International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 07 Issue 07 July 2024

DOI: 10.47191/ijsshr/v7-i07-84**,** Impact factor- 7.876

Page No: 5358-5362

The Awareness Gap in Personal Data Privacy in Indonesia's Cyberspace

Fitriah Faisal[1], Wa Ode Zuliarti[2]
[1,2]Law Faculty, Universitas Halu Oleo, Kendari

ABSTRACT: This study discusses the protection of personal data in the context of human rights, specifically the right to privacy in Indonesia. In the digital era, personal data has become a valuable asset that drives the operations of businesses, governments, and individuals. Digital literacy plays a crucial role in the protection of personal data, equipping individuals with the knowledge and skills to manage personal information effectively and safely. Although personal data protection laws in Indonesia have been implemented, many challenges remain, including the gap in public awareness about personal data protection and the readiness of infrastructure and human resources. This study also highlights survey results showing that the awareness of Indonesians about personal data protection is still low, with many data breach incidents occurring.

KEYWORDS: Personal Data, Digital Literacy.

I. INTRODUCTION

“You have the world at your fingertips” is a phrase we might come across without fully grasping its meaning. It can imply having control over the world, but it often refers to having access to the world's information and resources, particularly through technology or other information sources. It can have a different sense and it can refer to having command of the world. Every time you use a service, buy a product online, register for email, go to your doctor, pay your taxes, or enter into any contract or service request, you have to hand over some of your personal data. Even without your knowledge, data and information about you is being generated and captured by companies and agencies that you are likely to have never knowingly interacted with (Privacy International, 2018).

Since covid 19 pandemic globally outbreak, people around the world forced towards what we call Work From Home (WFH). Over the past three years, all aspect of life has shifted online from children’s education and virtual meetings to family gatherings, shopping for necessities and administrative task. The use of social media has skyrocketed, bringing both positive and negative effects. WhatsApp is the most commonly used chat platform in the country. In 2022 the number of WhatsApp users in Indonesia is approximately 120,35 million and people spent time around 29 hours and 6 minutes per month on it (Statista, 2023). People rely on WhatsApp as daily tool to share information about school and work, receive news and updates, and exchange data. They use WhatsApp for almost everything.

Indonesia placed on ranks 3rd in the number of social media users in the Asia-Pacific region with 167 million Indonesians currently using any kind of social media platform (Statista, 2023). It`s more than half of the Indonesian population (World Bank Group, 2022) But, in 2021 there was research conducted by Microsoft regarding the digital civility index and the result stated that Indonesian netizens were the most disrespectful netizens in Southeast Asia (CfDS, 2021) and then followed by personal data breaches cases, in the first quarter of 2023, the number of data breaches in Indonesia amounted to around 89.11 thousand records and According to Surfshark Indonesia ranks third globally for data leak incidents, with 13.3 million cases in 2022. What is the cause of this? Is it a lack of understanding of how to behave on social media, a fundamental misunderstanding of what social media entails, or a general unawareness of the importance of privacy and personal data?

WhatsApp is convenient and user-friendly, making it accessible to everyone, including teachers, civil servants, and even government officials. During the pandemic, it proved invaluable by supporting online shopping, enabling home learning, and facilitating remote work. Some private companies even adopted working from cafés. This period reinforced our reliance on social media platforms like WhatsApp for daily activities, turning it into a habitual tool for sharing information and staying connected.

Even after the pandemic restrictions are lifted, this trend of conducting routines online continues. We continue to use social media to share everything, even today. Many of us may not realize that social media platforms are products of companies that monitor their services. This means they likely know what we do, share, and discuss. The problem is that Indonesian users share everything, including identity cards, family cards, driver's licenses, and even a diploma. All kinds of administrative documents are shared, and it's not just the users; some administrative officers request that you send your files via WhatsApp, citing convenience. In community life, interaction habits have shifted, with social media serving as a platform for sharing daily activities through personal accounts. For instance, people celebrate buying a new house by uploading photos along with the address. Similarly, individuals who purchase a car express their joy by sharing a photo of the vehicle, often accompanied by a proof of vehicle ownership letter that includes their personal identity.

Based on the report on the Status of Digital Literacy in Indonesia 2022, a collaborative survey by the Ministry of Communication and Information (Kominfo) with the Katadata Insight Center (KIC) (Satu Data Kominfo, 2023), At the national level The National Digital Literacy Index scored 3.54. In general. or the Digital Ethics Pillar gets a 3.68 score, The Digital Skill Pillar gets a 3,52 Score and the Digital Culture Pillar is the pillar with the highest index score: of 3.84, while the Digital Safety pillar gets the lowest index score: of 3.12 (Kata Data Insight Center, 2024). From this data, we can conclude that public knowledge regarding digital safety, including personal data security, in Indonesia is quite low.

