

THE IMPROVEMENT OF DIGITAL LITERACY TO SECURE DATA AND PRIVACY IN THE DIGITAL AGE

Francisca Romana Nanik Alfiani, Rineke Sara

Universitas Borobudur, Indonesia

Email: ciscaromana@gmail.com rineke_sara@borobudur.ac.id

Abstract

Digital literacy is essential for navigating online spaces and ensuring safe and effective communication. In today's digital era, personal data and privacy are interconnected concepts crucial for individual rights and protection in an increasingly digital world. This study aims to assess digital literacy and its impact on digital security in Indonesia. The study takes a qualitative approach using descriptive methods, to aimed to answer questions about the state of digital literacy in society and how it can be improved to prevent cybercrime and enhance digital security. The findings can guide policymakers and organizations in promoting digital literacy as a means to enhance overall security.

Keywords: digitalisation, digital literacy, data, privacy

INTRODUCTION

Digitalization has become the mainstream in the development of Indonesian society. The Ministry of Communication and Informatics launched the Indonesian Digital Society Index (IMDI), which is used to assess the development of infrastructure, skills and digital empowerment of the Indonesian people (Irhamni, 2024). The IMDI increased from 43.18 to 43.34 in 2024, reflecting significant digital growth (Yesidora, 2024). Indonesia, with a population of around 280 million, 221.56 million internet users (79.5% of the population), and, 353 million active mobile connections in 2024 (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2024). Increasing internet penetration must be balanced with digital literacy, an individual's ability to access, understand, create, communicate, and evaluate information through digital technology that can be applied in economic and social life (Kominfo, 2024). Digital literacy is needed to address the major challenges behind the many positive effects of digital technology (Falloon, 2020; Neumeyer et al., 2021; Radovanović et al., 2020). The negative effects of a lack of digital literacy are no less numerous, such as the rampant spread of fake news (hoaxes), online fraud, cyberbullying, hate speech and digital-based radicalism, which need to be monitored as they threaten national unity.

Although Law No. 27 of 2022 on Personal Data Protection and Law and Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions have been enacted, they have not been effective in curbing cybercrime or preventing data leaks. Public awareness of personal data protection and privacy needs to be raised (Haque et al., 2022; Khando et al., 2021; Murdoch, 2021). Digital literacy should be taught from an early age, with government, academia and industry working together to promote it (Polizzi, 2020; Reddy et al., 2022, 2023). Expanding internet access, especially in rural areas, remains a priority to bridge the digital divide. By improving digital literacy, the public can better combat fake news, data breaches and radicalism, while promoting positive online content and reducing cybercrime.

This research aims to assess digital literacy and its impact on digital security. The research contributes to understanding the relationship between digital literacy and digital security by identifying how varying levels of digital literacy influence individuals' ability to

recognize and respond to security threats. It informs educational programs and training initiatives aimed at enhancing digital literacy, thereby improving security practices among users. Additionally, the findings can guide policymakers and organizations in promoting digital literacy as a means to enhance overall security. The study may also develop frameworks linking digital literacy and security, raise awareness of vulnerabilities associated with low digital literacy, and emphasize the need for targeted interventions in an increasingly digital world.

RESEARCH METHOD

This research takes a qualitative approach using descriptive methods, to aims to answer questions about the state of digital literacy in society and how it can be improved to prevent cybercrime and enhance digital security in Indonesia. Secondary data was collected from sources such as Ministry of Information and Communication surveys, non-governmental organizations, the internet, journals, and literature related to digital literacy and privacy. the data was collated, compared, and analysed using qualitative analysis methods, leading to key conclusions.

RESULT AND DISCUSSION

Digitalisation

Today, we have fully entered the digital age. Digitisation refers to the shift from analogue to digital technology, driven by advances in modern technology. This shift involves the widespread use of electronic devices such as computers, smartphones and the Internet to manage, store and access information more efficiently (Rizeki, 2024). The impact of digitisation spans multiple sectors, including education, healthcare, government, business and communications, with the aim of creating a more connected, efficient and inclusive society. Key benefits of digitalisation include improved access to services and information, faster and more convenient communication, improved operational efficiency through automation, and fostering innovation. Digitalisation also opens up new economic opportunities through e-commerce and online jobs, while enhancing public participation in various aspects of life, including democratic processes and decision-making. The functions of digitalisation include automating manual processes, enabling more efficient data collection and analysis, facilitating communication and collaboration, and expanding business opportunities by reaching larger markets and developing new business models based on digital technology.

