screenshot on social media. The right to privacy is basically giving the freedom to publish or not publish personal chat on social media. There are at least two privacies protected in personal chat namely the sender and recipient of the message, but they are not limited to people or things discussed in the personal chat. Uploading personal chat screenshots on social media has the potential to cause doxing (theft of personal data) and cyberbullying. Countries respond to these conditions with legal provisions in their respective countries. The act of spreading personal chat screenshot on social media has a legal consequence of a lawsuit for compensation for violations of personal data, criminal sanctions for defamation and cyberbullying.

I. Introduction

The internet has provided space for humans to evolve quickly. Many human works and activities are uploaded in cyberspace.¹ The rapid advancement of information technology with internet speed poses a difficulty in the acquisition, use, control, or transfer of personal data across borders.² Applications with social media platforms provide a vast space for users may engage in many types of communication, such as message services, such as personal chat, which also includes social networking features, all inside the same

¹ Karuppannan Jaishankar, "Cyber Criminology as An Academic Discipline: History, Contribution and Impact," *International Journal of Cyber Criminology* 12, no. 1 (2018): 1-8. <https://doi.org/10.5281/zenodo.1467308>

² Camille Blackburn, "New Technology, Personal Data Protection and Implications for Financial Services Regulation," *JASSA: The Journal of the Securities Institute of Australia* 4, (2015): 59-65.

application. Personal chat is a private conversation conducted by the sender of the message and the recipient of the message in the delivery of the message in the application used.

Personal chat is basically a form of communication that involves one's privacy. Edmon Makarim summarizes three aspects of privacy, namely privacy of a person, data privacy about a person and privacy of a person's communication. In certain situations, the right to privacy may also extend to online communication. Monitoring and disclosing the contents of electronic communications by other people, the sender or the person sent can be a violation of someone's privacy.³ Later, a new phenomenon emerges on social media in which the sender or recipient or even both of them deliberately take screenshots of their conversations and upload them to social media, even by including the hashtag.

The behavior of internet users shows that there is almost no boundary between public and private space. Recent messaging and social media applications are used to upload personal chat screenshots. Screenshots used in information technology systems include the natural domain for measurement. Nonetheless, screenshots used by humans are full of privacy material.⁴ Social media users take screenshots of their conversations with other people for various purposes. Some people consider what is said in personal chat as a funny thing to upload, showing a good personal relationship, even intimacy with a partner to the public. Online stores use personal chat screenshots between online store admins and customers as a marketing strategy to make prospective buyers believe that the products offered are the good quality products. On the other hand, there are times when uploading personal chat screenshots are used to submit complaints, express infidelity, and even bring down one's reputation.

Uploading of personal chat screenshots on social media illustrates virtual self-disclosure. A person opening himself is to achieve several goals, including: expression, relationship development, self-clarification, social validation, and social control. In addition, self-disclosure is also carried out strategically.⁵ Once an information or electronic document is uploaded to social media, the privacy nature of the information or electronic document will be lost due to its uncontrolled distribution. Laws in Indonesia and also in various countries do not specifically regulate the prohibition to open virtually to the public, but rather regulates the protection of personal data and privacy. Under certain conditions, the behavior of using personal chat screenshots is not a problem, but in other conditions, these actions can violate the privacy of others, both among the sender or recipient of the message and to the things discussed in the personal chat. Personal chat uploads on social media open up opportunities to become a crime or used as a way to commit a crime.

This research will discuss privacy rights in personal chats uploaded on social media. Next will be discussed about which actions are allowed, which actions tend to cause crime and

³ Edmon Makarim, (2005). *Pengantar Hukum Telematika Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2006).

⁴ Joseph Cooley, and Sean Smith, "Privacy-preserving Screen Capture: Towards Closing the Loop for Health IT Usability," *Journal of Biomedical Informatics* 46, no. 4 (2013): 721-733. <https://doi.org/10.1016/j.jbi.2013.05.007>

⁵ Maya Puji Lestari, "Hubungan Romantis di Media Sosial (Resepsi Pengguna terhadap Keterbukaan Hubungan Romantis yang Diunggah Selebgram di Instagram)," *Komuniti: Jurnal Komunikasi dan Teknologi Informasi* 11, no. 1 (2019): 28-44. <https://doi.org/10.23917/komuniti.v10i3.5944>

which actions constitute a crime. In the final section, we will analyze how the state's legal responses to the spread of personal chat screenshot on social media. This study describes conditions in which uploading a personal chat is a violation of the law, and which is not a violation of the law.

2. Research Method

This study is a normative legal investigation that examines the void of norms regarding concerning online conversations as a matter of privacy. Legal resources are derived from primary legal sources and secondary legal sources. The statutory instruments used are Criminal Code, the Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the Law of Information and Electronic Transactions 2008), The Law of the Republic of Indonesia No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the Law of Information and Electronic Transactions 2016) and the Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the Law of Personal Data Protection). Secondary legal documents include academic journals, books, and electronic articles. Legal documents are entered via a library query. The analysis was carried out qualitatively.

3. Result and Discussion

3.1 Privacy Rights in Personal Chats Uploaded on Social Media

The term "social media" refers to a range of Web 2.0-based online applications that encourage the development and dissemination of user-generated content and enable participation, communication, and presentation in a variety of formats, including blogs, social networks, forums, wikis, etc.⁶ The advent of Web 2.0 technology in 2003, enhancing pre-existing web-based services. In which the advantages of this internet platform service is that it is easy to use and be adopted by users. The popularity of social media like Facebook and Youtube, is one indication of the development of this Web 2.0 technology.⁷ The use of those social media is quite popular in Indonesia beside Instagram, Whatsapp, and Line.

