Jurnal Yudistira: Publikasi Riset Ilmu Pendidikan dan Bahasa
Volume 3, Nomor 4, Oktober 2025
e-ISSN: 3021-7814; p-ISSN: 3021-7792, Hal. 110-123
DOI: https://doi.org/10.61132/yudistira.v3i4.2372
Available Online at: https://journal.aripi.or.id/index.php/Yudistira

Digital Literacy Analysis in Increasing Students' Privacy Awareness as an Effort to Prevent Doxing Crimes in the Social Media Era

Bambang Mudjiyanto[1], Launa[2*], M. Daffa Shilbi[3], Afkar Khaibar Alfaruqi[4]
National Research and Innovation Agency (BRIN)[1], Indonesia, Sahid University Jakarta, Indonesia[2], Al-Hikmah Islamic Collage, Indonesia[3], International Open University (IOU), Indonesia[4]

Alamat: Jl. Prof. Dr. Soepomo No. 84, Tebet Dalam, South Jakarta, 12870, Indonesia
*Korespondensi penulis: launa@usahid.ac.id**

Abstract. *This study aims to explore the significant role of digital literacy in enhancing students' awareness of privacy as a preventive measure against doxing crimes, which remain a growing threat in the era of social media. Doxing, defined as the act of deliberately disclosing private information without consent, has increasingly targeted adolescent students who are active users of digital platforms. The research adopts a qualitative methodology with a descriptive-interpretive analysis and a phenomenological approach to deeply understand students' experiences and perceptions. The findings illustrate that the level of students' understanding regarding digital privacy, risky online behaviors, and preventive actions varies considerably. Digital education and literacy are shown to be effective in equipping students with the technical skills required to secure personal data and manage privacy settings on social media. In particular, students with higher exposure to digital literacy programs demonstrate better awareness of online threats and greater competence in identifying potential risks associated with doxing practices. Nevertheless, challenges persist. Peer pressure often influences adolescents to share excessive personal information online, undermining their privacy awareness. In addition, limitations in access to resources and the practical application of privacy-protection measures hinder students from fully implementing the knowledge they acquire. These barriers highlight the need for a more systematic and continuous approach to digital education. This study emphasizes that comprehensive digital literacy initiatives should not only focus on technical abilities but also foster a strong culture of privacy awareness. By doing so, students can be empowered to make responsible digital decisions, balance social interactions with personal security, and actively contribute to building a safer digital ecosystem. Overall, the research contributes to formulating strategies aimed at reducing the prevalence of doxing crimes by strengthening digital competencies and cultivating privacy-conscious behavior among adolescents.*

Keyword: *Digital Crime, Digital Security, Doxing, Student Digital Literacy, Student Privacy Awarness.*

1. BACKGROUND

The development of information and communication technology, particularly the emergence of social media, has significantly changed the landscape of social interaction and information among users, especially students and teenagers known as Gen Z. Social media is not merely a digital communication platform but also a virtual public space—where users' identities and personal data are constantly exposed and vulnerable to cybercrime threats, such as doxing or phishing.

Simply put, doxing is the act of deliberately hacking someone's personal data without permission. Meanwhile, phishing is the act of luring potential victims into providing important information. Both can potentially harm victims, both psychologically, socially, and physically. The phenomenon of doxing not only triggers concerns among social media users but also mass panic, especially among vulnerable groups, such as students and young social media users who have not yet fully developed the awareness, technical skills, and anticipatory

Received: July 05, 2025; Revised: July 20, 2025; Accepted: August 17, 2025; Online Available: August 19, 2025

abilities needed to protect their personal data from digital crimes. Data from Komdigi (2025) indicates that Indonesia has over 212 million active social media users, equivalent to 50.2% of the total population, with an average daily usage time of 3.8 hours. However, exposure to unfiltered information and the risks of digital privacy breaches also increase alongside the growing mass adoption of social media.

At the beginning of 2025, the average age of Indonesian social media users was 30.4 years, with half of the population above that age and the other half below it. The breakdown of Indonesia's population by age group at the beginning of 2025 is as follows: 0–4 years old (7.7%); 5–12 years old (13.1%); 13–17 years old (8.4%); 18–24 years old (11.0%); 25 -34 years old (15.1%); 35-44 years old (14.5%); 45-54 years old (12.9%); 55-64 years old (9.7%); and those aged 65 and above account for 7.5% (Kemp, 2025).