There have been 94 cases of data leaks in Indonesia since 2019. A total of 62 cases were related to private electronic system operators (PSE) (CNN Indoensia, 2023). According to Surfshark in the third quarter of 2022, Indonesia occupies the third position as the country with the most data leak cases with 13,3 Million cases data leak cases (Surfshark, 2024). The spread of personal data of public figures by hackers known as 'Bjorka' in September 2022, became one of the big cases of data leakage in Indonesia that attracted the most public attention because Bjorka has attacked official government websites as well as those official websites of a state-owned enterprise-such customer personal data from MyPertamina, The State Electricity Company (PLN), PT. Telkom, Health Insurance Agency (BPJS), and General Election Commission (KPU)- and the worst thing is Indonesian Ministry of Communication and Informatics responded by saying “If you can, don't attack” (CNN Indonesia, 2022).

The issue extends beyond simply understanding how to use social media and protect our data. The Indonesian government also faces challenges in monitoring and safeguarding its citizens' right to personal data privacy. The state has regulated the Law on personal data protection (Law Number 27 of 2022) this law aims to increase the effectiveness in the implementation of personal data protection and of course to also protect and guarantee the basic rights of citizens related to personal data protection (MKRI, 2023). So, what is personal data and personal data protection? according to this law, personal data is data about a person that is identified or identifiable alone or in combination with other information, either directly or indirectly through electronic or non-electronic systems. Meanwhile, Personal data protection is a whole effort to protect personal data in the processing of personal data to guarantee the constitutional rights of the subject of personal data. However, we still frequently encounter news about personal data breaches these days.

II. WHAT IS PERSONAL DATA AND WHY IT IS CRUSIAL

Personal data refers to any information that relates to an identified or identifiable individual. This includes a broad range of identifiers such as names, identification numbers, location data, online identifiers, and factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person. The scope of what constitutes personal data is vast, encompassing everything from a person's IP address to their social media activity and financial information (Quinn, 2021).

Understanding personal data is crucial in the context of data privacy and security. The General Data Protection Regulation (GDPR) in the European Union, for instance, defines personal data broadly to ensure comprehensive protection of individuals' privacy rights. This regulation mandates that personal data must be processed lawfully, transparently, and for a specific purpose, and it grants individuals rights over their data, such as the right to access, correct, and delete their information (Lalit Kalra, 2023). In the age of artificial intelligence and big data, the significance of personal data extends to national security concerns. Personal data is often commodified, leading to privacy risks and potential misuse by malicious actors, including foreign governments. This underscores the need for robust data protection laws and measures to safeguard individuals' privacy and security (Kat Duffy, 2024)

Privacy and Personal Data Protection are a part of human rights. In Europe, privacy and data protection are considered two separate rights and vital components of a sustainable democracy (EDPS, 2024). Privacy is a part of human dignity and is recognized as an absolute fundamental right to a private life. We have full control of information about ourselves and the right to be let alone and is not only an individual right but also a social value. The right to privacy or private life can be found in Article 12 of the Universal Declaration of Human Rights, Article 8 of The European Convention of Human Rights, and Article 7 of The European Charter of Fundamental Rights. However, when it comes to Personal Data Protection, not every country recognizes data protection in the same way. In the United States of America, they have U.S Privacy Laws since 1974, USA recognized privacy as a part of liberty but data protection has not been put into comprehensive federal law yet. Meanwhile, China and countries in the European Union (UNCTAD, 2024) have implemented comprehensive data privacy and protection laws (Paul Andersen, 2023), followed by Japan with their Japanese Act on the Protection of Personal Information (APPI) which was first enacted in 2003 (Kiteworks. 2023).

In Indonesia Privacy and Personal data are recognized as a part of human rights more specifically the right to private life. Article 28 G paragraph 1 of the Indonesian Constitution states that every person has the right to protection of himself, his family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear of doing or not doing something which is a human right (JDIH, 2000). Referring to the Indonesian personal data protection law that protecting personal data is one of the human rights, which is part of personal self-protection rights, it is necessary to provide a legal basis to provide security for personal data. According to that, we can see that the law in Indonesia does not specifically mention privacy rights and personal data protection as two separate rights. We can conclude that in Indonesia, personal data is considered part of the right to privacy.