In 2020, Indonesia is expected to have 175.4 million internet users, according to the most recent We Are Social research. It is also known in this report that 338.2 million Indonesians are currently using mobile phones. In addition, there are 160 million active users of social media.⁸ The presence of social media becomes its own challenge for protecting one's privacy in the midst of virtual self-actualization behavior. Subject to ever-changing privacy policies, users are required to negotiate complex technological architectures to determine the level of privacy on social media. At the same time, public law attempts to

⁶ A. K. Sherlyanita, and N. A. Rakhmawati, "Pengaruh dan Pola Aktivitas Penggunaan Internet serta Media Sosial pada Siswa SMPN 52 Surabaya," *Journal of Information Systems Engineering and Business Intelligence* 2, no. 1 (2016): 17-22.

⁷ Mardiana Purwaningsih, "Standar Etika bagi Perusahaan yang Menggunakan Media Sosial sebagai Enterprise's Official Presence," *Jurnal Sistem dan Informatika* 11, no. 1 (2016).

⁸ A. Y. Haryanto, "Riset: Ada 175,2 Juta Pengguna Internet di Indonesia," (2020). Retrieved from <https://inet.detik.com/cyberlife/d-4907674/riset-ada-1752-juta-pengguna-internet-di-indonesia>

regulate these relationships under conditions in which the legal concept of “private life” takes on different dimensions in social life. The intersection of these two legal forms probably lies in the daily life of users/citizens.⁹

The conception of the Internet connectivity feature allows for interactive two-manner communicate and may be woven into humans's lives extra in detail than different media inclusive of connecting humans with locations and those with humans. Thus, this will pose an information privacy threat. This speedy development approach that records received and processed may be effectively and affordably collected, saved and exchanged, even the records that can be taken into consideration touchy with the aid of using the person concerned.¹⁰

The improvement and development of era increases a public recognition that there's a person's proper to revel in life. The proper to experience lifestyles is interpreted as a person's proper now no longer to be disturbed through his private lifestyles both through a person else, or through the state; therefore, the regulation have to understand and defend the proper to privacy.¹¹ The entitlement to confidentiality has evolved to incorporate the entitlement to safeguard individual information, as expressed in Clause 17 of the General Assembly Committee No. 16 on the Entitlements to Consideration for Family, Dwelling, and Communication and Preservation of Dignity and Esteem. Other international legal instruments that also discuss privacy rights include Guidelines for Data Protection and Transboundary Flow of Personal Data by the Organization for Economic Co-operation and Development (OECD) in 1980; the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) in 1981; and the General Assembly resolutions 45/95 and E/CN.4/1990/72 on Guidelines for the Regulation of Computer Files Containing Personal Data.

The basic right to privacy is the cornerstone upon which many other human rights are based. For autonomy and the preservation of human dignity, privacy is essential. In every part of the world, there are constitutional protections for privacy in over 130 nations. Currently, laws governing data protection and privacy exist in over 100 nations.¹² A fundamental human right is the preservation of one's privacy. Many nations now recognise data protection as a constitutional right or as "habeas data," which is the right of an individual to get security for his or her data and to receive justification when mistakes are discovered in that data. Portugal is an example of a nation that, under Article 35 of its Constitution, recognised data protection as a constitutional right. In addition, despite their historical and cultural distinctions, Armenia, the Philippines, Timor-Leste, Colombia, and Argentina are nations that have guaranteed the protection of private data in their constitutions. These nations also have distinct histories and cultures. The right to data privacy is also expressly acknowledged in the ASEAN Human Rights Declaration,

⁹ Katharine Sarikakis, and Lisa Winter, “Social Media Users’ Legal Consciousness About Privacy,” *Social Media+ Society* 3, no. 1 (2017): 1-14. <https://doi.org/10.1177/2056305117695325>

¹⁰ Helmy Prasetyo Yuwinanto, “Privasi Online dan Keamanan Data,” *Palimpsest* 31, no. 11 (2015).

¹¹ Sinta Dewi, *CyberLaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional* (Bandung: Widya Padjajaran, 2009).

¹² “What is Privacy?” accessed July 21, 2023, <https://privacyinternational.org/explainer/56/what-privacy>.

which ASEAN nations recently ratified.¹³ This privacy protection becomes very important considering the speed of development of information technology that affects the behavior patterns of social media users.

In Japan, this issue of protection of privacy has come to the attention of the authorities by making rules that contain protection for violations and the misuse of personal information from one source into a list and sell it to other parties.¹⁴ Danrivanto Budhijanto is on the view that freedom of information is a human right which must end because of the protection of personal rights. He further points out that the US liberal state also respects and upholds freedom of information, but it is not permitted to violate the personal rights of a person.¹⁵

Provisions regarding privacy protection in uploading personal chat screenshots are an attempt to balance the interests of the public with the interests of individuals. Regarding this matter, Fawn Ngo and K. Jaishanka state the following:

Along with finding a balance between personal freedom and public safety, the topic of online anonymity has to be researched. Because it is seen as the foundation of democracy and is linked to the idea of "freedom of expression," anonymity in cyberspace is an important subject - and concern - for the worldwide community. Online users may voice their opinions without worrying about retaliation or negative public opinion because to anonymity. Anonymity allows people to voice their thoughts in various regions of the world without being associated with any particular published viewpoints. However, anonymity in cyberspace also gives criminals the power to hurt the public while having little chance of being caught.¹⁶

Personal chat is actually a privacy among parties who communicate privately. The concept of privacy is a human rights concept. The right to decide whether and to what degree someone is prepared to open up to others is one way that privacy is commonly portrayed, as is the notion that privacy is the ability to be undisturbed.¹⁷ Privacy is not always interpreted as a decision to shut down, but also includes a decision to open up. There are several justifications for protecting privacy, as follows:

- a. A person must seal off a part of his personal life while forming interactions with others in order to keep his position at a specific level.
- b. He requires privacy because someone in his life needs time to be alone (solitude).

