Dicoment: Journal Digital Communications and Media Networks
Dicoment, 1(1) (2024); 23-32
E-ISSN: xxxx-xxxx DOI: 10.xxxxx/jepp.xxxx.xxxx
Available online: https://jurnal.literasipublisher.co.id/index.php/Dicoment

Digital Transaction Communication: Understanding Teenagers' Privacy in Data Protection

Edi Nurwahyu Julianto[1*], Ilham Setyawan[2], Hilda Rahmah[1]

[1] Program Studies Communication Science, Universitas Semarang, Indonesia
[2] Program Studies Digital Communication, Universitas Insan Cita, Indonesia

ARTICLE INFO
Keywords: Communication management, personal data protection, digital transactions

Received: 28 February 2024
Accepted: 7 February 2024

ABSTRACT

This research aims to determine the privacy management of personal data protection in digital transactions. Personal data protection is often best with various information sharing models. Data threats often cause problems that are detrimental to young people, but these problems are often ignored. Privacy management and protection of personal data in digital transactions is becoming increasingly important along with the increasing use of digital technology in everyday life. Using qualitative methods by conducting interviews with young people who use applications for digital transactions. The research results show that communication management is carried out in the form of organizing, analyzing and optimizing personal data protection. Teenagers understand about protecting personal data on the platform. The platform's certainty of protecting personal data in digital transactions increases teenagers' confidence in sharing data. To ensure effective privacy management teens review the security and surveillance system rules according to security standards. The emergence of a proactive and continuously monitoring attitude in privacy management as a form of awareness among young people about digital transactions.

*Corresponding Author: Edi Nurwahyu Julianto
Email: *edi@usm.ac.id*

INTRODUCTION

Increasingly intensive digital communication encourages different forms of interaction, such as sharing activities and increasing digital transactions such as buying and selling. This condition allows each user to share personal information in the transaction process. Often, this condition causes negative effects such as fraud and theft of personal information. According to Bank Indonesia (BI), in 2023, the value of digital banking transactions will be recorded at IDR 58,478.24 trillion or an annual growth of 13.48 percent. Meanwhile, in 2024, digital transactions are expected to grow by 9.11 percent on an annual basis to reach IDR 63,803.77 trillion. This optimism is based on the performance of digital economic and financial transactions supported by a secure, smooth and reliable payment system (Subekti, 2024). Transaction security and compliance with security protocols in online transactions are often problems for people when using digital transactions. Lack of protection of personal data and limited knowledge of regulations are barriers. According to the Association of Indonesian Internet Network Providers (APJII), the number of internet users in Indonesia has reached 79.5% at the beginning of 2024, an increase of 2.75% from the beginning of 2023. The increase is higher compared to the 2022-2023 period, which was only 2.66%. About 221 million Indonesians are connected to the internet. Meanwhile, the number of people connected to the internet will reach 215 million in 2023. Strong cooperation between the private sector and the government in efforts to expand internet access throughout Indonesia (Suhartanto, 2024).

The development of the internet is also beginning to have an impact on the economic sector, giving rise to various types of innovation. This innovation is known as fintech (financial technology), which is an innovation in the economic sector with a digital basis. Fintech refers to the use of technology to provide solutions to various financial problems. The presence of fintech has changed people's behaviour in carrying out economic activities with the various conveniences offered. The advancement of digital skills offered by the information technology era has the potential to be a tool of empowerment, but it also opens up opportunities for criminals to take advantage of society's ignorance and negligence (Azzani et al., 2023). Based on data from SimilarWeb cited from the databases page, Shopee is the e-commerce site with the highest number of website visitors in Indonesia in the first quarter of 2023. In the period January-March 2023, the Shopee site achieved an average of 157.9 million monthly visits. . In the same period, Tokopedia achieved an average of 117 million visits, followed by Lazada with 83.2 million visits, BliBli with 25.4 million visits and Bukalapak with 18.1 million visits per month. 2023 (Ahdiat, 2024). This means that the potential for digital interaction described above allows a lot of personal data to be exchanged in transactions. One of these is online credit, which allows consumers to obtain credit online without having to register with money-lending institutions such as banks, cooperatives and the like. However, users are required to register first, with the condition that they provide a photo ID. This raises concerns about the security of personal data protection when using e-commerce applications. Security in e-commerce platforms is one of the important factors that consumers consider when making transactions. There are potential crimes that can occur in online transactions, such as fraud, credit card hijacking, theft of personal data, storage of funds whose security is not guaranteed, and many more. Consumers' perception of risk in online transactions is higher than in traditional transactions.