According to BPS data from 2024, 39.71% of young children in Indonesia have used a mobile phone (smartphone), while 35.57% have accessed the internet. When broken down by age group, 5.88% of children under the age of 1 have already used smartphones, and 4.33% of children under the age of 1 have accessed the internet in 2024. Additionally, 37.02% of children aged 1–4 years and 58.25% of children aged 5–6 years use mobile phones, while 33.80% of children aged 1–4 years and 51.19% of those aged 5–6 years have accessed the internet. Even in underdeveloped areas, children aged 13–14 are already addicted to accessing social media. According to UNICEF data, every half second, a child somewhere in the world accesses the internet for the first time (komdigi.go.id, 2025).

Concerns about the increasing number of students in the child and adolescent categories who are active social media users are reinforced by several study findings, where awareness of privacy and personal data protection among adolescents is still suboptimal. Many adolescent students still do not understand the use of privacy features on social media platforms, thereby opening the door for doxing perpetrators to access and disseminate their personal data (Heriyanto, 2024). Although teenagers have relatively high digital literacy skills, they are still not sufficiently critical in evaluating content and filtering messages on social media. This lack of analytical skills leaves teenagers vulnerable to exposure to false information and digital manipulation, which could potentially make them victims of online scams or the spread of fake news (Silvana, 2024).

Similar to Silvanah's study (2024), according to Yanti et al. (2025), adolescent students have advanced critical thinking and information evaluation skills (>80%), but aspects of electronic security such as online privacy management and awareness of cyber threats are still

at an intermediate level (~72%). This data indicates that there are still gaps that make students vulnerable to cybercrimes such as data theft and cyberbullying. Another study revealed that 61% of high school/vocational school students have moderate digital literacy, and only 36% have high literacy. This condition shows that there are still quite a number of high school/vocational school students who have limitations in understanding and managing digital information correctly, making them vulnerable to spreading false information and becoming targets of online manipulation (Rahma et al., 2024).

A study by Virga and Astuti (2024) revealed that many teenage students lack education, literacy, and focus on digital privacy awareness, as well as understanding digital ethics, making them frequent victims of data theft and online fraud. A study by Agustin and Firdos (2024) shows that the average Indonesian teenager who uses social media lacks understanding of cybercrime modes, such as online fraud, cyberbullying, the spread of false information, and data theft. A study by Pratiwi et al. (2024) also states that digital literacy among teenagers only focuses on technical skills and entertainment, without accompanying cybersecurity education. This condition makes Indonesian teenage social media users vulnerable to cybercrime. Based on the above issues, this study aims to identify the level of privacy awareness and analyze the level of digital literacy among Indonesian teenagers who use social media in relation to the risks of doxing and digital crime threats.

2. THEORITICAL STUDY

Digital literacy is the technical ability to use information from various sources and digital devices, as well as the critical ability of users to understand risks and manage information wisely, including maintaining privacy and security of personal data in the digital space. Digital literacy includes the ability to access, evaluate, create, and communicate information using digital devices. Digital literacy is also related to ethics and security in the use of digital technology. Effective digital literacy will promote increased digital awareness among users regarding all risks and potential threats, as well as encourage protective behavior, appropriate privacy settings, and selective information sharing (Park, 2011; Rundhovde, 2013; Revillia & Irwansyah, 2020; Suhendri et al., 2021).

Meanwhile, privacy awareness is an individual's understanding and attitude regarding the urgency of protecting personal data and sensitive information from unauthorized access. In practice, privacy awareness involves the importance of anticipating potential risks and reducing the risk of privacy intrusion. Normatively, information privacy refers to an

individual's moral right to have direct or indirect control over access to: information about oneself; situations in which others can obtain information about oneself; and technologies that can be used to generate, process, or disseminate information about oneself (Setiawan, et al., 2019, p. 6).

Theoretically, there are six important elements to consider in the digital ecosystem: (1) technology skills; (2) assigning responsibilities; (3) knowledge of risks; (4) understanding exposure; (5) notion of information sensitivity, and (6) managing vulnerability. These six elements help social media users, including students, recognize various modes of digital crime, including doxing (the disclosure of personal data without permission, which can cause psychological and social harm) and phishing (Rundhovde, 2013).

Privacy awareness in the context of social media acts as a key defense against doxing. Users with low privacy awareness are more susceptible to manipulation and theft of personal data (Gathegi, 2014, p. 103). Understanding data flow and protection mechanisms is key for users to control the personal information they publish (Heriyanto, 2024). However, many studies have identified the phenomenon of the 'privacy paradox,' where despite being aware of privacy risks, users often continue to share personal data excessively due to a lack of understanding or motivation to implement protective measures (Fortes & Rita, 2016).