Recognising the importance of digitalisation in Indonesia, President Joko Widodo has instructed the Ministry of Communication and Information to take five key steps to accelerate the country's digital transformation. These steps include: expanding internet access; creating a strategic roadmap for the digital transformation of various sectors; integrating data systems and establishing a national data centre; promoting human resource development in the digital sector; and establishing regulations, funding schemes and budgets to support these efforts.

Digital technology is growing rapidly in Indonesia. In early 2024, Indonesia, with a population of 280 million, had 221 million internet users and 353 million active mobile connections, according to a survey by the Indonesian Internet Service Providers Association (APJII). Meanwhile, the Indonesian Digital Data Portal 2024 reported that 185.3 million people (66.5% of the population) were internet users and 139 million were active on social media (49.9% of the population) (Datareportal, 2024). There were 353.3 million active mobile connections, outnumbering the population by 126.8%. Indonesia's 278.7 million people, 58.9% lived in urban areas. Internet connection speeds improved significantly, with average mobile speeds reaching 24.53 Mbps (up 42%) and fixed internet speeds reaching 28.34 Mbps (up 16.4%). Social media usage remained strong, with platforms such as Facebook, YouTube, Instagram and TikTok seeing high engagement, although Facebook's ad

reach declined by 1.9%. While digital adoption continues to grow, challenges remain in terms of unique users and ad reach accuracy as user behaviour evolves and data collection methods improve.

According to We Are Social and Hootsuite's 2023 report (We are Social, 2023), Indonesia had a population of 276.4 million, with 212.9 million internet users (77% of the population) and 167 million active social media users (60.4%). The average time spent online per day was 7 hours and 42 minutes, with 83.2% of users seeking information online. Social media platforms were very popular, with WhatsApp being used by 92.1% of internet users, Instagram by 86.5%, Facebook by 83.8% and TikTok by 70.8%. The average time spent on social media was 3 hours and 18 minutes per day.

Despite Indonesia's rise to 45th place in the 2023 World Digital Competitiveness Index, the country still faces significant challenges with low digital literacy (IMD World Competitiveness Center, 2023). The rise of misinformation, particularly ahead of the 2024 elections, is a growing concern. Election-related hoaxes increased tenfold in 2023, with the Ministry of Communication and Information recording 98 hoaxes by October, compared to just 10 in 2022. This underscores the urgent need for improved digital literacy to safeguard democracy and national unity.

Digital Literacy

In today's digital age, digital literacy plays a vital role in navigating online spaces and ensuring safe and effective communication. With rapid technological advances and the increasing threat of cybercrime, it is important that individuals not only understand how to use digital tools, but also how to protect their personal information and engage responsibly online. In the context of Industry 4.0, digital literacy encompasses three main components: data literacy, or the understanding and analysis of large data sets (big data); technological literacy, or the effective use of digital tools for communication and information processing; and human literacy, or the understanding of diverse cultural contexts and the impact of technology on society (Lemhannas, 2024). These skills are essential for navigating in an interconnected global world and for the responsible use of digital technologies.

Digital literacy encompasses several core skills, such as social networking, trans-literacy (the ability to work across platforms), privacy management, content creation and the ability to filter information (Syaripudin et al., 2024). With the proliferation of digital devices, users need to become adept at managing their online identities, creating content, and organising and sharing it across platforms. In addition, protecting personal data is critical, especially in an era of widespread cybercrime, where threats such as phishing and hacking are becoming more common.

Digital literacy also encompasses key principles such as understanding online information, social interaction and the ability to store and curate content (Pradana, 2018). Wheeler (2012) identifies nine components of digital literacy: social networking, trans-literacy (working across platforms), privacy management, digital identity, content creation, content organisation, content re-use, information filtering and self-promotion. With multiple social media platforms such as Facebook, Instagram and WhatsApp, users need to be careful about the information they consume. Privacy is critical in the digital age as cybercrime, including phishing and hacking, is on the rise. Managing one's digital identity and navigating these platforms safely is a key aspect of digital literacy.

In simple terms, literacy refers to the ability to read and write, but in today's digital age it has evolved into digital literacy. Gilster (1997), an ICT expert, defines digital literacy as the ability to use and understand information in different formats on a computer or smartphone. This skill is as important as a driving licence. UNESCO (2018) has now expanded this

definition to include the ability to safely access, manage and create information through digital technology, which essential for employment and entrepreneurship.