III. PERSONAL DATA AND DIGITAL LITERACY

In the digital age, personal data has become a valuable asset, driving the operations of businesses, governments, and individuals. As the use of digital technologies expands, so does the importance of protecting personal data. Digital literacy plays a crucial role in personal data protection, equipping individuals with the knowledge and skills to manage their personal information effectively and securely. Paul Gilster define Digital literacy as the ability to understand and use information in multiple formats from a wide range of sources when it is presented via computers. It extends beyond basic computer skills to include the critical thinking and evaluative skills necessary to use technology effectively (Paul Gilster, 1997).

There are 4 components to measuring digital literacy, namely Digital Skill, Digital Ethics, Digital Safety, and Digital Culture. Digital Skill or digital proficiency is an individual's ability to know, understand, and use hardware software, and systems digital operations in everyday life. Digital Ethics is an individual's ability to realize, exemplify, adapt, rationalize, consider, and develop digital ethical governance in everyday life. Digital Safety or digital security is the ability of the user to recognize, pattern, apply, analyze, consider, and increase awareness of personal data protection and digital security in everyday life. Digital Culture is an individual's ability to read, describe, familiarize, examine, and build national insight, the values of Pancasila and Bhinneka Tunggal Ika in everyday life, and the digitalization of culture through the use of technology (KataData, 2022).

Digital literacy enables individuals to understand how their personal data is collected, used, and shared. This awareness is crucial for making informed decisions about online activities and data sharing. The connection between personal data and digital literacy is integral to navigating the digital world safely and responsibly. Digital literacy provides the necessary skills and knowledge to protect personal data. As digital environments continue to evolve, enhancing digital literacy remains essential for safeguarding personal privacy and security.

IV. PERSONAL DATA PRIVACY AWARENESS GAP IN INDONESIAN CYBERSPACE

Based on a survey conducted by the Indonesian Ministry of Communication and Information Technology in collaboration with KIC, awareness among Indonesian citizens regarding personal data protection remains low. They survey included 10.000 respondents aged between 13 to 70 years from across 34 provinces in Indonesia who have accessed the internet. The survey revealed that 53.6% of respondents exhibit a low level of personal data protection, while 46.4% demonstrate a high level of personal data protection (Cindy Mutia Annur, 2022).

From the survey results, several key points can be described as follows.

1. Awareness Gap, the survey indicates a significant gap in awareness regarding personal data protection among Indonesian citizens. With 53.6% of respondents displaying a low level of personal data protection, it shows that more than half of the surveyed population still lacks understanding of the importance of securing their personal data. This presents a major challenge for the government and related institutions to enhance education and awareness about data privacy.
2. Age and Geographic Distribution, the survey covers a wide age range, from teenagers to the elderly, and includes respondents from all 34 provinces in Indonesia. This provides a comprehensive view of awareness levels across different demographics. However, the fact that almost half of the respondents demonstrate a high level of data protection awareness is encouraging, though there is still a need for improvement across all age groups and regions.
3. Role of Technology and Education, the low awareness level could be attributed to a lack of education and understanding about cybersecurity risks. The government and relevant institutions need to be more proactive in providing socialization and education on personal data protection, through both digital campaigns and educational programs in schools and communities.
4. Policy Implications, these survey results can serve as a foundation for the government to formulate more effective policies for protecting personal data. This might include stricter regulations, better law enforcement, and resources dedicated to education and awareness campaigns.
5. Shared Responsibility, awareness of personal data protection is not solely the responsibility of the government. Technology companies, internet service providers, and individuals also play crucial roles. Companies must be transparent in their data management practices and provide tools that help users protect their personal information.
6. Significance of Survey Results, the survey results are important as an initial indicator to measure the effectiveness of past campaigns and initiatives. They also serve as a basis for planning more targeted strategies in the future.

There is a widespread lack of knowledge among Indonesian citizens about their personal data privacy rights. Many individuals are unaware of the steps they can take to protect their data or the recourse available if their data is misused. Article 39 of Law Number 27 of 2022 mandates that personal data controllers prevent unlawful access to personal data. However, this prevention is less effective if individuals are not aware of their rights and do not recognize potential data privacy threats. The law's objectives can only be fully realized if the public is well-informed about personal data protection.

Small and medium-sized enterprises (SMEs) often struggle with compliance due to limited resources and knowledge about data protection regulations. Larger corporations may have the means but still face challenges in adapting to the new legal requirements. Article 37 requires personal data controllers to supervise all parties involved in data processing. Lack of awareness and understanding of data protection laws among businesses can lead to non-compliance, resulting in legal penalties and reputational damage. Effective enforcement of Article 38, which aims to protect data from unlawful processing, depends on businesses comprehending and implementing the necessary measures.