On the other hand, Communication Privacy Management (CPM) by Petronio and Caughlin (2006) provides an important conceptual framework for studying digital literacy and privacy awareness. According to Petronio and Caughlin's CPM theory, individuals establish rules to control the personal information they share in various social contexts, including peer groups on social media. Digital literacy acts as a medium to help individuals consciously and effectively establish these privacy rules. Quantitative research on students shows a positive relationship between digital literacy levels and communication privacy management, although the contribution of digital literacy to privacy protection is still limited due to other factors such as social influence and digital habits.

Furthermore, digital literacy also serves to shape digital social ethics among students, promote responsible use of information, and encourage respect for the privacy of others. Digital social ethics are essential in reducing data theft and the unauthorized dissemination of information, which can lead to crimes such as doxing. Digital social ethics refer to the moral principles and values that guide behavior in the digital ecosystem. This ethics encompasses how individuals interact, share information, and use digital technology ethically and

responsibly, such as considering aspects of data privacy, cybersecurity, and the impact of online interactions on mental well-being (Aini et al., 2024, p. 1521).

Continuous and comprehensive privacy and digital literacy education—covering data protection techniques, awareness of digital risks, and the development of digital character and ethics—is a preventive strategy and measure to reduce cases of doxing among students as active social media users (Swasthi et al., 2025).

3. RESEARCH METHODE

This study is based on the constructivist paradigm (qualitative, subjective, and interpretive). Qualitative studies of social construction draw their data from literature studies and social media content related to the phenomenon of doxing.

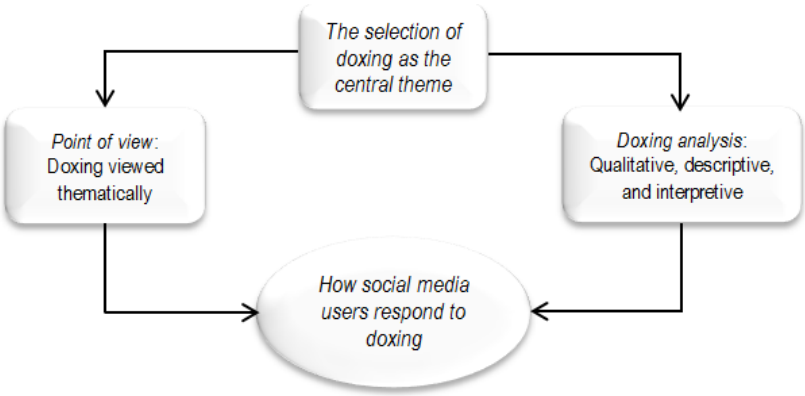

Figure 1. Qualitative Research Model with the Study Object
The Phenomenon of Doxing on Social Media
Source: Spradley, 1997, p 35

Literature studies were used to provide background information on the problem related to the phenomenon of doxing as a form of cybercrime, especially for early social media users. The data sources for this study are entirely based on secondary data, namely non-partisan observations derived from social media content and relevant qualitative data findings from literature reviews, document analyses, and supplementary tertiary sources. Non-participant observation methods were used to observe the phenomenon of doxing, which operates silently in social media spaces. Meanwhile, literature studies were used to map the phenomenon of doxing occurring in the social-actual realm.

Non-participant observation and literature studies were deliberately chosen as the analysis model to maintain objectivity and minimize research bias (Hasanah, 2017). The results of data observation (both data from mining social media content and data from literature studies) were then analyzed descriptively, interpretively, and thematically through the following four steps:

(1) data collection and organization; (2) data identification and categorization; (3) data interpretation and analysis; and (4) conclusion drawing/verification.

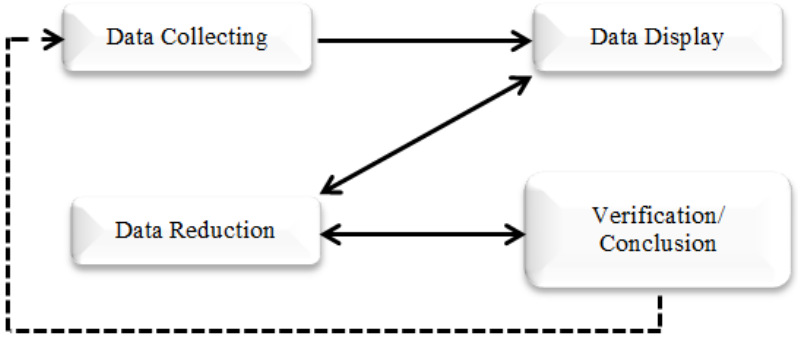

Figure 2. Qualitative Data Analysis of Miles & Huberman Model
Source: Miles & Huberman, 1992, p 16.