The Indonesian government has launched a Digital Literacy Programme for 2020-2024, which aims to increase the digital literacy of the Indonesian population. This programme includes government electronic services such as the National Library of Indonesia, which provides access to journals, e-books and multimedia content. The e-Perpus digital library service, initiated by Kompas Gramedia, provides digital library management for schools and organisations, while Gramedia Digital offers a complete e-book application that can be accessed on smartphones and tablets. These efforts aim to improve information literacy, especially among students who are used to searching for information online. The digital literacy program carried out by the government has increased the digital literacy status in 2022 to 3.54 compared to the previous year. This is reflected in the 2022 Digital Literacy Status Report in Indonesia from the Ministry of Communication and Information. Measurements are carried out using four pillars, namely Digital Skills, Digital Ethics, Digital Security and Digital Culture. Despite the increase, the Indonesian Government still needs to carry out sustainable digital literacy development to foster a culture of literacy and information processing in the digital era.

In addition, digital literacy acts as an important shield for the user community against cybercrime. According to Brian Wright, there are ten benefits of digital literacy, including time saving: Digital literacy enables individuals to efficiently find reliable information for tasks, saving time for both users and service providers. Faster learning: Searching for terms online is quicker than using printed resources, so tasks can be completed more quickly. Cost savings: Users can easily find discounts and compare prices online. Increased security: Access to multiple sources of information helps users make informed decisions, such as when travelling abroad. Up-to-date information: Frequent updates to smartphone applications ensure users have the most up-to-date information and can verify its accuracy. Connectivity: The Internet facilitates direct communication, allowing users to stay in touch with others. Better decision-making: Digital literacy enables users to analyse and compare information, leading to more informed decisions. Job readiness: Skills in software such as Microsoft Word and Excel are essential for everyday tasks and can be learned through practice. Improved well-being: Access to a variety of online content can be enjoyable, although users need to filter out negative influences. Global impact: Thoughtful sharing of content can drive social change and have a positive impact on the world. In short, digital literacy empowers individuals to navigate the digital landscape effectively for personal and societal growth (Maulana, 2015).

Personal Data and Privacy

Every interaction with people or organizations involves the exchange of personal data, such as names, phone numbers, and addresses. While any single piece of data might not identify a person, when combined, it can constitute personally identifiable information (PII). Data is no longer considered private once anonymized, but true anonymization must be irreversible. Encrypted or de-identified data that can be re-linked to individuals remains personal data (European Commission, 2024).

Personal data refers to any information related to an identified or identifiable natural person (data subject). Under the European Union's General Data Protection Regulation (GDPR), personal data includes online identifiers like names, identification numbers, IP addresses, and location data. Context is key; information about a person's job, physical characteristics, or even political opinions can also qualify as personal data. Examples of personal data include Name and surname. Email address. Phone number. Home address. Date of birth. Race and gender. Credit card numbers. Medical records. Identification card numbers.

Cookie IDs. IP address. Location data. According to the Personal Data Protection (PDP) Law, personal data encompasses both general data (like names and addresses) and specific data (such as health or biometric data).

Personal data holds significant economic value. As Clive Humby stated, "data is the new oil," emphasizing that, like oil, data must be processed to be valuable. Companies often use personal data for targeted promotions based on users' online activities. Digital content service companies, such as those owned by Mark Zuckerberg, profit by utilizing personal data, sometimes leading to violations of privacy (Suarez-Davis, 2022). It is essential to keep personal data confidential and not share it publicly. Protecting personal data is crucial to preventing misuse, especially in the context of rising cybercrime. Examples of misuse include unauthorized credit card charges, account takeovers, and targeted scams.

Meanwhile, privacy is an abstract concept influenced by cultural and social factors, resulting in varying perceptions globally. Initially framed by Warren and Brandeis, privacy is recognized as the right to be alone and is essential for protecting human dignity and individual rights. Privacy allows individuals to control access to their information and protects against the misuse of power. It fosters dignity, freedom of association, and freedom of speech, making it a critical human rights issue today.

Data privacy refers to an individual's ability to control the communication of their personal data. Each person has the right to manage their data, including organizing, editing, and deleting it, as well as deciding how and with whom it is shared. With the rise of information technology, the importance of data privacy has increased. While services often require data collection, some platforms may overreach, compromising user privacy. Others may fail to protect collected data, leading to breaches that expose sensitive information. In summary, personal data and privacy are interconnected concepts crucial for individual rights and protection in an increasingly digital world. The types of companies that usually use personal data as a promotional tool in cyberspace are those that produce digital content services, such as Mark Zuckerberg's company with WhatsApp, Instagram, and Facebook content products. digital content to serve society's social communication relations. the profits obtained by digital content companies by using someone's data constitute a violation of personal data (Forbes, 2023).

