Personal Data Protection in Digital Communications During the Covid-19 Pandemic

Nani Nurani Muksin[1(✉)], Wichitra Yasya[2], Tria Patrianti[1], and Donny Kurniawan[1]

[1] Universitas Muhammadiyah Jakarta, Jakarta, Indonesia
{naninuranimuksin,tria.patrianti,donny.kurniawan}@umj.ac.id
[2] Universitas Bhayangkara, Jakarta, Indonesia
Wichitra.yasya@dsn.ubharajaya.ac.id

Abstract. Life in the cyber era during the COVID-19 pandemic is marked by digital communication. When doing digital communication, personal data is stored on the internet. The importance of this study because it presents the experience of the audience about the importance of personal data protection in digital communication. This study aims to explore the understanding of personal data protection, the experience of digital communication during the pandemic and the meaning of personal data protection in digital communications. This study uses a qualitative approach with the phenomenological method. The results showed that Personal data protection is understood as a protection against personal data that cannot be shared arbitrarily. Cybercrimes that have been experienced include fraud and being hacked. Personal data protection is interpreted as a warning when doing digital communication, protection is carried out for example by activating a double password or entering a data protection application. The findings of this study indicate that the protection of personal data is an important matter for both data owners, data managers and the government to pay attention to. The implication is the need for a legal protection from the Government of Indonesia in the form of a Law on Personal Data Protection.

Keywords: personal data protection · digital communications · COVID-19 pandemic period

1 Introduction

In the era of Industry 4.0 and society 5.0, most of the communication is done digitally and online. Especially during this COVID-19 pandemic, almost all activities are carried out through digital communication such as Work from Home, Study from home, and online shopping. There are advantages from online digital communication because it is more practical, flexible, and the data is stored properly. Technological developments are used to meet human needs and communicate digitally to meet their needs so as not to be stressed during the COVID-19 pandemic [1]. Digital communication can provide benefits and convenience during the COVID-19 pandemic if managed properly. COVID-19 survivor in Indonesia has competence in communication management specially by

O. Purnamasari et al. (Eds.): ICORCOM 2021, ASSEHR 729, pp. 220–229, 2023.
https://doi.org/10.2991/978-2-38476-016-9_22

digital communications and considers that communication is an important factor in helping recovery [2].

Behind the advantages of using digital communication, there are things to watch out for regarding personal data. Personal data stored on the internet in various platforms that have been used can be used by irresponsible parties to commit online crimes (cyber*crime*). One of the latest cases of cybercrime is the alleged leak of personal data of 279 million Indonesians. Ministry of Communication and Information Technology (Kominfo) through Press Release No. 178/HM/KOMINFO/05/2021, May 20, 2021, Responding to the alleged leak of personal data through the Direktorat Pengendalian Aplikasi Informatika Ditjen Aplikasi Informatika Kementerian Komunikasi dan Informatika [3]. Through the press conference, Kominfo asked all digital platform providers and personal data managers to further improve the security of managed personal data. Kominfo also invites the public to be more careful and vigilant in protecting their personal data.

Kominfo through Press Release No. 179/HM/KOMINFO/05/2021 on Friday, May 21, 2021 carried out *an update regarding the* alleged leak of personal data of Indonesian residents the Based on the investigation, Kominfo found an account named Kotz selling personal data on Raid Forums. Kominfo took various anticipatory steps to prevent the wider spread of data by requesting termination of access to the link to download the personal data. In addition, the Ministry of Communication and Information has summoned the Board of Directors of BPJS Kesehatan as the manager of the personal data that was allegedly leaked for a more in-depth investigation process according to the mandate of Government Regulation Number 71 of 2019 [4].

The previous case was the theft of personal data from Facebook, Instagram, and LinkedIn accounts of 214 million. The data stolen was the user's email address, phone number and full name, and in some cases, specific location data. This breach of personal data collection was uncovered by researchers Safety Detectives [5]. Potential consequences of disclosing this personal information include identity theft and financial fraud perpetrated on other platforms. Personal data in the form of photo ID cards and selfies with ID cards are often misused for illegal online loans [6].