Table 1. Qualitative Data Analysis Stage (Miles & Huberman)

Stage	Data Collection Method	Instruments Data Source	Sample Focus	Information
Conducting a literature survey	Virtual observation and document analysis	Researchers as the main instrument, qualitative observation guide, and literature (journals, books, documents, and other sources)	Study issues related to the theme of digital literacy and privacy awareness of adolescent students	Analyzing the level of digital literacy and privacy awareness of adolescent students

Source: Data processed by resercher

4. RESULT AND DISCUSSION

Data from qualitative studies on the role of digital literacy in raising awareness of privacy among teenage students as a means of preventing doxing crimes on social media found the following:

Understanding of digital literacy still varies. Teenage students acknowledge having a basic understanding of digital literacy, particularly in the use of devices and social media platforms. However, their understanding of the concept of literacy, privacy awareness, and personal data protection remains limited and incomplete. Many students still view privacy as a technical matter (e.g., privacy settings), without fully grasping the long-term risks if personal data is leaked or disseminated unlawfully. The results of Utami's (2023) study indicate that digital literacy has a significant influence on psychological privacy management (informational privacy), physical access (accessibility privacy), and self-expression (expressive privacy) among teenagers. Furthermore, Komalasari's (2024) study also shows a significant influence

between digital literacy competence and the prevention of oversharing behavior among 70 students of the KPI Study Program at UIN Jakarta Class of 2021 on the Instagram platform who were the respondents.

Meanwhile, the results of a study by Saufa and Yusuf (2020) found that digital literacy can explain 36.30% of communication privacy management among adolescents, although social environmental factors also play a significant role. Furthermore, the study by Rullah et al. (2025) also found that targeted and inclusive communication aspects, as well as direct digital practices and continuous digital education, can enhance awareness and protective capabilities among teenage students who are novice social media users.

Limitations in Privacy Awareness Among Teenage Social Media Users. Most teenage students admit that they have not consistently practiced privacy management. Factors such as peer pressure and the habit of sharing information for the sake of popularity influence students' attitudes toward sharing personal content, which opens up opportunities for doxing risks. Students are unaware that such actions can be exploited as a means of digital crime by irresponsible parties.

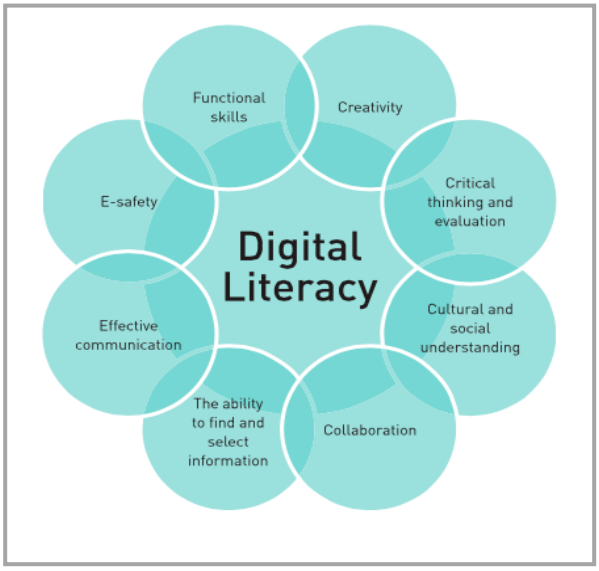

Figure 3. Digital Skills Vs Digital Literacy

Source: Green, 2017

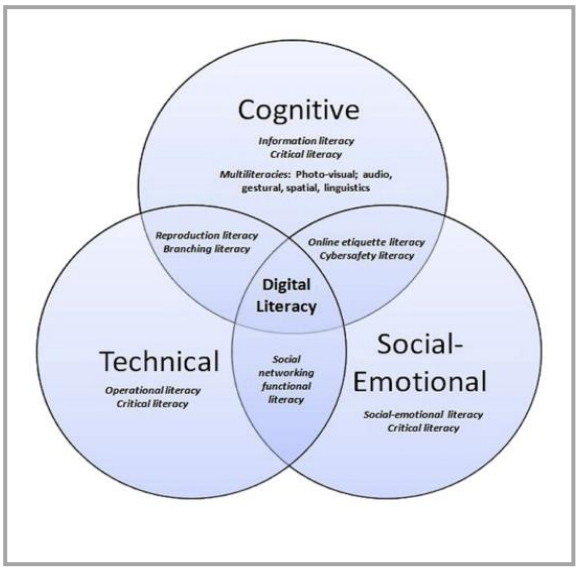

Figure 4. Digital Natives and Digital Litercy

Source: Wang Ng, 2012

A study by Pragusma (2024) shows that Indonesia's digital awareness index is still low, ranking 3.5 on a scale of 5. This makes Indonesia one of the countries with the biggest digital awareness problems in the world, including in terms of accessing, managing, and storing information. The digital divide, driven by geographical, economic, and educational quality factors—particularly among teenage students—impacts the ability to filter information and

understand the risks of cybercrime, such as online fraud and cyberbullying. Meanwhile, the quantitative study by Kangko et al. (2023) found that information security awareness influences the misuse of personal data, based on t-test results and the Coefficient of Determination, where variable X (privacy awareness) has an influence on variable Y (misuse of personal data) of 0.039 < 0.05 with a calculated t-value of 2.095 > 1.664.