¹³ Sinta Dewi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia," *Yustisia Jurnal Hukum* 5, no. 1 (2016): 35-53. <https://doi.org/10.20961/yustisia.v5i1.8712>

¹⁴ Asril Sitompul, *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace)* (Bandung: Citra Aditya Bakti, 2004).

¹⁵ Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi Regulasi dan Konvergensi* (Bandung: Refika Aditama, 2010).

¹⁶ Fawn T. Ngo, and K. Jaishankar, "Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime," *International Journal of Cyber Criminology* 11, no. 1 (2017). <https://doi.org/10.5281/zenodo.495762>

¹⁷ E. Krisnawati, "Mempertanyakan Privasi di Era Selebgram: Masih Adakah?," *Jurnal Ilmu Komunikasi* 13, no. 2 (2016): 179-200.

- c. The right to privacy is independent and unrelated to anything else, yet it is forfeited if someone makes private information publicly available.
- d. A person's right to privacy extends to their ability to engage in domestic interactions, such as how they raise their families and form marriages. Later, Warren referred to this as their "right against the word."
- e. Because it has interrupted his personal life, the loss is difficult to quantify and is believed to be far higher than the physical loss; therefore, if a loss is incurred, the sufferer must be compensated.¹⁸

In accordance with Altman, privacy serves a variety of purposes, including regulating and controlling interpersonal interactions, which refers to the degree to which relationships when it's okay to be alone and when it's appropriate to be with people, are wanted; making plans and methods for social interaction, which may involve proximity or a greater degree of distance; as well as confirming the source's identity.¹⁹ Sharing private conversation screenshots has the potential to harm the relationships between individuals who are part of or mentioned in the chat, and may result in unforeseen outcomes.

The concept underlying privacy protection is not new, but the advances in modern technology have caused privacy problems to develop.²⁰ At least in the personal chat screenshot uploader, there are a number of people involved namely two people who are talking in a personal chat, and maybe also the person who is being talked about in their conversation. This condition can disturb someone's privacy, both one of the communicating parties and the party discussed in the chat. If both parties consent to uploading the chat content and the chat only pertains to the communicating parties, sharing personal chat screenshots online cannot be considered a violation of privacy. Uploading personal chat screenshots can be an invasion of privacy and even violations of the law also contain contempt contents. Uploading activity can aim to embarrass the sufferer. Accusations of victim blaming often stem from the presumption that the sufferer bore responsibility for the crime committed against them.²¹

3.2 Potential Crimes for Uploading Personal Chat

Technology is viewed as a tool for emancipation, a platform for democracy and participation, and a method of realising human autonomy. On the other hand, technology may also serve as a restriction on one's ability to exercise free will.²² The virtual world

¹⁸ Dewi, *loc. cit.*, 20.

¹⁹ I. T. Islamy et al., "Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi," *JTIP: Jurnal Teknologi Informasi dan Pendidikan* 11, no. 2 (2018): 21-28. <https://doi.org/10.24036/tip.v11i2.137>

²⁰ David J. Houghton, and Adam N. Joinson, "Privacy, Social Network Sites, and Social Relations," *Journal of Technology in Human Services* 28, no. 1-2 (2010): 74-94. <https://doi.org/10.1080/15228831003770775>

²¹ Tegan S. Starr, and Tiffany Lavis, "Perceptions of Revenge Pornography and Victim Blame," *International Journal of Cyber Criminology* 12, no. 2 (2018). <https://doi.org/10.5281/zenodo.3366179>

²² Agus Raharjo, Yusuf Saefudin, and Rini Fidiyani, "The Influence of Technology Determinism in Forming Criminal Act of Legislation," *E3S Web of Conferences* 73, no. 12011 (2018). <https://doi.org/10.1051/e3sconf/20187312011>

provides so much space for anyone to express freedom. Someone who uses social media does not need to include their real personal identity. Internet thieves are constantly looking for new ways to maintain their anonymity while navigating the internet terrain.²³ K. Jaishankar in Space transition theory states "Identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime."²⁴ Further research was conducted into the traits and criminal conduct of each group, revealing that several factors contribute to individuals engaging in cybercrime. One such factor is social conventions, where commonly accepted behaviors cause individuals to disregard the illegality of their actions.²⁵

Crime in cyberspace is always associated with behavior that violates social norms. Screenshot facilities available on mobile phones are used to take personal visuals and feature on social media. According to media-richness theory, screenshots are the best media to describe problems and problem solving in the context of computer software. ²⁶ Screenshot is considered as proof and used as proof or testimony. Unconsciously, the uploader who wants to prove his proposition actually commits acts that violate the law or at least have the tendency to break the law. The screenshot upload aims to make other users believe what the uploader wants to prove.