Government efforts to raise awareness about personal data protection have been limited and not comprehensive enough to reach the entire population. Agencies like the Directorate General of Population and Civil Registration (Ditjen Dukcapil) and the National Data Center play crucial roles but need more extensive outreach programs. Articles 27 and 39 of Law Number 27 of 2022 outline the responsibilities of personal data controllers, which include the government. Without significant government-led initiatives to increase public and business awareness, the law's implementation remains incomplete and less effective.

For instance, the Directorate General of Population and Civil Registration (Ditjen Dukcapil) under the Ministry of Home Affairs (Kemendagri) records residents' personal data for state and public benefit. Similarly, the National Data Center, part of the Ministry of Information and Communications, manages personal data in accordance with Article 27 of the presidential regulation on Electronic-Based Government Systems (SPBE). This regulation defines a Data Center as a facility for placing electronic systems and related components for data placement, storage, processing, and recovery. According to Article 27, paragraphs (4) and (5), the National Data Center serves central and regional government agencies, providing a shared and interconnected data storage solution organized by the Ministry of Communications and Informatics.

With the existence of the law on personal data protection in Indonesia, it appears that the government is trying to fulfill its role in fulfilling the right to protect personal data which is part of the right to privacy in Indonesia, more specifically the right to personal self-protection. However, there are still many problems that arise regarding personal data leaks or data breaches in Indonesia. Speak of the devil, recently the National Data Center was hit by a ransomware attack, resulting in the loss of 282 data files from various Indonesian ministries and government departments. Alarmingly, the center did not have backup data. The Indonesian Ministry of Communication and Information has yet to provide a solution. This raises the question: Who is responsible for the security of our data centers? While European countries have the GDPR (General Data Protection Regulation) for data protection (Rossana Ducato, 2020), Indonesia has its own regulations regarding personal data protection.

The implementation of Law Number 27 of 2022 on Personal Data Protection presents significant challenges, especially regarding the readiness of infrastructure and human resources. This law aims to protect personal data from unlawful processing and unauthorized access. Various institutions and organizations must build systems capable of effectively protecting personal data, which includes developing internal policies, appointing data protection officers, and training employees on proper data governance according to the regulation. However, many face difficulties due to inadequate infrastructure and insufficiently trained personnel.

In upholding human rights, the state acts as a duty bearer, with obligations to respect, protect, and fulfill these rights (Manfred Nowak, 2005). The obligation to respect requires the state to refrain from intervening in the rights of individuals except when justified by legitimate law. The obligation to fulfill mandates the state to take legislative, administrative, judicial, and practical steps necessary to ensure the implementation of human rights. Meanwhile, the obligation to protect extends to safeguarding rights from violations by both state and non-state actors (Manfred Nowak, 2003).

CONCLUSIONS

While the law provides a robust framework for personal data protection, its effective implementation requires significant improvements in infrastructure, public awareness, and enforcement mechanisms. Collaboration between the government, private sector, and public is crucial to overcoming these challenges and ensuring comprehensive data security and compliance.

Finally, what should the government do about this? **Firstly,** strengthening data protection, learning from the ransomware tragedy, where the Indonesian national data center did not have strong data protection, was the source of this problem (CNN Indonesia, 2024). The government must start getting serious about protecting the personal data of Indonesian people. Reflecting on other countries, where cases of data leaks or illegal access still occur, their government is quick to respond. **Secondly,** Collaborative Governance. Collaborative governance involves various stakeholders, including government agencies, private sector entities, non-profits, and the public, working together to achieve common goals (Ansell, C., & Gash, A., 2008). In the context of protecting personal data, collaborative governance can play a significant role in several ways such as shared responsibility, comprehensive framework, enhanced compliance, public trust and transparency, innovation and adaptation, and crisis management. In essence, if the government is unable to overcome personal data protection, then it would be a good idea to invite the private sector to work together to develop appropriate data protection methods or tools. **Lastly,** Increasing Digital Literacy is vital. Indonesia should address the lack of digital literacy, as it is linked to cybersecurity risks. Individuals without digital literacy are more vulnerable to cyber threats such as scams, phishing, and identity theft, which can lead to personal and financial harm (Hadlington. L, 2017).

Additionally, lack of digital literacy can result in reduced participation in digital culture and media, limiting cultural exchange and understanding (DiMaggio, P., & Hargittai, E., 2001). This is why people are so rude on the internet (Suler. J, 2004).