Personal data is important to keep confidential. and it is best not to share it in the public realm or on digital platforms. protection of personal data must be conducted optimally so that potential misuse of data is not exploited by cybercrime. currently, many crimes are committed via digital platforms using personal data. misuse of online loan account registration can have an impact on people who feel they have never registered a credit card but suddenly have a credit card bill. other crimes can include the potential for accounts to be taken over, profiling for political targets or advertising on social media, hacking of service accounts, and even telemarketing purposes (Indonesia Baik, 2024).

Data Protection and Privacy Regulations

Privacy is considered a fundamental human right in many countries, and privacy laws are designed to protect this right. For individuals to participate online, they need to trust that their information will be handled carefully. Organisations use privacy practices to demonstrate to customers and users that they can be trusted with their personal information. If personal information is not kept confidential, or if people cannot control how it is used, it can be misused. Misuse of personal information can take many forms, such as fraud, harassment, or being sold to third parties without consent, often leading to unsolicited marketing. As well as harming individuals, this can damage a company's reputation and result in fines, sanctions and other legal consequences.

Data breaches continue to increase around the world, including in Indonesia, where incidents are becoming more frequent. For example, the BPJS Kesehatan data leak in 2021, which exposed the information of more than 279 million Indonesian citizens, illustrates the seriousness of the threat. In early 2023, several other major data leaks occurred, such as the Tokopedia customer data case and the National Cyber and Crypto Agency (BSSN), which also demonstrated the weakness of the data protection system.

The European Union has become a mecca for the formation of personal data protection laws. The General Data Protection Regulation (GDPR), implemented in the European Union, has had a significant impact on the formation of data protection laws in various countries (Greenleaf, 2022). Several countries such as Canada, Japan, Australia and Singapore have enacted comprehensive data protection laws. In the United States, for example, the California Consumer Privacy Act (CCPA) gives consumers the right to know what personal information is being collected and gives them control over that information, including the right to prohibit the sale of their personal information. However, the act of tracking and monitoring an individual's activities can chill freedom of expression and interfere with privacy, especially in countries with repressive governments.

Indonesia has laws and regulations in the information and communication technology (ICT) sector, including Law No. 11 of 2020 on Job Creation in the Post, Telecommunications and Broadcasting Sectors; Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions; the Personal Data Protection Law (PDP Law); Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions and its Implementing Regulations; Government Regulation No. 46 of 2021 on Post, Telecommunications and Broadcasting; Ministerial Regulation No. 5 of 2020 on Electronic System Providers for Personal Interests.

The Personal Data Protection Law (PDP Law) in Indonesia is based on Article 28G of the 1945 Constitution, which mandates the protection of citizens' personal data. The law categorises personal data into two types: specific and general. Specific personal data includes health, biometric, genetic, financial information, criminal records and children's data. General personal data includes names, gender, nationality, religion and marital status. The protection of personal data, based on privacy as a fundamental human right, ensures that individuals control the disclosure of their information.

The PDP Law reaffirms Indonesia's commitment to upholding this right. It provides legal certainty for data protection, which is essential for the preservation of human dignity, freedom and privacy, including spiritual, religious and political expression. The law gives individuals control over their data and sets out the conditions for data sharing and protection by the state. Under Articles 24, 36 and 39, data controllers must obtain consent, maintain confidentiality and prevent unauthorised access. Data processors, under Article 51, must follow the instructions of data controllers and obtain authorisation before involving third parties. As of 17 October 2024, the PDP Law is fully enforceable and allows for criminal sanctions in case of violation (Article 76). However, administrative sanctions require the establishment of a supervisory authority, which is still pending, limiting current enforcement.

Despite progress, challenges remain. Data breaches, such as those at IndiHome and other providers, show that many organisations are not yet fully compliant. Stronger enforcement and oversight are needed to address these breaches, which harm both the public and businesses. The government is expected to establish a Personal Data Protection Agency to ensure effective implementation of the PDP Act and protect citizens' personal data.

CONCLUSION

The digital age has significantly transformed access to information, benefiting various sectors such as education, business, and communications. Despite progress in digital

adoption, Indonesia faces challenges like low digital literacy, misinformation, and cybercrime, particularly during elections. To combat these issues, the country is implementing digital literacy programs aimed at enhancing skills, ethics, security, and cultural awareness among citizens. Protecting personal data is essential for safeguarding privacy rights, especially as cybercrime rises, prompting the adoption of laws like the Personal Data Protection Law. Future research should evaluate the effectiveness of these digital literacy programs in raising awareness of digital security and personal data protection, explore the link between digital literacy and cybercrime incidence, assess public understanding of the Personal Data Protection Law, and compare Indonesia's efforts with those of other countries to identify best practices in digital literacy and data protection.