Social media is used by its users to express their personal relationships with others. It is common thing for users to show romantic conversations between him and his partner to prove to the public that he has an intimate relationship with someone. Social media is also enlivened with evidence of infidelity by uploading a couple's personal chat with other people. This post attracts the attention of the public which is seen from the many comments of social media users to make the judgment of the parties involved in the affair. This phenomenon illustrates the change in community behavior in which a relationship that had been a private matter turning into public consumption.

The right to privacy will be related to personal data The provisions regarding personal data in Indonesia are regulated for the first time in the Law of Personal Data Protection. Article 4 states that personal data consists of specific and general personal data. Specific personal data includes health data and information; biometric data; genetic data; crime records; child data; personal information data; and/or other data in accordance with the provisions of laws and regulations. General personal data includes full name; gender; nationality; religion; marital status; and/or personal data combined to identify a person.

²³ Noura Al-Suwaidi, Haitham Nobanee, and Fauzia Jabeen, "Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator," *International Journal of Cyber Criminology* 12, no. 2 (2018): 392-407. <https://doi.org/10.5281/zenodo.3365895>

²⁴ Karuppappan Jaishankar, "Establishing A Theory of Cyber Crimes," *International Journal of Cyber Criminology* 1, no. 2 (2007): 7-9.

²⁵ Nuttapol Assarut, Piyabutr Bunaramrueang, and Patanaporn Kowpatanakit, "Clustering Cyberspace Population and the Tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory," *International Journal of Cyber Criminology* 13, no. 1 (2019). <https://doi.org/10.5281/zenodo.3550473>

²⁶ Travis K. Huang, "Exploring the Antecedents of Screenshot-based Interactions in the Context of Advanced Computer Software Learning," *Computers & Education* 80, (2015): 95-107. <https://doi.org/10.1016/j.compedu.2014.08.011>

The distribution of personal chat screenshots under certain conditions is not only an invasion of privacy, but also causes victims to become victims of crime. Uploading of personal chat screenshots is a violation of personal data. In the terminology of criminology, the dissemination of personal data is termed doxing. Doxing is the deliberate search and disclosure of personal information about someone on the internet without his consent, and is often used to impose sentences.²⁷ Doxing occurs when someone finds someone else's personal information and publishes it for everyone to see. In personal chat, someone might tell about his personal information. Any type of private, sensitive, or intimate information is a potential target for doxing. Doxing differs from just exposing information since it involves the activity of looking for information about other people.²⁸

Dissemination of personal information or doxing is a violation of privacy. Doxing is when private or identifying information about a person or organisation is taken and made public.²⁹ At least, There are three different types of doxxing: deanonymizing doxxing, which involves disclosing personal information to reveal the identity of a previously anonymous person; targeting doxxing, which involves disclosing personal information to reveal particular details of a person's circumstances that are typically private, obscure, or obfuscated; and delegitimizing doxxing, which involves disclosing intimate personal information to undermine that person's credibility.³⁰ Doxing enables a variety of crowdsourced forms of harassment and intimidation, such as unauthorised pizza delivery and relentless rape and murder threats. Doxing is one of the ways perpetrators of crime commit cyberbullying.

Social media provides ample room for cyberbullying. Noma Nazish reported that Instagram became the most common social media platform for cyberbullying. Recent research shows that more than 40% of young people face online bullying in photo sharing applications. In the meantime, Facebook witnesses intimidation in 37% of reports, while Snapchat experiences it in 31%.³¹ Social networking site users engage in flaming, verbal abuse, and defamation of images or information shared on social media, which is facilitated through cyberbullying perpetrated by a collective of social media users. Uploading of personal chat on social media has the tendency to cause cyberbullying.

According to Charles E. Notar, Sharon Padgett, and Jessica Roden, cyberbullying is a new form of harassment that involves harassment through the use of technology, including social media websites (such as MySpace, Facebook, etc.), email, chat rooms, SMS and

²⁷ Qiqi Chen, Ko Ling Chan, and Anne Shann Yue Cheung, "Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong," *International Journal of Environmental Research and Public Health* 15, no. 12 (2018): 2665. <https://doi.org/10.3390/ijerph15122665>

²⁸ Mengtong Chen, Anne Shann Yue Cheung, and Ko Ling Chan, "Doxing: What Adolescents Look for and Their Intentions," *International Journal of Environmental Research and Public Health* 16, no. 2 (2019): 218. <https://doi.org/10.3390/ijerph16020218>

²⁹ Isabella Hansen, and Darren J Lim, "Doxing Democracy: Influencing Elections Via Cyber Voter Interference," *Contemporary Politics* 25, no. 2 (2019): 150-171. <https://doi.org/10.1080/13569775.2018.1493629>

³⁰ David M. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology* 18, no. 3 (2016): 199-210. <https://doi.org/10.1007/s10676-016-9406-0>

³¹ Noma Nazish, "Instagram is the Worst Social Media Platform for Cyber-bullying," *Blastingnews* (2018.) Retrieved from <https://uk.blastingnews.com/tech/2017/07/instagram-is-the-worst-social-media-platform-for-cyber-bullying-001864525.html>.

cellphone cameras, picture messages (including sexting), IM (instant messaging), and blogs.³² They emphasized the notion of cyberbullying as an act transformed from traditional bullying using information technology and social networking applications. Social media with the "tagging" facility can easily spread personal chat screenshots to several people, and can be redistributed by others who are friends in cyberspace.