The context of personal data protection is an important and relevant issue. According to the 2024 Indonesian Internet Penetration Survey Report, online fraud is the case of data security vulnerabilities that most frequently attack internet users with 32.50%, cases of data theft experienced by 20.97%, devices affected by viruses (19.31%), no can access the application (10.04%) and other cases (5.32%). However, there are still many respondents, namely 42.45%, who do not know about the cases of data security vulnerabilities they have experienced (Muhamad, 2024). In 2024, it is predicted that personal data theft will dominate (CNN Indonesia, 2024). The choice of control mechanism for disclosing personal information is an attempt to use online application systems related to privacy (Yel & Nasution, 2022). The protection of personal information is becoming increasingly important as the number of online transactions increases. Under these conditions, it is important to see what is teenagers' understanding and awareness of efforts to protect personal data in digital transactions? and what is the communication strategy to increase awareness of personal data protection in digital transactions.

THEORETICAL OVERVIEW

Attention to the protection of personal data is recognized as a human right that requires legal protection of personal data. Privacy policies emerged from the common law system, a system as a self-regulatory approach. The privacy policy is adapted to the principles of personal data protection established by national laws and regulations (Rahmawati et al., 2023). Indonesia provides legal protection for human rights as expressly stated in the 1945 Constitution. This shows that legal protection for personal data is only accommodated in sectoral regulations that have certain comprehensive laws (Yuniarti, 2019). This means that consumer protection and protection of consumers' personal data are very necessary (Priliasari, 2019). According to Law no. 27 of 2022, personal data is defined as data about natural persons who are identified or can be identified individually or combined with other information, either directly or indirectly, through electronic or non-electronic systems. Another definition of personal data is data in the form of a person's identity, codes, symbols, letters or numbers that are personal and confidential. High interaction in various transaction needs, encouraging privacy management in the digital era is very important (Saidah, 2021).

Communication that increasingly relies on technology but is not balanced with regulations can have an impact on the security of user privacy data (Hamonangan, 2023).

Users' concerns about the distribution of their personal information on social media are often demonstrated by looking at the service provisions for personal information (Aji & Utari, 2022).Communication privacy management is the main consideration when deciding to use digital interactions such as social media (Tobing, 2021). Digital literacy as a means of managing communication privacy (Yusuf et al., 2022). Solutions for protecting individual data privacy when creating, storing and processing data (Winarsih & Irwansyah, 2020).

The Indonesian government regulates the protection of personal data as regulated in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) which stipulates that individuals, including those who carry out business or e-commerce activities at home, can be categorized as personal data controllers. So that he is legally responsible for the processing of personal data that he holds and fulfills the provisions in the PDP Law. Therefore, the claim of loss from the Petitioner in Case 108/PUU-XX/2022 has actually been accommodated in Article 2 paragraph (1) of the PDP Law which stipulates that this norm applies to everyone. Law No. 11 of 2018 concerning Information and Electronic Transactions or the ITE Law and its derivative legal products, Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems. According to Law No. 8 of 1999 concerning Consumer Protection, one of the basic rights of consumers that is protected is legal certainty. In this problem, one of the legal certainties that must be protected is the confidentiality of documents. Therefore, e-commerce Shopee also applies these regulations in its services.

METHODOLOGY

The research method in this study uses a qualitative research method with a descriptive approach. Qualitative research methods focus on explanations rather than generalizations. Data collection techniques were carried out using observation, interviews and document study. In-depth interviews were conducted with generation Z informants with the criteria of routinely carrying out digital transactions for various purposes such as business, sharing activities and shopping. The criteria are intended to explore information regarding awareness of personal data protection and communication strategies to increase awareness of privacy management in digital transactions. Document studies are carried out by collecting documents related to personal data protection. The data analysis technique used uses an interactive data analysis model. Interactive data analysis techniques are an approach to qualitative data analysis that is carried out interactively and takes place continuously. This approach includes three main stages, namely data reduction, data display, and conclusion or verification. Data reduction involves breaking down, synthesizing, and looking for patterns in the data, while data display is related to presenting the data systematically, and the final stage is drawing conclusions or verification (Miles et al., 2014). This technique is used in qualitative research to understand, organize and process qualitative data in order to find certain meanings, interpretations and conclusions from all the data in the research.

RESULTS & DISCUSSION

Awareness of the importance of Communication Privacy Management

The tendency to convey shared privacy information such as name, age, family, domicile, status, as well as hobbies and personal character as an effort to manage privacy (Wahyuni et al., 2024). This condition allows various negative impacts to occur. Digital Literacy is an aspect of raising awareness regarding the protection of personal data as an effort to early detect potential misuse of personal data in digital transactions. The privacy management carried out tends to be limited. Teenagers have difficulty distinguishing between private and public boundaries. According to a 20 year old teenage informant, digital transactions are youthful and profitable. Even though you submit data in the form of address and personal identity, there is no worry that this could be misused.