REFERENCES

1) Privacy International. 2018, A Guide for Policy Engagement on Data Protection | PART 1: Data Protection, Explained, Part 1 - Data Protection Explained | Privacy International
2) Statista. 2023, https://www.statista.com/statistics/1253240/indonesia-leading-android-social-media-apps-by-monthly-hours-used/#:~:text=In%202022%2C%20the%20number%20of,131.21%20million%20users %20by%202028.
3) Statista. 2023 https://www.statista.com/statistics/295606/social-media-mau-asia-pacific-countries/
4) WorldBankGroup.2022https://data.worldbank.org/indicator/SP.POP.TOTL?end=2022&locations=ID&start=1960&view=chart.
5) Center for Digital Society. 2021, https://cfds.fisipol.ugm.ac.id/2021/04/27/press-release-the-downfall-of-indonesian-netiquette-and-whom-to-blame-netizen-or-policy-difussion-47/
6) Satu Data Kominfo. 2023, https://databoks.katadata.co.id/datapublish/preview/2023/12/14/indeks-literasi-digital-indonesia-terus-meningkat-sampai-2023.
7) Kata Data Insight Center, 2024, https://survei.literasidigital.id/indeks-literasi-digital-nasional
8) CNN Indonesia's article "35 Data Leaks in 2023, Kominfo Admits Only Giving Recommendations and Warnings" https://www.cnnindonesia.com/technology/20230619141948-192-963776/35-kebocoran-data-2023-kominfo- admit-only-recommend-and-reprimand
9) Surfshark. 2024, https://surfshark.com/blog/data-breach-statistics-2022-q3
10) CNN Indonesia. 2024, https://www.cnnindonesia.com/teknologi/20221223042459-185-891031/pernyataan-viral-kominfo-2022-bukan-tugas-kami-jangan-nyerang
11) Mahkamah Konsititusi Republik Indonesia. 2023, https://en.mkri.id/news/details/2023-02 13/Govt:_Law_on_Personal_Data_Protection_Provides_Legal_Protection
12) Quinn. 2021, P. Research under the GDPR – a level playing field for public and private sector research?. Life Sci Soc Policy. https://doi.org/10.1186/s40504-021-00111-z
13) Lalit Kalra. 2023, Decoding the Digital Personal Data Protection Act, https://is.gd/aG8qZi
14) Kat Duffy. 2024, In The Age of AI, Personal Data Security Is National Security, https://is.gd/lKnRti
15) European Data Protection Supervisor. 2024, Data Protection, https://is.gd/wMQcl6
16) Paul Andersen. 2023, H.R. 8152 –The American Data Privacy And Protection Act: The United States' Solution For The Current "Patchwork" Of Data Privacy & Protection Laws, https://is.gd/cSxozv
17) Kiteworks. 2023, Introduction to The Japanese Act on the Protection of Personal Information (APPI) https://is.gd/CNI5XV
18) JDIH. 2000, https://jdih.komisiyudisial.go.id/upload/produk_hukum/UUD1945PerubahanKedua.pdf
19) Paul Gilster.1997,"Digital Literacy:A Conceptual Framework for Survival Skills in the Digital Era",NewYork:Wiley Computer Pub
20) KataData. 2022, Status Literasi Digital Indonesia 2022 .https://cdn1.katadata.co.id/media/microsites/litdik/ReportSurveiStatusLiterasiDigitalIndonesia2022.pdf
21) Cindy Mutia Annur. 2022, Pelindungan Data Pribadi Warga Ri Masih Tergolong Rendah, Pelindungan Data Pribadi Warga Ri Masih Tergolong Rendah (Katadata.Co.Id)
22) Rossana Ducato. 2020, Data protection, scientific research, and the role of information. Computer Law & Security Review, Vol. 37, 2020, https://doi.org/10.1016/j.clsr.2020.105412
23) Manfred Nowak. 2005, UN Covenant on Civil and Political Rights. CCPR Commentary (2nd rev. ed.). Kehl am Rhein: Engel, Pp. xxxix + 1277. ISBN: 3-88357-134-2.
24) Manfred Nowak 2003, Introduction to Human Rights Regime, Martinus Nijhoff Publishers
25) CNN Indonesia. 2024, https://www.cnnindonesia.com/teknologi/20240629082357-192-1115574/ahli-sindir-proyek-data-center-rp700-m-pakai-windows-defender
26) Ansell, C., & Gash, A. 2008, Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543-571. This article explores the theory and practice of collaborative governance, emphasizing the importance of stakeholder involvement.
27) Hadlington, L. 2017, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours." Heliyon, 3(7), e00346.
28) DiMaggio, P., & Hargittai, E. 2001, "From the 'digital divide' to 'digital inequality': Studying Internet use as penetration increases." Princeton University Center for Arts and Cultural Policy Studies, Working Paper Series (15).Suler, J. (2004). "The Online Disinhibition Effect." Cyberpsychology & Behavior, 7(3).