The perpetrator uploads his personal chat on his social media. This action changes the private nature of communication into public. Through the features in the available social networking applications, internet users can easily pass the electronic information to other users, even this personal chat screenshot can be the content discussed in a gossip account. Participants stressed how the contemporary era and the usage of smartphones allowed for gossiping themes to be immediately available and allowed their chatter to be maintained current, with 71% of adults using smartphones to access the internet and dedicating over 2 hours a day to SNSs on a smartphone.³³ Posts in the gossip account easily get comments from cyberspace residents. Cyberbullying can only occur in the comments column, even users try to find the personal account of the person in the conversation and attack the account together. When the spread has occurred, of course it will be difficult to control the spread.

Personal chat screenshots are intact electronic documents and / or information. Normatively, electronic documents and / or information, including printouts, can become evidence that is recognized in statutory regulations. The Law of Information and Electronic Transactions 2008 characterizes electronic information and/or electronic records and/or hard copies as expansions of the instruments specified in Article 5 section (2). Valid evidence in line with Indonesian procedural law in force. However, in paragraph (3) it is stated that if using the Electronic System in compliance with the rules outlined in this Law, electronic information and/or documents are deemed legitimate. Additionally constrained by the truth statement concept are personal conversation snapshots used to demonstrate compliance.

The truth statement principle must fulfill several conditions. First, to be able to say a statement is a true value, it ought to be established via way of means of a courtroom docket choice that has everlasting felony force. Second, this reality have to be supported with the aid of using situations of public interes. Next, there exists a restriction on the truth principle. This restriction pertains to statements that have been deemed true by a court ruling with enduring legal effect, but are utilized to harm or bully another party. Therefore, when disclosing the truth, it must also serve the common good.³⁴ Even though what is expressed in a personal chat is true and can be used to prove something, if it is not used in the right place, and there is no element of public interest there, then the act will be unlawful. Actions intended to prove something should be done in court, not on social

³² Charles E. Notar, Sharon Padgett, and Jessica Roden, "Cyberbullying: A Review of the Literature," *Universal Journal of Educational Research* 1, no. 1 (2013): 1-9.

³³ Hannah Simpkin, *Exploring the Impact of Social Networking Sites (SNSs) on Modern Gossip from Female Perspectives* (Manchester Metropolitan University, Dissertations, 2017). <https://e-space.mmu.ac.uk/id/eprint/619201>

³⁴ Nanda Yoga Rohmana, "Prinsip-Prinsip Hukum tentang Tindak Pidana Penghinaan dan Pencemaran Nama Baik dalam Perpspektif Perlindungan Hak Asasi Manusia," *Yuridika* 32, no. 1 (2017): 105-133.

media. The truth statement principle aims to protect the legal interests of all parties so that there is no excessive public judgment.

The act of uploading a personal chat does not all become a legal problem, as long as it does not spread personal data, does not contain elements of bullying, insults, or has the tendency to cause harm and crime, and is used for purposes that do not violate the law, then the act is not a criminal offense. Some marketing strategies use uploaded personal chat screenshots that tell testimonials of the successful use of products sold by businesses.

3.3 The State's Legal Response to the Spread of Personal Chat Screenshot on Social Media

Uploading of personal chat screenshots is closely related to the privacy protection. Countries in the European Union have rules regarding privacy called the EU General Data Protection Regulation (EU GDPR). EU GDPR was created to strengthen the form of protection of the personal data of every European Union community. Article 4 paragraph (1) of the EU GDPR defines "personal data means any information relating to an identified or identifiable natural person ("data subject"); a person who can be identified, either directly or indirectly, in particular by reference to an identifier like a name, an identification number, location information, or an online identifier, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural, or social identity". Provisions in the GDPR ensure how consistent the application of regulations regarding privacy protection works in the European Union.

Indonesia already has a law governing electronic information, namely the the Law of Information and Electronic Transactions 2008 and its already amendment into the Law of Information and Electronic Transactions 2016 to as the Information and Electronic Transactions Law 2016). Protecting personal data is one facet of personal rights (privacy rights) in the use of information technology. Article 26 of the the Law of Information and Electronic Transactions 2016"Unless otherwise stipulated by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the approval of the person concerned." First, personal rights are the right to enjoy personal life and be free from all types of interruptions, according to the Elucidation of Article 26 of the Law of Information and Electronic Transactions 2016. Second, personal rights include the freedom to interact with people without being tracked. Third, the right to control who has access to information about one's personal life and data is a component of personal rights.

Communication made by a person is a personal right that contains an element of privacy. On the one hand, everyone has the right to publish his personal chat as long as it does not violate the rights of others. Conversely, an individual is entitled to prohibit the disclosure of their private conversation, particularly when shared online, enabling others to peruse the content. Violation of personal rights in law in Indonesia provides an opportunity for the injured party to file a claim for compensation. In Article 26 paragraph (2) the Law of Information and Electronic Transactions 2016 it is stated "Any person whose rights are violated as referred to in paragraph (1) may file a claim for damages incurred under this Law."

Mills (2017) says "Another evident consequence of these developments is that individuals are at much greater risk of committing defamation than existed under traditional media, which would generally exercise editorial control in which individuals are publishing material to a wide audience".³⁵ Uploading personal chat screenshots will be included as an insult in Indonesian law. In Indonesian law, insults are the domain of criminal law, not civil law. Public chat publications allow a person's dignity and good name to be attacked.