> *"When I shop, I like to go online, sometimes I make a story when the goods arrive. That's often the case. If you ask me why, I'm just happy to post it, especially if someone asks, where to buy it, share the link. Think about helping people's fortunes,"* (Source: interview, 2024).

Digital interaction requires each individual to have a high level of awareness. Often individuals' understanding of the risk of personal data leakage in digital transactions is still often overlooked. Their information security when operating online or carrying out digital transactions tends to be indifferent to privacy. Teenagers have a tendency to be active on social media, by sharing personal information such as email addresses, telephone numbers, or locations openly, this condition can trigger fraud and identity theft. This data is used for various transaction actions. For example, the desire to gain recognition or popularity on social media encourages teenagers to have a tendency to open themselves up so that communication can be established. The notion of sharing a lot of information about yourself can attract attention and then followers. This condition is part of an effort to build self-existence.

Digital security risks require a different communication approach. This condition not only fosters knowledge, but also action and prevention. In Law no. 27 of 2022 Personal Data Protection as an overall effort to protect personal data in the process of personal data processing in order to guarantee the constitutional rights of personal data subjects. Meanwhile, according to article 28 G of the 1945 Constitution, personal data protection is a type of privacy protection that is directly regulated by the Constitution of the Republic of Indonesia. Privacy is also included in the realm of confidentiality and needs to be protected. Under these conditions, communication may increase individual awareness, resulting in desired behavioral changes. Efforts to increase awareness of the importance of protecting personal data in digital transactions require real efforts such as utilizing communication channels, outreach and in-depth outreach. Including regulatory restrictions that limit teenagers from carrying out transactions.

In the context of communication management, the openness of information that occurs between teenagers and the platform actually increases the quality of the information that occurs, even though personal identity gives rise to sensitive communication, the intensity of communication that occurs makes the communication that occurs open and transparent, thus allowing for reciprocity and feedback. This encourages satisfaction that arises between platforms and teenagers. Positive responses and good response speed in trusting platforms are often driven by the desires that arise from these actions.

Strategy for Managing Personal Data Protection

Personal data protection communications strategies must be carefully designed to effectively educate and persuade individuals to take the necessary actions to protect their information in digital transactions. Provide clear and easy-to-understand information about the risks of personal data leakage in digital transactions. This low awareness makes it important to protect personal data. In addition to the emerging knowledge drive, the emphasis on individual values such as privacy, and security becomes the individual's duty of control over personal information. This condition can show the consequences of disclosing personal data in digital transactions, thereby strengthening data protection efforts. Be aware that text messages, images, audio, and video are personal data so it requires awareness of the importance of this data.

Although communication establishes trust in the message conveyed, the boundaries of openness determine the level of security in the interaction. Conveying consistent messages that prioritize protection can strengthen awareness and understanding which can change user behavior in taking data protection steps after receiving information or communication messages. Customers' or users' trust in social media business communication content (Utami, 2021), often increases the desire to exchange messages in digital transactions. These conditions allow the intensity of interaction to increase. In Indonesia, personal data protection is not yet a big issue, but to avoid leaks of people's data, the government has made regulations regarding personal data protection. It is said that personal data is a matter of privacy. Where privacy is an idea of maintaining a person's integrity and dignity. The right to privacy is a person's ability to determine who has the right to hold information about them and determine how that information is used.

Even though teenagers have become aware of the protection of personal data. Users themselves must also filter themselves to differentiate between information and secrets (Okditazeini & Irwansyah, 2018). Youth speakers define personal data protection as protecting private data that cannot be shared or known by just anyone. However, the practice often ignores this privacy, reasons of trust and regulation are often the driving force for this action.

> *"If in the application or Pay Later feature you have to use your identity, we'll just follow it. If that's a requirement, if you don't meet it, you can't. I'll just follow it*," (Source: interview, 2024)

Interviewees 11 out of 13 have a high level of awareness, but they are also active users of the Pay Later feature. This means that to be able to use this feature, users are required to input some personal data such as; full name, telephone number, home address, and also photo identification (KTP). This data is data that should not be known carelessly by other people. These conditions encourage individuals' understanding of the concrete steps they can take to protect their personal data after receiving communication messages. The protective steps include; First, measuring private messages. The communication carried out tends to give rise to an attitude of evaluating personal data involved in the data protection program by ensuring that the data is not for public consumption. It encourages individuals to assess the individual's level of engagement with the communication message, such as the number of interactions with online content or participation in organized community events.