The problem in this study is "What is the meaning of personal data protection in digital communication during the COVID-19 Pandemic?" The purpose of this research is to find out and analyze: 1) Understanding of personal data protection; 2) Digital communication experience during the COVID-19 pandemic; 3) The meaning of personal data protection in digital communication during the COVID-19 Pandemic.

The urgency of this research is the importance of understanding the protection of personal data so that caution is necessary when conducting digital communications. Considering that digital communication will leave a trail of data on all platforms that can be misused by irresponsible parties to commit cybercrimes. Theoretically**,** this research will contribute to the development of Digital Communication theory, and the concept of Personal Data Protection. Practically**,** the significance of this research for the public is to provide an understanding of the importance of protecting personal data so that they are wise and vigilant in conducting digital communications. For providers of digital platform managers to further improve the security of the personal data they manage.

2 Literature Review

Digital Communication

Digital communication is marked by the birth of the digital era in the form of internet networks and computer information technology. Digital communication is an interaction through *computer mediated communication (CMC*), Cantoni and Tardini [7]. According to Nasrullah (2016: 79), CMC is a process of human communication through computers involving audiences, in certain contexts, where the process utilizes media for certain purposes [8]. In connection with this research during the COVID-19 Pandemic, Individuals conduct digital communication *online* to find information and carry out all communication activities that cannot be done *offline* due to implementing health protocols.

The internet-based digital world makes all the activities of its residents unlimited by space and time. The legal protection to regulate all forms of these activities, such as the Electronic Information and Transaction Law (UU ITE) in 2008 continues to be refined [9]. Digital communication with various online platforms makes it easier for people to carry out activities during the COVID-19 pandemic. Digital communication has two sides, namely positive and negative sides. The positive side is the ease of digital communication, which is easier, faster, more flexible as if without the constraints of space and time. The downside is that digital communication makes it seem as if people's privacy is missing. Personal data recorded on a computer makes internet user data easy to track with various indications such as surfing habits, hobbies, and other preferences. This becomes vulnerable and opens space for cybercrimes to occur.

Personal Data Protection Concept

Based on Ministerial Regulation (Permen) No. 20 of 2016 concerning the Protection of Personal Data (PDP) which was stipulated 7 November 2016, promulgated and effective from 1 December 2016, Personal Data is certain individual data that is stored, maintained, and kept true and protected by confidentiality [10]. Personal Data Owner is the individual to whom Certain Personal Data is attached. Each Electronic System Operator must prepare internal rules for the protection of Personal Data as a form of preventive measure to avoid failures in the protection of the Personal Data it manages. The acquisition and collection of Personal Data by the Electronic System Operator must be based on Approval or based on the provisions of laws and regulations.

In this Ministerial Regulation, it is emphasized that the electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal rules regarding the protection of personal data which must pay attention to aspects of technology application, human resources, methods, and costs. The owner of personal data has the right to the confidentiality of his data; has the right to file a complaint in the context of resolving personal data disputes; has the right to have access to historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system [11].

The Electronic system operator is obliged to provide access or opportunity for the Personal Data Owner to change or update his/her Personal Data without disturbing the Personal Data management system, unless otherwise stipulated by the provisions of laws and regulations; destroying Personal Data in accordance with the provisions in this

Ministerial Regulation or the provisions of other laws and regulations that specifically regulate the respective Supervisory and Regulatory Agencies of the Sector for that purpose; and provide a *contact person* who is easily contacted by the Personal Data Owner regarding the management of his Personal Data [12].