Degradation and/or defamation in cyberspace is considered a prohibition under Art. 27 sec. 3 of the Law of Information and Electronic Transactions 2008 which states "Everyone intentionally, and without the right to distribute and / or transmit and / or make access to Electronic Information and / or Electronic Documents which have content of insult and / or defamation. " In the Law of Information and Electronic Transactions 2008, lawmakers equalize insults with defamation, even though insults themselves constitute a group of acts, whereas one form of insults is defamation. Thus, defamation is part of the insults. According to the Attachment To Joint Decree Minister of Communication And Information Technology Of The Republic Of Indonesia, The Attorney General of The Republic of Indonesia, And The Head Of Police Of The Republic Of Indonesia Number 229 of 202, Number 154 of 2021, Number KB/2/VI/2021 Regarding Guidelines for Implementation of Certain Articles In Law Number 11 Of 2008 Concerning Electronic Information and Transactions as Amended by Law Number 19 of 2016 Regarding Amendments to Law Number 11 of 2008 Concerning Information And Transactions Electronic, not an offense related to insulting and/or defamatory content in Article 27 paragraph (3) of the Law of Information and Electronic Transactions, if the content or content that is transmitted, distributed, and/or made accessible is in the form of an assessment, opinion, evaluation result or a fact. In the event that the alleged fact is an act that is currently in legal process, the truth must be proven first before the Law Enforcement Officials process a complaint regarding the offense of insult and/or defamation of the Law of Information and Electronic Transactions.

The third paragraph of Article 27 in the Electronic Information and Transactions Law (2008) deals with cyber defamation and cyber denigration, specifically stating that these provisions do not establish fresh criminal law regulations. Instead, they serve to strengthen the implementation of contempt norms from the Criminal Code into a new law, given the unique and distinctive features of electronic or cyber activities. Therefore, the interpretation of norms contained in Article 27 paragraph (3) of the a quo the Law of Information and Electronic Transactions 2008 relating to insult and/or defamation and criminal legal standards found in Chapter XVI relating to insult included in Articles 310 and 311 of the Criminal Code cannot be separated. Therefore, Articles 310 and 311 of the Criminal Code must be considered in determining whether Article 27 paragraph (3) of the Law of Information and Electronic Transactions 2008 is valid. The Criminal Code's Articles 310 and 311 are genus delicts that call for the prosecution of a complaint (*klacht*).

The maximum punishment for defamation in Indonesia is nine months in prison or a fine of 4,500 rupiah. It is defined as an act committed by someone who maliciously attacks another person's honour or reputation by accusing them of something that is obviously

³⁵ Alex Mills, "Choice of Law in Defamation and the Regulation of Free Speech on Social Media: Nineteenth-Century Law Meets Twenty-first-century Problems," *In the Legal Challenges of Social Media*. (2017): 270-292. <https://doi.org/10.4337/9781785364518.00028>

known to the public. Defamation is punishable by a maximum of four thousand five hundred rupiah in fines or a maximum of one year and four months in jail if it is done using words or photos that are broadcast, shown, or posted in public. This provision is excluded as defamation or written defamation if the act is clearly done in the public interest or because they are forced to defend themselves.

A person can use computers and internet networks to insult others, for example by publishing an insult about someone on his personal social media account, a website, or sending e-mails that contain information and personal things about someone to someone else. Humiliation can be done by uploading a personal chat screenshot that has the potential to attack someone's reputation. In 2003, the European Union Court of Justice passed a law explaining the law in connection with publications containing content that was defamatory or embarrassing. The European High Court ruled that sending personal information, images or video clips of others without the consent of the person concerned violated the law under the EU 1995 European Data Protection Directive, even though it did not include some activities such as journalism.³⁶

The imposition of criminal sanctions for defamation has been largely abandoned in many democratic countries. In addition to inhibiting freedom of expression, actions that are considered defamation are often only opinions that result from one's perception of a problem. The United States Supreme Court ruling in the case of the New York Times versus Sullivan in 1964, which stressed that public officials can only hold responsibility for the actions of someone who is considered "defamation" if the official is able to prove that the person's actions are not in accordance with facts. In the ruling, the United States Supreme Court states that government officials (public figures), can only hold the accountable media or those who make civil defamation statements. Following the ruling of the Supreme Court, there has been a significant decline in defamation lawsuits brought before the Court, as the claimant must furnish evidence to substantiate the falsity or fabrication of the defendant's submission or publication. Malaysia knows two types of criminal defamation both criminal and civil. Civil libel refers to the 1957 Defamation Act. Criminal defamation that contains fines, imprisonment, or both, originates from Chapter XXI Article 499 of the Criminal Code.³⁷

Provisions in criminal law in Indonesia that can be used against uploading personal chat screenshots on social media are provisions prohibiting cyberbullying. Article 45B The Law of Information and Electronic Transactions 2016 states that violators may face up to 4 (four) years in prison and/or a fine of Rp750,000,000.00 (seven hundred fifty million rupiah) for sending electronic information and/or electronic documents that contain threats of violence or intimidation addressed personally as described in Article 29 the Law of Information and Electronic Transactions 2008. This Article's provisions cover online harassment (cyberbullying) that involves threats of violence or intimidation and causes material, psychological, or bodily harm.