Furthermore, studies by Dewi (2023) and Nopriandi (2024) show that teenagers need to continue to raise their awareness of privacy in order to protect information security (by being careful and thorough in receiving information, checking the accuracy of the information received, and safeguarding personal data). Meanwhile, among university students, privacy awareness to protect personal data needs to be continuously enhanced, particularly through educational practices and digital literacy integrated into the mandatory curriculum of higher education institutions.

Figure 5. 4 Pillars of Privacy Awareness
Source: Harshintha, 2025

Recognizing Doxing

Many parties, including teenage students who are early users of social media, are unaware of the 'signs' of doxing carried out by hackers, so it is only natural that they are also unaware when their personal data is exposed to doxing (or phishing). There are at least three phases in recognizing doxing, phishing, or forms of disinformation—whether in the form of news content (text/narrative) or in the form of images or video content—namely the initial signal phase, semantic phase, and social context phase. The findings of Alamsyah et al. (2024) from the fact-checking website show that the majority of news content, especially video content that has been subjected to doxing, phishing, or disinformation, is marked by cropping, slicing, frame cropping, wave cutting, tempo editing, vignetting, and recoloring. In addition to

obscuring the original manipulated video, this is also aimed at making the news text or video content pass the initial censorship of the content management team or YouTube.

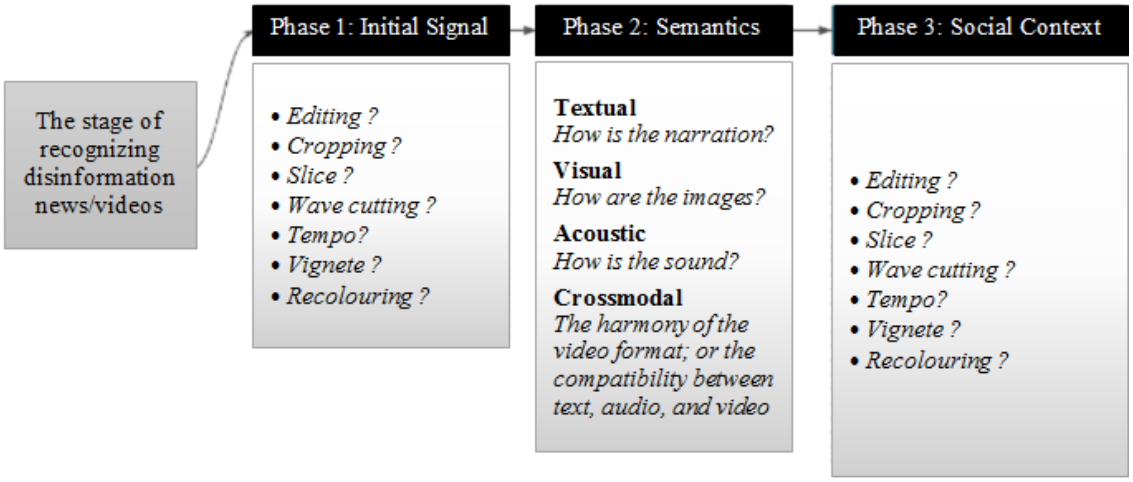

Figure 6. DisinformationWorkflow

Source: Alamsyah et al., 2024, p. 30

Figure 7. Videos Exposed to Doxing/Disinformation from the Garuda Politik Channel

Source: Alamsyah et al., 2024, p. 30

One of the disinformation videos identified by this fact check (as shown in Figure 7 above) is used as an illustration of how disinformation is recognized. According to research by Alamsyah et al. (2024, pp. 30–31), this identification process can be accessed via the website: https://turnbackhoax.id/2023/10/04/salah-dipimpin-langsung-megawati-kader-pdip-kampanyekan-anies-cak-imin/. From the initial signal phase, this video has used frame cropping techniques (red circle 1), marked by the video's lack of precision on the screen. The audio used is a narrative voiceover that partially cuts off Megawati's audio narrative or uses wave cutting techniques (red circle 2). This video has used color editing techniques (recoloring), making it darker, and vignetting, where the diagonal edges are darker (red circle 3). Furthermore, there is no semantic consistency between the narration and the video. Finally,

from a social context, it is difficult to trust an account whose videos do not reflect the actual political reality or are far removed from the real political dynamics at play.