Previous Research

Several relevant studies show *the state of the art* and *novelty* of this research. Nurhidayati [13], Settings for Personal Data Protection in the Use of Pedulilindungi Applications. The protection of the personal data of this application user is based on the regulations governing Information and Communication Technology, Health, and the Implementation of Population administration, although the government provides security guarantees for PeduliLindung users [13]. Sri Ayu Astuti [14], Era of Technological Disruption 4.0 And Legal Aspects of Personal Rights Data Protection. The use of technological advances, especially during the COVID-19 pandemic, is faced with the lack of maximum legal protection for personal rights, including personal data. This is the responsibility of the state, namely the organizers of the Government of the Republic of Indonesia in the jurisdiction of Indonesia [14].

Newlands [15], Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. Digital technology helps governments and organizations to enforce protective measures, such as contact tracing, hasty deployment and adoption, also raising concerns about surveillance, privacy and data protection. Is there a way to speed up privacy assessments that can anticipate and help reduce the potential adverse privacy implications this may have on society [15].

Christofidou [16], A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. In the European Union, the GDPR acts as a regulatory framework that provides the necessary draft laws for dealing with personal data in the COVID-19 crisis, particularly in the context of health mobile applications, in order to be lawful, fair and reflect the social and ethical values underlying the Union. Europe. However, this raises the question of the extent to which GDPR can be applied when this particular type of data and information is required for research under time pressure. Ethical issues arise when using citizen data broadly and placing the public interest and individual privacy on the opposite scale [16]. Ventrella [17], Privacy in emergency circumstances: data protection and the COVID-19 pandemic. The pandemic has required balancing privacy with health and security. The European approach demonstrates the highest standards of maintaining data protection and privacy, even in exceptional circumstances given the increased risk associated with cybercrime to the security of personal data during the pandemic [17].

Zwitter [18], Big data, privacy and COVID-19 learning from humanitarian expertise in data protection. The use of big data to control the spread of COVID-19 raises potential and concerns about ongoing practices. However, principles and standards of data practice in the humanitarian field apply during this crisis, and consider the use of data-driven monitoring tools to address the COVID-19 crisis [18]. Ienca [19], On the responsible use of digital data to tackle the COVID-19 pandemic. The European Data Protection Council issued a statement on the importance of protecting personal data when used in the fight against COVID-19 and highlighted certain articles of the General Data Protection Regulation that provide the legal basis for processing personal data in that

context. Careful data management practices should govern data collection and data processing. Gaining access to data from personal devices for contact tracing purposes, for example, may be justified if it occurs within certain limits, has a clear purpose for example, warns and isolates people who may have been exposed to a virus and is no less invasive alternative for example, uses mobile positioning data anonymized is suitable for that purpose [19]. Abeler [20], COVID-19 Contact Tracing and Data Protection Can Go Together. The application of application-based contact tracing to control the coronavirus disease (COVID-19) pandemic can go hand in hand with aspects of data protection and user acceptance [20].

3 Research Methodology

This research approach is qualitative and phenomenological method. The study of phenomenology aims to explore the deepest awareness of the subjects regarding experience and its meaning [21]. The source of information in this study was the student informant of MIKOM FISIP UMJ. The informants of this study were 15 students who were selected using a purposive technique. The reason for choosing students as informants is because students are a millennial generation who are very close to the use of *gadgets* and digital communication.

The data collection technique was done by *online interview.* While the data analysis technique used in this study is a modification of the phenomenological analysis technique of Van Kaam, namely:

1. *Listing and Preliminary Grouping*

List all expressions relevant to experience, namely a list of answers from informants or research subjects *(horizontalization)*

2. *Reduction and Elimination*

Tests each and eliminates the existing expressions.

3. *Clustering and Thematizing the Invariant Constituents (Thematic portrait)*
4. *Final Identification of the Invariant Constituents and Themes by Application: Validation*

Is the process of validating the *Invariant Constituent.* The activity in this stage is to check the *Constituent Invariants* and the accompanying themes against the complete recording of the research respondents' statements.

5. *Individual Texture Description*
6. *Individual Structural Description*

The results of the preparation of *Individual Textural Description* and *Imaginative Variation* will build *an Individual Structural Description* from the experience of each research subject.