Second, the a tendency to activate additional security features and avoid sharing personal information unnecessarily. This was done considering the potential crimes that threaten users. Youth speakers are aware of the potential long-term impact of communication messages that spread personal data. This awareness and behavior is demonstrated by finding out about various information, such as feature reviews, finding out from colleagues and various potential dangers.

> "If I usually use double security, after that, to decide to share an application that provides a play later feature, look at application reviews and ask friends. If they have used it, of course, they already know the contents of the application and security", Source: Interview, 2024).

In the law that regulates the protection of personal data, it is regulated in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) which regulates that individuals, including those who carry out business activities or*e-commerce*at home can be categorized as a personal data controller. So that he is legally responsible for the processing of personal data that he holds and fulfills the provisions in the PDP Law.

Personal data protection really depends on digital platform developers. Policymaker and platform developer aiming to improve online privacy protection in Indonesia's digital landscape. In addition, the clarity of privacy policies increases the level of trust digital platforms have in user behavior (Fathni et al., 2023). Even though the registration process requires entering personal data such as identity card, address, and telephone number, several sources explained that this was not something to worry about. This condition refers to the legality of applications that have been registered in Indonesia, thereby increasing trust. Although there are concerns regarding leaks of personal data, the government's confidence in providing regulations has taken into account the worst impacts so that government supervision can encourage positive action.

> "This application is legally registered, right? So if there is a leak of personal data, we should be able to report it to the authorities.'So far I have never encountered any cases of data leakage in the application. "So in my opinion, the protection of personal data in this application is quite guaranteed, even though there are concerns, just trust the government to monitor it,"Source: Interview,2024)

The aspect of individual trust in institutions or communication sources that convey information about the protection of personal data in digital transactions has the effect of increasing awareness and sustainable behavior changes over a longer period of time. However, personal data protection policies are different for each application, leading to lower levels of trust in society. According to a teenage resource person (19), he had experienced personal data being spread, so he decided not to use the application.

> "I think in several product packages that I purchased from this application, my personal identity such as telephone numbers and addresses were not censored. And I'm a little sensitive about that."Source: Interview, 2024)

CONCLUSIONS

Fintech innovations increase digital transactions and the behavior of teenagers in digital transactions. The protection of personal data is important for teenagers in digital transactions. However, a small number actually consider the risks associated with the use of personal data in digital transactions. Effective communication strategies are implemented by teenagers by looking at a lot of reviews, reading applicable regulations, and being aware of the limits of existing information. Teenagers' awareness arises about protecting personal data when data theft occurs. Meanwhile, teenagers are confident in deciding to provide their personal identity because the transaction platform provider is recognized for its legality. The majority of teenagers are aware of the possibility of data leaks, but they still use the application for comfort and security which is guaranteed by government regulations. A platform strategy that provides comfort and security even though the user provides their identity, encourages increased confidence among teenagers. This condition makes teenagers more confident in the security of their personal information when transacting via digital platforms.

REFERENCE

Ahdiat, A. (2024). *5 E-Commerce dengan Pengunjung Terbanyak Sepanjang 2023*. Databoks.Katadata.Co.Id. https://doi.org/https://databoks.katadata.co.id/datapublish/2024/01/10/5-e-commerce-dengan-pengunjung-terbanyak-sepanjang-2023

Aji, P. W., & Utari, P. (2022). Manajemen Privasi Generasi Z Menghadapi Komersialisasi Data Pribadi di Media Sosial. *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *24*(2), 103–116. https://doi.org/https://doi.org/10.17933/iptekkom.24.2.2022.103-116

Azzani, I. K., Purwantoro, S. A., & Almubaroq, H. Z. (2023). Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *10*(7), 3556–3568. https://doi.org/http://dx.doi.org/10.31604/jips.v10i7.2023.3556-3568

CNN Indonesia. (2024). *Penipuan Online dan Pencurian Data Pribadi Diprediksi Dominasi 2024*. CNN Indonesia. https://doi.org/www.cnnindonesia.com/teknologi/20240201105221-192-1057074/penipuan-online-dan-pencurian-data-pribadi-diprediksi-dominasi-2024.