Doxing Cases Among Students and Adolescents (2024-2025)

Doxing cases involving students and teenagers during the 2024-2025 period remain a concern for many parties due to their significant implications for mental health (particularly stress, anxiety, depression, and even serious mental disorders among victims) and digital security (protecting digital data/information from theft, unauthorized access, or destruction). Below is a statistical overview of several doxing cases throughout the years 2024-2025.

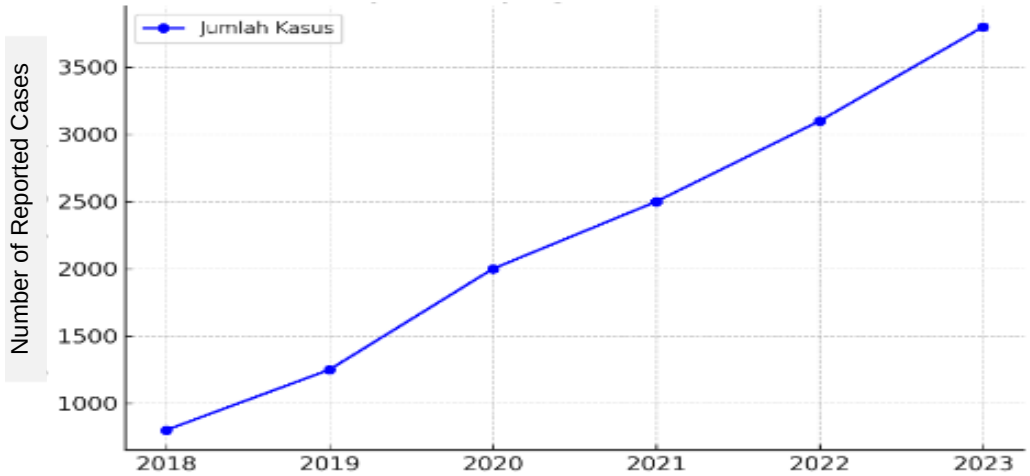

Figure 8. Trends in Cyberbullying Cases Among Adolescent Students in Indonesia (2018-2023)
Source: Alamsyah et al., 2024, p 30

Table 2. The Case of Doxing Students Who Use Social Media (2024 – 2025)

Year	City (Locus Delicti)	Description
2024	Jakarta	Cases of doxing involving students/teenagers, both as perpetrators and victims. These cases highlight the negative impact of doxing on privacy and digital security, as well as the need for more effective digital literacy among teenagers.
2024	Jakarta	Cases of fraud in the Kartu Indonesia Pintar Kuliah (KIP-K) program went viral and led to doxing of those suspected of fraud, according to information on Instagram JAGA. This action shows that good intentions must be accompanied by wise actions, and doxing can be an unintended consequence of the dissemination of personal information, according to information on Instagram JAGA.
2024	Jakarta	Another case of personal data hacking by Gnosticplayes has occurred on the Tokopedia platform. Gnosticplayes claims to have hacked 91 million Tokopedia app user data and 7 million seller data in March 2020. The leaked

		data includes: email addresses, phone numbers, dates of birth, and other personal information.
2024	Jakarta	Instagram celebrity Michelle Halim (on her Instagram Story account @michellehalim) is suspected of doxing a minor. She posted the child's face and compared it to the color of her own armpits. The child's personal data and photos were widely shared through an anonymous social media account, followed by harassment and defamation. This case highlights how vulnerable children and teenagers who use social media are to the unauthorized sharing of personal data.
2024	Cianjur	A viral case on social media involving an elementary school student who experienced physical violence and doxing spread among other students, drawing the attention of the school and local government. The school principal was involved in handling the case, which showed that doxing also occurs among elementary school children and resonates with bullying behavior in schools.
2024	Tasikmalaya	One viral case of doxing involving students was the stalking and doxing of a high school student in Tasikmalaya in 2024. This story gained widespread attention after an anonymous Twitter account posted the story of a victim who was stalked by an adult man who intimidated the victim. The post highlighted how vulnerable school students are to becoming victims of digital stalking and targets of doxing.
2025	Surabaya	There have been cases of teenagers who are active users of Instagram and TikTok becoming victims of doxing, whereby the victim's personal data is exposed and disseminated as negative content. This method of doxing is often used to intimidate, seek revenge, and humiliate targets in the virtual world.
2025	Cirebon	Local media reports in Cirebon show that there have been quite a number of cases of doxing in schools, such as the dissemination of students' personal data, accompanied by audio recordings, photos or videos, which are then shared in chat groups or on social media. Although many of these cases are not officially reported, many students are affected by trauma and severe stress.
2025	Grobogan	The case of a 14-year-old girl who was raped by six adult teenagers in October 2024. The rape occurred after the victim was invited to meet the perpetrators, whom she had known for a long time. The victim was picked up on a motorcycle and promised dinner. She was then forced into a hotel room that had been rented by the perpetrators. The incident came to light when one of the perpetrators intentionally recorded the rape on video and then shared it via WhatsApp messages.