³⁶ J. A. Castañeda, F. J. Montoso, and T. Luque, "The Dimensionality of Customer Privacy Concern on the Internet," *Online Information Review* 31, no. 41 (2007): 420-439. <https://doi.org/10.1108/14684520710780395>

³⁷ Edwin Pardede, Eko Soponyono, and Budhi Wisaksono, "Kebijakan Hukum Pidana dalam Upaya Penegakan Tindak Pidana Pencemaran Nama Baik Melalui Twitter," *Diponegoro Law Journal* 5, no. 3 (2016) 1-22. <https://ejournal3.undip.ac.id/index.php/dlr/article/view/12541>

The uploading of chat content on social media can also be threatened with criminal provisions as stipulated in Article 67 paragraph (2) of the Law of Personal Data Protection. The provision stipulates the criminal penalty for every person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp 4,000,000,000.00 (four billion rupiah). Sanksi Pidana is a means of providing personal data protection. Adequate protection of Personal Data will be able to give the public confidence to provide Personal Data for various greater public interests without being misused or violating their personal rights. This regulation on Personal Data Protection will make a great contribution to the creation of order and progress in the information society.

4. Conclusion

Privacy rights are related to the decision to open up virtually or not. Uploading of personal chat screenshots on social media is closely related to violations of privacy rights. Privacy covers one's communication. Uploading on social media can cause a person to lose his privacy. Actions to upload screenshots on social media on the one hand have no legal consequences, but on the other hand can cause crime, even included in the crime category. This screenshot upload causes other people steal personal data from people involved in the personal chat. The parties involved in personal communication also have the potential to become victims of cyberbullying. Countries in the world regulate the protection of privacy and personal data rights. In the legal system in Indonesia, the act of uploading personal chat screenshots can lead to lawsuits. Violation of personal data provides an opportunity for the injured party to claim compensation. The act of uploading a personal chat screenshot has the potential to defame someone's reputation. The act is a crime in Indonesian criminal law, both in the form of insults and cyberbullying.

Acknowledgments

On this occasion, allow us to express our gratitude to the Dean of the Faculty of Law at Universitas Pendidikan Nasional, the Dean of the Faculty of Law at Universitas Hindu Negeri I Gusti Bagus Sugriwa Denpasar, and the Dean of the Faculty of Law at Universitas Dwijendra, and all parties contributed in this research.

References

- Al-Suwaidi, Noura, Haitham Nobanee, and Fauzia Jabeen. "Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator." *International Journal of Cyber Criminology* 12, no. 2 (2018): 392-407. <https://doi.org/10.5281/zenodo.3365895>
- Assarut, Nuttapol, Piyabutr Bunaramrueang, and Patanaporn Kowpatanakit. "Clustering Cyberspace Population and the Tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory." *International Journal of Cyber Criminology* 13, no. 1 (2019). <https://doi.org/10.5281/zenodo.3550473>
- Blackburn, Camille. "New Technology, Personal Data Protection and Implications for Financial Services Regulation." *JASSA: The Journal of the Securities Institute of Australia* 4, (2015): 59-65.

- Blessman, S. "What to Look for. How to Prevent it Law Enforcement Technology." *Fort Atkinson* 43, no. 7 (2016): 33-34.
- Budhijanto, Danrivanto. *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi Regulasi dan Konvergensi*. Bandung: Refika Aditama, 2010.
- Castañeda, J. A., F. J. Montoso, and T. Luque. "The Dimensionality of Customer Privacy Concern on the Internet." *Online Information Review* 31, no. 41 (2007): 420-439. <https://doi.org/10.1108/14684520710780395>
- Chen, Mengtong, Anne Shann Yue Cheung, and Ko Ling Chan. "Doxing: What Adolescents Look for and Their Intentions." *International Journal of Environmental Research and Public Health* 16, no. 2 (2019): 218. <https://doi.org/10.3390/ijerph16020218>
- Chen, Qiqi, Ko Ling Chan, and Anne Shann Yue Cheung. "Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong." *International Journal of Environmental Research and Public Health* 15, no. 12 (2018): 2665. <https://doi.org/10.3390/ijerph15122665>
- Cooley, Joseph, and Sean Smith. "Privacy-preserving Screen Capture: Towards Closing the Loop for Health IT Usability." *Journal of Biomedical Informatics* 46, no. 4 (2013): 721-733. <https://doi.org/10.1016/j.jbi.2013.05.007>
- Dewi, Sinta. "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 35-53. <https://doi.org/10.20961/yustisia.v5i1.8712>
- Dewi, Sinta. *CyberLaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran, 2009.
- Douglas, David M. "Doxing: A Conceptual Analysis." *Ethics and Information Technology* 18, no. 3 (2016): 199-210. <https://doi.org/10.1007/s10676-016-9406-0>
- Hammond, B. (2015). *Icann uRged to Reject Proposal to Display Website Owners' Addresses*. *Cybersecurity Policy Report* 13 (2015).
- Hansen, Isabella, and Darren J Lim. "Doxing Democracy: Influencing Elections Via Cyber Voter Interference." *Contemporary Politics* 25, no. 2 (2019): 150-171. <https://doi.org/10.1080/13569775.2018.1493629>
- Haryanto, A.Y. "Riset: Ada 175,2 Juta Pengguna Internet di Indonesia." (2020). Retrieved from <https://inet.detik.com/cyberlife/d-4907674/riset-ada-1752-juta-pengguna-internet-di-indonesia>
- Houghton, David J., and Adam N. Joinson, "Privacy, Social Network Sites, and Social Relations." *Journal of Technology in Human Services* 28, no. 1-2 (2010): 74-94. <https://doi.org/10.1080/15228831003770775>
- Huang, Travis K. "Exploring the Antecedents of Screenshot-based Interactions in the Context of Advanced Computer Software Learning." *Computers & Education* 80, (2015): 95-107. <https://doi.org/10.1016/j.compedu.2014.08.011>
- Islamy, I. T., S. T. Agatha, R. Ameron, B. H. Fuad, Evan Evan, N. A. Rakhmawati. "Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi." *JTIP: Jurnal Teknologi Informasi dan Pendidikan* 11, no. 2 (2018): 21-28. <https://doi.org/10.24036/tip.v11i2.137>
- Jaishankar, Karuppannan. "Cyber Criminology as An Academic Discipline: History, Contribution and Impact." *International Journal of Cyber Criminology* 12, no. 1 (2018): 1-8. <https://doi.org/10.5281/zenodo.1467308>
- Jaishankar, Karuppannan. "Establishing A Theory of Cyber Crimes." *International Journal of Cyber Criminology* 1, no. 2 (2007): 7-9.