7. *Textural-Structural Description*

This stage is a process of combining *Textural Description* and *Structural Description* from the experiences of each research subject. After that, a *Composite Description is made* of the meaning and essence of the experience so that it displays a complete picture of the experience [22].

Data validity techniques through expert triangulation with Digital Communication experts, namely Dr. Rulli Nasrallah.

4 Findings and Discussion

The findings of this study are as follows:

1. **Understanding of Personal Data Protection**

Personal data is understood as all data relating to a person's personal identity that is private, either identified or individually identifiable, which can be found or accessed electronically or non-electronically. Personal data is data that contains personal information, regarding personal identity that cannot be shared arbitrarily because not everyone may know it, so personal data must be protected.

Personal data is data that is created and stored that contains information about a person's privacy. Examples of personal data such as Population Identification Number (NIK), Identity Card, Family Card, biological mother's name, home address, email address, date of birth, birth certificate, medical records, and others. Personal data is related to everything that is personal, so the photos in someone's social media gallery are actually personal data.

An understanding of the importance of protecting personal data is obtained from several articles and also reports in various media. Reports about personal data leaks and cybercrimes further strengthen the understanding that personal data needs to be protected. Personal data should not be known and used by other people carelessly. Personal data is privacy, so the data owner is obliged to keep it secret, especially to guard against bad deeds from irresponsible persons.

2. **Digital Communication Experience During the COVID-19 Pandemic**

Digital communication is almost always carried out during the COVID-19 Pandemic, because most activities are carried out using digital *platforms.* Banking activities, online transportation, work from home, online lectures, online shopping are all done digitally, as well as when accessing cyber media and using social media. The majority of informants use Instagram social media, followed by Youtube, Facebook, Twitter and tiktok. While cyber media, especially the use of email, websites, blogs, and Wikis.

Most of the informants use the digital *platform* Zoom Cloud Meetings, Google Meet, and WhatsApp for purposes in the fields of education, friendship, organization, and including for work purposes, there are also some who use Skype and Teams for these

purposes. Then for purposes in the economic and business fields, most of the informants use M-Banking applications, e-commerce, including digital payments.

Almost all informants have had memorable experiences when doing digital communication, both pleasant and unpleasant experiences. These pleasant experiences are generally related to communication that can be carried out without being limited by distance and time, but becomes less pleasant because it is limited by the internet network which sometimes has obstacles that cause *delays in response, lack of certainty*, and lack of interaction.

Some of the informants have made digital communication by including personal data which is generally done for administrative completeness during registration or online data collection, whether in the fields of education, health, transportation, for purchases on e-commerce and so on. So, almost all informants have shared or *shared* personal data on social media or perform digital communications.

The data shared by informants generally include place and date of birth, telephone number, and personal photos. There are also informants who share other personal data such as domicile and school origin. In addition, the informants also share personal data as a complete social media registration, but do not post them but *submit* the data to social media applications. The experience of digital communication during the Pandemic period that provided personal data was when filling out "Application Care to Protect Data for COVID-19 vaccination", where currently, Care to protect data is always needed when entering government agencies, private sector or shopping malls.

3. The Meaning of Personal Data Protection in Digital Communication During the COVID-19 Pandemic

Several informants have experienced *cybercrime.* Experience being a victim of cybercrime These are frauds with various modes; besides that, they are also *hacked* and receive *spam.* There is one informant who experienced cybercrime with a stranger. Initially friends on social media but then ended up getting threats to be *hacked* and sending obscene messages to friends from the informant.

Based on the experience of informants who have experienced cybercrime, and several reports about cybercrime in various online media and social media, the informant means that personal data absolutely must be protected, *especially* by the owner of the personal data. The majority of informants protect personal data by not disseminating personal data on social media and other people except with a clear purpose, as well as being more selective and careful in providing personal data both to other people and the intended agency if it is necessary. Most of the informants also protect personal data by taking steps to protect their email and social media accounts, namely by activating two-step verification, two-system security, *double passwords,* or entering data protection applications.