Source: Data compiled from various sources

5. CONCLUSION AND RECOMMENDATIONS

This study highlights the crucial role of digital literacy in enhancing students' awareness of privacy risks to effectively prevent doxing crimes in the social media era. Findings indicate that higher levels of digital literacy correlate positively with better understanding and management of personal data privacy among students. However, gaps remain in students' practical knowledge of privacy settings and the behavioral aspects influenced by peer pressure and social media culture.

To address these challenges, comprehensive and continuous digital literacy education—integrating technical skills, privacy risk awareness, and ethical digital behavior—is essential. Collaboration among educators, parents, and policymakers is necessary to foster a safe and responsible online environment for students. Strengthening digital literacy will empower students to protect their digital identities, reduce vulnerability to doxing, and promote a culture of privacy-conscious social media use.

REFERENCES

Agustin, N. A., & Firdos, R. M. (2024). Studi literatur: Ancaman cybercrime di Indonesia dan pentingnya pemahaman akan fenomena kejahatan digital. *JAMASTIKA: Jurnal Mahasiswa Teknik Informatika*, *3*(1), 126–131. https://doi.org/10.35473/jamastika.v3i1.2841

Aini, F. N., et al. (2024). The role of technology and ethics in shaping humanity's digital future. *Proceeding of International Conference on Education, Society and Humanity (Third International Conference on Education, Society and Humanity)*, *2*(2), 1518–1524. https://ejournal.unuja.ac.id/index.php/icesh/article/view/10368/3957

Alamsyah, P., et al. (2024). *Jurnalisme cek fakta melawan disinformasi Pemilu 2024* (Cet. 1). Cek Fakta-AJI-Asosiasi Media Siber Indonesia.

Dewi, E. P. T. (2023). *Pengaruh kesadaran privasi remaja terhadap penyalahgunaan data pribadi dalam penggunaan media sosial Twitter* [Diploma thesis, Universitas YARSI]. Universitas YARSI Digital Library. https://digilib.yarsi.ac.id/12517/2/2.ABSTRAK.pdf

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics, 22*(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002

Gathegi, J. N. (2014). Social media networking literacy: Rebalancing sharing, privacy, and legal observance. In S. Kurbanoğlu, S. Špiranec, E. Grassian, D. Mizrachi, & R. Catts (Eds.), *Information literacy: Lifelong learning and digital citizenship in the 21st century* (pp. 101–108). Springer. https://doi.org/10.1007/978-3-319-14136-7_11

Green, C. L. (2017). Digital literacies and the skills of the digital age. In *Learning in the Digital Age*. Oklahoma State University.

https://open.library.okstate.edu/learninginthedigitalage/chapter/digital-literacies-and-the-skills-of-the-digital-age/

Harshitha. (2025). Four pillars of data privacy literacy. LinkedIn. https://www.linkedin.com/posts/adv-harshitha-reddy-b186b7303_data-privacy-literacy-activity-7346404525928284160-Jp00

Hasanah, H. (2017). Teknik-teknik observasi (sebuah alternatif metode pengumpulan data kualitatif ilmu-ilmu sosial). *At-Taqaddum*, *8*(1), 21–46. https://doi.org/10.21580/at.v8i1.1163

Kangko, D. D. (2023). Pengaruh kesadaran keamanan informasi remaja terhadap penyalahgunaan data pribadi dalam penggunaan media sosial Twitter. *JURNAL TIMES: Technology Informatics & Computer System*, *12*(2), 1–8. https://doi.org/10.51351/jtm.12.2.2023693

Kementerian Komunikasi dan Digital. (2025, February 27). Komitmen pemerintah melindungi anak di ruang digital. *Komdigi.go.id*. https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital

Kemp, S. (2025, February 25). Digital 2025: Indonesia. *DataReportal*. https://datareportal.com/reports/digital-2025-indonesia

Komalasari, E. F. (2024). *Pengaruh tingkat kompetensi literasi digital terhadap pencegahan perilaku oversharing pada mahasiswa program studi KPI UIN Jakarta angkatan 2021 di Instagram* [Skripsi, UIN Syarif Hidayatullah Jakarta]. Repository UIN Jakarta. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/83203/1/11200510000012_Emilia_Fitri_Komalasari%20(2).pdf

Miles, M. B., & Huberman, M. A. (1992). *Analisis data kualitatif*. Universitas Indonesia Press.