- Krisnawati, E. "Mempertanyakan Privasi di Era Selebgram: Masih Adakah?." *Jurnal Ilmu Komunikasi* 13, no. 2 (2016): 179-200.
- Lestari, Maya Puji. "Hubungan Romantis di Media Sosial (Resepsi Pengguna terhadap Keterbukaan Hubungan Romantis yang Diunggah Selebgram di Instagram)." *Komuniti: Jurnal Komunikasi dan Teknologi Informasi* 11, no. 1 (2019): 28-44. <https://doi.org/10.23917/komuniti.v10i3.5944>
- Makarim, Edmon. *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Jakarta: PT RajaGrafindo Persada, 2006.
- Mills, Alex. "Choice of Law in Defamation and the Regulation of Free Speech on Social Media: Nineteenth-Century Law Meets Twenty-first-century Problems." *In the Legal Challenges of Social Media*. (2017): 270-292. <https://doi.org/10.4337/9781785364518.00028>
- Nazish, Noma. "Instagram is the Worst Social Media Platform for Cyber-bullying." *Blastingnews* (2018.) Retrieved from <https://uk.blastingnews.com/tech/2017/07/instagram-is-the-worst-social-media-platform-for-cyber-bullying-001864525.html>.
- Ngo, Fawn T., and K. Jaishankar. "Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime." *International Journal of Cyber Criminology* 11, no. 1 (2017). <https://doi.org/10.5281/zenodo.495762>
- Notar, Charles E., Sharon Padgett, and Jessica Roden. "Cyberbullying: A Review of the Literature." *Universal Journal of Educational Research* 1, no. 1 (2013): 1-9.
- Pardede, Edwin, Eko Soponyono, and Budhi Wisaksono. "Kebijakan Hukum Pidana dalam Upaya Penegakan Tindak Pidana Pencemaran Nama Baik Melalui Twitter." *Diponegoro Law Journal* 5, no. 3 (2016) 1-22. <https://ejournal3.undip.ac.id/index.php/dlr/article/view/12541>
- Privacy International (2020). What Is Privacy? Retrieved from <https://privacyinternational.org/explainer/56/what-privacy>.
- Purwaningsih, Mardiana. "Standar Etika bagi Perusahaan yang Menggunakan Media Sosial sebagai Enterprise's Official Presence." *Jurnal Sistem dan Informatika* 11, no. 1 (2016).
- Raharjo, Agus, Yusuf Saefudin, and Rini Fidiyani. "The Influence of Technology Determinism in Forming Criminal Act of Legislation." *E3S Web of Conferences* 73, no. 12011 (2018). <https://doi.org/10.1051/e3sconf/20187312011>
- Rohmana, Nanda Yoga. "Prinsip-Prinsip Hukum tentang Tindak Pidana Penghinaan dan Pencemaran Nama Baik dalam Perpspektif Perlindungan Hak Asasi Manusia." *Yuridika* 32, no. 1 (2017): 105-133.
- Sarikakis, Katharine, and Lisa Winter. "Social Media Users' Legal Consciousness About Privacy." *Social Media+ Society* 3, no. 1 (2017): 1-14. <https://doi.org/10.1177/2056305117695325>
- Sherlyanita, A. K., and N. A. Rakhmawati. "Pengaruh dan Pola Aktivitas Penggunaan Internet serta Media Sosial pada Siswa SMPN 52 Surabaya." *Journal of Information Systems Engineering and Business Intelligence* 2, no. 1 (2016): 17-22.
- Simpkin, Hannah. *Exploring the Impact of Social Networking Sites (SNSs) on Modern Gossip from Female Perspectives*. Manchester Metropolitan University, Dissertations, 2017. <https://e-space.mmu.ac.uk/id/eprint/619201>
- Sitompul, Asril. *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace)*. Bandung: Citra Aditya Bakti, 2004.

Starr, Tegan S., and Tiffany Lavis. "Perceptions of Revenge Pornography and Victim Blame." *International Journal of Cyber Criminology* 12, no. 2 (2018). <https://doi.org/10.5281/zenodo.3366179>

Yuwinanto, Helmy Prasetyo. "Privasi Online dan Keamanan Data." *Palimpsest* 31, no. 11 (2015).

"What is Privacy?" Accessed July 21, 2023. <https://privacyinternational.org/explainer/56/what-privacy>.

Law and Regulations

Criminal Code.

The Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions.

The Law of the Republic of Indonesia No. 19 of 2016 concerning Amendments to the Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions.

The Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.