REFERENCES

- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2024). *Hasil Survei Internet oleh APJII 2024*. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).
- Datareportal. (2024). *Digital 2024: Indonesia*. Datareportal.
- European Commission. (2024). *Data protection explained*. European Commission.
- Falloon, G. (2020). From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Educational Technology Research and Development*, 68(5). <https://doi.org/10.1007/s11423-020-09767-4>
- Forbes. (2023). *Meta Layoffs-Facebook Continue to Cut Cost by Culling Headcount*. Forbes.
- Gilster, P. (1997). Digital literacy. In *Seoul Heanaem*. John Wiley & Sons.
- Greenleaf, G. (2022). *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*.
- Haque, A. K. M. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems*, 39(5). <https://doi.org/10.1111/exsy.12753>
- IMD World Competitiveness Center. (2023). *World Digital Competitiveness Ranking 2023*. IMD World Competitiveness Center.
- Indonesia Baik. (2024). *Jaga Privasi Lindungi Data Pribadi*. Indonesia Baik.
- Irhamni, M. A. F. (2024). *Survei Kominfo: "Skor Indeks Masyarakat Digital Indonesia Capai 43,34 di 2024."* Goodstat.
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, 106. <https://doi.org/10.1016/j.cose.2021.102267>
- Kominfo. (2024). *Literasi Digital Indonesia*. Kominfo.
- Lemhannas. (2024). *Making Indonesia 4.0 untuk Pemimpin Indonesia Masa Depan*. Lemhannas.
- Maulana, M. (2015). *Definisi, Manfaat dan Elemen Penting Literasi Digital*. Seorang Pustakawan Blogger.
- Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*, 22(1). <https://doi.org/10.1186/s12910-021-00687-3>
- Neumeyer, X., Santos, S. C., & Morris, M. H. (2021). Overcoming barriers to technology adoption when fostering entrepreneurship among the poor: The role of technology and digital literacy. *IEEE Transactions on Engineering Management*, 68(6). <https://doi.org/10.1109/TEM.2020.2989740>
- Polizzi, G. (2020). Digital literacy and the national curriculum for England: Learning from how the experts engage with and evaluate online content. *Computers and Education*, 152. <https://doi.org/10.1016/j.compedu.2020.103859>
- Pradana, Y. (2018). Atribusi kewargaan digital dalam literasi digital. *Untirta Civic Education Journal*, 3(2).

- Radovanović, D., Holst, C., Banerjee Belur, S., Srivastava, R., Vivien Hounghonon, G., Le Quentrec, E., Miliza, J., Winkler, A. S., & Noll, J. (2020). Digital literacy key performance indicators for sustainable development. *Social Inclusion*, 8(2). <https://doi.org/10.17645/si.v8i2.2587>
- Reddy, P., Chaudhary, K., & Hussein, S. (2023). A digital literacy model to narrow the digital literacy skills gap. *Heliyon*, 9(4). <https://doi.org/10.1016/j.heliyon.2023.e14878>
- Reddy, P., Sharma, B., & Chaudhary, K. (2022). Digital literacy: a review in the South Pacific. *Journal of Computing in Higher Education*, 34(1). <https://doi.org/10.1007/s12528-021-09280-4>
- Rizeki, D. N. (2024). *Digitalisasi adalah: Pengertian, Contoh, dan Tujuan*. Digitaloka.
- Suarez-Davis, J. (2022). *Data isn't 'The New Oil' - It's Way More Valuable than That*. The Drum.
- Syaripudin, A., Ahmad, D., Ningrum, D. W., Banyumurti, I., & Magdalena, M. (2024). *Kerangka Literasi Digital*. Kemendikbud.
- UNESCO. (2018). *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2*. UNESCO.
- We are Social. (2023). *Digital 2023 October Global Statshot Report*. We Are Social.
- Wheeler, S. (2012). Digital literacies for engagement in emerging online cultures. *ELearn Center Research Paper Series*, 14–25.
- Yesidora, A. (2024). *Indeks Masyarakat Digital Indonesia 2024 Meningkat, Tertinggi di Jakarta*. Katadata.

Copyright holders:

Francisca Romana Nanik Alfiani, Rineke Sara (2024)

First publication right:

INJURY: Journal of Interdisciplinary Studies



This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International