Informants have different ways of responding to digital communications in the future, however, they are generally more adaptive, more careful, and more selective in conducting digital communications. There are also *informants* who still don't know how to respond, because they are still unable to adapt to the digital era, this is where the importance of socialization and education about digital communication security and the importance of personal data protection.

The informant means that personal data must be guarded and protected. Informants think that the protection of personal data is very important to avoid misuse of personal data by irresponsible parties. In general, informants protect their personal data by being more selective and careful in conducting digital communications by not sharing personal data without clear interests and providing protection on platforms that have personal data. The action taken in the event of misuse of personal data is to take action to report the misuse or theft of the personal data to related parties, such as the police. If the cybercrime is committed on *a digital platform,* then report and ask for accountability to the "manager" *of the platform* the *digital.*

Regarding the protection and prosecution of personal data theft and cybercrime, clear rules are needed in the form of legislation as other regulatory protection. Until now, the Law on Personal Data Protection, still in the form of a Draft Law (RUU), urgently needs to be promulgated.

5 Findings and Discussion

The conclusions and implications of this research are:

Personal Data Protection is understood as all data relating to a person's identity and is private. Personal data is data that contains personal information, regarding personal identity which not everyone has the right to know, so personal data must be protected. Examples of personal data such as Population Identification Number (NIK), Identity Card, Family Card, biological mother's name, home address, email address, date of birth, birth certificate, medical records, and others. Personal data is related to everything that is personal, so the photos in someone's social media gallery are actually personal data.

Experience of digital communication during the COVID-19 Pandemic especially related to *work from home activities*, banking, online transportation, online shopping, and all activities carried out digitally. These digital communication activities use the Zoom Cloud Meetings, Google Meet and Skype digital media *platforms.* The experience of digital communication is also related to the increased activity of social media and cyber media during the pandemic. The social media used are mainly Instagram, Youtube, Facebook, Twitter, and Tiktok. While cyber media, especially the use of email, websites, blogs, and Wikis. Meanwhile, for the purposes of friendship, including the purposes of work and sharing information within the organization, especially using the WhatsApp, Line, Telegram applications. For economic and banking needs, M-Banking applications, e-commerce, and digital payments are used. Memorable experiences when doing digital communication are generally related to communication that can be done without being limited by distance and time, but becomes less pleasant because it is limited by the internet network which sometimes has obstacles that cause *delays in response*, *lack of certainty*, and lack of interaction. Experience in conducting digital communication by including personal data which is generally done for administrative completeness during registration or online data collection, whether in the fields of education, health, transportation, for purchases on e-commerce and so on. Experience digital communication during the Pandemic by including personal data, especially when filling out "Application Care to Protect Data" for COVID-19 vaccination.

Personal data protection in digital communication during the COVID-19 pandemic is interpreted as protection and prudence in maintaining personal data. Cybercrime can be in the form of fraud with various modes, being *hacked* and receiving obscene *spam messages*. Protecting personal data is done by not disseminating personal data on social media and other people except with a clear purpose. Protect personal data by taking protective steps on its email and social media accounts, namely by activating two-step verification, two-system security, *double passwords*, or entering data protection applications. The meaning of personal data is also interpreted as to avoid misuse of personal data by irresponsible parties. The action taken in the event of misuse of personal data is to take action to report the misuse or theft of the personal data to related parties, such as the *platform "Manager" digital* and cybercrime police. It is hoped that Indonesia will soon have a Personal Data Protection Law as a legal protection.