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, *59*(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

Nopriadi. (2024). Menjaga privasi digital: Studi tentang kesadaran mahasiswa dalam perlindungan data pribadi di media sosial. *POLYGON: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam*, *2*(6), 87–97. https://doi.org/10.62383/polygon.v2i6.297

Petronio, S., & Caughlin, J. P. (2006). Communication privacy management theory: Understanding families. In D. O. Braithwaite & L. A. Baxter (Eds.), *Engaging theories in family communication: Multiple perspectives* (pp. 35–49). Sage Publications. https://doi.org/10.4135/9781452204420.n3

Pragusma, Z. B. (2023, February 27). Rendahnya literasi digital di Indonesia. *BINUS University*. https://binus.ac.id/character-building/2023/02/rendahnya-literasi-digital-indonesia/

Pratiwi, W. T., et al. (2024). Analisis deskriptif pengaruh penggunaan TikTok terhadap literasi digital di kalangan generasi Z Indonesia. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, *4*(1), 365–374. https://doi.org/10.33005/sitasi.v4i1.872

Rahma, D. A., et al. (2024). Kemampuan literasi digital pada jenjang SMA/SMK dalam mengurangi penyebaran hoaks. *HARMONI: Jurnal Ilmu Komunikasi dan Sosial*, *2*(2), 99–108. https://doi.org/10.59581/harmoni-widyakarya.v2i2.3086

Revillia, D., & Irwansyah. (2020). Social media literacy: Millennials' perspective of security and privacy awareness. *Jurnal Penelitian Komunikasi dan Opini Publik, 24*(1), 1–15. https://doi.org/10.33299/jpkop.24.1.2375

Rullah, A. D., et al. (2025). Strategi komunikasi untuk meningkatkan literasi digital di kalangan pemuda. *Jurnal Pemberdayaan Ekonomi dan Masyarakat, 2*(1), 2–16. https://doi.org/10.47134/jpem.v2i1.568

Rundhovde, H. M. (2013). *I am not that interesting: Social media, privacy literacy, and the interplay between knowledge and experience* [Master's thesis, University of Bergen]. BORA. https://bora.uib.no/bora-xmlui/handle/1956/8582

Saufa, A. F., & Yusuf, S. (2020). Literasi privasi di sosial media: Analisis kesadaran privasi pada grup Facebook Komunitas Peduli HBV (Hepatitis B Virus) di Indonesia. *LENTERA PUSTAKA: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan, 6*(2), 119–130. https://doi.org/10.14710/lenpust.v6i2.31407

Setiawan, A. (2019). Kesadaran keamanan privasi dan masyarakat 5.0. *JABS: Journal of Accounting and Business Studies, 4*(2), 3–14. https://doi.org/10.61769/jabs.v4i2.467

Silvana, H. (2023). Literasi digital dalam produksi pesan remaja pada Instagram. *EDUTECH: Jurnal Teknologi Pendidikan, 22*(3), 311–323. https://doi.org/10.17509/e.v22i3.68971

Suhendri, D., et al. (2021). *Peran literasi digital di masa pandemi*. Cattleya Darmaya Fortuna.

Swasthi, R. A., et al. (2025). Pemberdayaan literasi digital: Edukasi siswa tentang proses data di platform media sosial. *Innovative Action for Community Empowerment, 1*(1), 88–100. https://iace.nastech.co.id/index.php/iace/article/view/1/10

Utami, E. S. N. (2023). *Pengaruh literasi digital terhadap privasi komunikasi pada remaja: Studi kuantitatif tentang pengaruh literasi digital Instagram terhadap privasi komunikasi pada remaja di Garut Kota* [Skripsi, Universitas Garut]. Repository Universitas Garut. https://repository.uniga.ac.id/file/mahasiswa/351143562.pdf

Virga, R. L., & Astuti, Y. D. (2024). Penguatan literasi digital pada remaja berbasis masjid. *MENARA RIAU: Jurnal Ilmu Pengetahuan dan Pengembangan Masyarakat Islam, 19*(1), 74–88. https://doi.org/10.24014/menara.v18i1.27173

Yanti, A. P., et al. (2025). Profil literasi digital siswa SMP pada materi perubahan lingkungan. *BIOSFER: Jurnal Biologi & Pendidikan Biologi, 10*(1), 103–111. https://journal.unpas.ac.id/index.php/biosfer/article/view/20973/13829