Fathni, I., Basri, B., Zulaika, S., & Dewi, R. S. (2023). Pengaruh Kebijakan Privasi, dan Tingkat Kepercayaan Pada Platform Digital terhadap Perilaku Pengguna dalam Melindungi Privasi Online di Indonesia. *Sanskara Hukum Dan HAM*, *2*(02), 118–126. https://doi.org/https://doi.org/10.58812/shh.v2i02.305

Hamonangan, H. K. (2023). Etika Dan Regulasi Industri Komunikasi: Studi Kasus Pada Regu-Lasi Privasi Data Digital Di Indonesia. *Media Bina Ilmiah*, *18*(1), 235–244.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). A methods sourcebook. In *Qualitative data analysis*. Sage Thousand Oaks.

Muhamad, N. (2024). *Ini Ragam Kasus Kerentanan Keamanan Data yang Dialami Pengguna Internet Indonesia*. Databoks.Katadata.Co.Id. https://doi.org/https://databoks.katadata.co.id/datapublish/2024/02/01/ini-ragam-kasus-kerentanan-keamanan-data-yang-dialami-pengguna-internet-indonesia

Okditazeini, V., & Irwansyah, I. (2018). Ancaman privasi dan data mining di era digital: Analisis meta-sintesis pada social networking sites (sns). *Jurnal Studi Komunikasi Dan Media*, *22*(2), 109–122. https://doi.org/https://doi.org/10.31445/jskm.2018.220202

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 1–27. https://doi.org/https://doi.org/10.33331/mhn.v49i2.44

Rahmawati, S. N. E., Hasanah, M., Rohmah, A., Pratama, R. A. P., & Anshori, M. I. (2023). Privasi dan etika dalam manajemen sumber daya manusia digital. *Lokawati: Jurnal Penelitian Manajemen Dan Inovasi Riset*, *1*(6), 1–23. https://doi.org/https://doi.org/10.61132/lokawati.v1i6.328

Saidah, M. (2021). Manajemen Privasi Komunikasi di Era Transparansi Informasi (Studi Pada Pelanggaran Privasi Dalam Hubungan Pertemanan). *INTERAKSI PERADABAN: Jurnal Komunikasi Dan Penyiaran Islam*, *1*(2). https://doi.org/https://doi.org/10.15408/interaksi.v1i2.24905

Subekti, R. (2024). *BI Proyeksikan Transaksi Digital 2024 Naik 9,11 Persen*. Ekonomi.Republika.Co.Id. https://doi.org/https://ekonomi.republika.co.id/berita/s7fvf1457/bi-proyeksikan-transaksi-digital-2024-naik-911-persen

Suhartanto, C. (2024). *Pertumbuhan Pengguna Internet Indonesia 2024 Meningkat, tapi Belum Merata*. Teknologi.Bisnis.Com. https://doi.org/https://teknologi.bisnis.com/read/20240131/101/1737117/pertumbuhan-pengguna-internet-indonesia-2024-meningkat-tapi-belum-merata.

Tobing, N. K. L. (2021). Pengaruh Media Sosial Berbasis Web 4.0 Terhadap Manajemen Privasi Komunikasi. *Jurnal Muara Ilmu Sosial, Humaniora, Dan Seni*, *5*(1), 92–103. https://doi.org/https://doi.org/10.24912/jmishumsen.v5i1.8185.2021

Utami, B. A. (2021). Komunikasi Bisnis melalui Social Media Trust guna Meningkatkan Customer Engagement pada Pixy Cosmetic. *Jurnal Riset Manajemen Komunikasi*, 46–53.

https://doi.org/https://doi.org/10.29313/jrmk.v1i1.116

Wahyuni, S., Rosalyn, C., & Jalil, A. (2024). Analisis Manajemen Privasi Komunkasi Pengguna Instagram (Studi Kasus: 3 Selebgram di Kota Makassar). *Journals of Social, Science, and Engineering*, *3*(1), 131–137.

Winarsih, W., & Irwansyah, I. (2020). Proteksi Privasi Big Data Dalam Media Sosial. *Jurnal Audience: Jurnal Ilmu Komunikasi*, *3*(1), 1–33. https://doi.org/https://doi.org/10.33633/ja.v3i1.3722

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/https://doi.org/10.59697/jik.v6i1.144

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147–154. https://doi.org/https://doi.org/10.21512/becossjournal.v1i1.6030

Yusuf, N. M., Cahyani, I. P., & Nathanael, G. K. (2022). Pengaruh Tingkat Literasi Digital Terhadap Pengelolaan Privasi Komunikasi Remaja Dalam Peer Group (Survei Pada Siswa Ma Usb Filial Man Batam). *Jurnal Ilmiah Komunikasi Makna*, *10*(2), 90–107. https://doi.org/http://dx.doi.org/10.30659/jikm.v10i2.21999