References

1. M. U. Batoebara, M. S. I. Lubis, and M. Saleh, "Komunikasi Digital Dan Perubahan Sosial Di Masa Pandemic Covid 19," Liwaul Dakwah J. Kaji. Dakwah dan Masy. Islam, vol. 10, no. 2, pp. 21–28, 2020.
2. N. N. Muksin, M. Habibi, T. Patrianti, H. Hidayat, and R. Djalun, "Communication Management of Covid-19 Survivors in Indonesia," in 3rd Jogjakarta Communication Conference (JCC 2021), 2021, pp. 143–147.
3. D. Permadi, "Pernyataan Kominfo terkait Dugaan Kebocoran Data Pribadi 279 Juta Penduduk Indonesia," Kominfo Siaran Pers No. 178/HM/KOMINFO/05/2021, 2021. .
4. D. Permadi, "Update terkait Dugaan Kebocoran Data Pribadi Penduduk Indonesia," Siaran Pers Kominfo No. 181/HM/KOMINFO/05/2021, 2021. .
5. CNBC, "Data Pribadi 214 Juta Pengguna Facebook & Instagram Dicuri," CNBC Indonesia, 2021. https://www.cnbcindonesia.com/tech/20210114181641-37-216058/data-pribadi-214-juta-pengguna-facebook-instagram-dicuri.
6. P. Anugerah, "Pinjaman online: 'Bagaimana saya menjadi korban penyalahgunaan data pribadi,'" BBC News Indonesia, 2021. https://www.bbc.com/indonesia/majalah-57046585.
7. L. Cantoni and S. Tardini, Internet. Routledge, 2006.
8. R. Nasrullah, "Cyber media theory and research," Jakarta Prenadamedia Gr., 2014.
9. Peraturan Menteri, "Ministerial Regulation (Permen) No. 20 of 2016 concerning Personal Data Protection (PDP)." 2016.
10. Kominfo, "Issues Discussed on Social Media, Strategy for Implementation of Personal Data Protection Regulations in Indonesia, Ministry of Communication and Information Technology Research and Development Agency for Aptika and IKP 2019 Research and Development Cente." 2019.
11. W. Setiawan, "The Digital Age and Its Challenges," Era Digit. dan Tantangannya, p. 1, 2017.
12. R. Komalasari, "Manfaat Teknologi Informasi dan Komunikasi di Masa Pandemi Covid 19," Temat. J. Teknol. Inf. Komun., vol. 7, no. 1, pp. 38–50, 2020.
13. N. Nurhidayati, S. Sugiyah, and K. Yuliantari, "Pengaturan Perlindungan Data Pribadi Dalam Penggunaan Aplikasi Pedulilindungi," Widya Cipta J. Sekr. Dan Manaj., vol. 5, no. 1, pp. 39–45, 2021.
14. S. A. Astuti, "Era Disrupsi Teknologi 4.0 dan Aspek Perlindungan Data Hak Pribadi," PAJOUL (Pakuan Justice J. Law), vol. 1, no. 1, 2020.
15. G. Newlands, C. Lutz, A. Tamò-Larrieux, E. F. Villaronga, R. Harasgama, and G. Scheitlin, "Innovation under pressure: Implications for data privacy during the Covid-19 pandemic," Big Data Soc., vol. 7, no. 2, p. 2053951720976680, 2020.

16. M. Christofidou, N. Lea, and P. Coorevits, "A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection during a time of Crisis," Yearb. Med. Inform., vol. 30, no. 01, pp. 226–232, 2021.
17. E. Ventrella, "Privacy in emergency circumstances: data protection and the COVID-19 pandemic," in ERA Forum, 2020, vol. 21, no. 3, pp. 379–393.
18. A. Zwitter and O. J. Gstrein, "Big data, privacy and COVID-19–learning from humanitarian expertise in data protection," Journal of International Humanitarian Action, vol. 5, no. 1. SpringerOpen, pp. 1–7, 2020.
19. M. Ienca and E. Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic," Nat. Med., vol. 26, no. 4, pp. 463–464, 2020.
20. J. Abeler, M. Bäcker, U. Buermeyer, and H. Zillessen, "COVID-19 contact tracing and data protection can go together," JMIR mHealth uHealth, vol. 8, no. 4, p. e19359, 2020.
21. M. B. Miles, A. M. Huberman, and J. Saldana, Qualitative Data Analysis: A Methods Sourcebook, 3rd ed. London: Sage, 2014.
22. C. Moustakas, Phenomenological research methods. Sage publications, 1994.