Lavish Opulent Education

International Journal of Social, Economic, and Business
Vol.2, No.3, 2024, pp. 165-174
Journal homepage: https://ejournal.lavishopulent.com/ojs/index.php/ijseb/index
E-ISSN: 3063-9832

Digital Literacy and Personal Data Sharing Attitudes: A Study of AI Image Generator Users Among East Java's Generation Z

Nisrina Maulida Putri [1]*, Sumardjijati [2]

[1] Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia, 22043010200@student.upnjatim.ac.id
[2] Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia, sumardjijati@gmail.com

Corresponding Author Email: 2204301200@student.upnjatim.ac.id

Received : 5 April 2026
Accepted : 27 April 2026
Published : 30 April 2026

Keywords:
Digital literacy, Personal data, Privacy attitude, Artificial Intelligence, Generation Z.

ABSTRACT

The rapid adoption of artificial intelligence image generators among Generation Z introduces significant privacy threats, particularly regarding the collection and exploitation of biometric data. This study aims to examine the correlation between digital literacy levels and personal data sharing attitudes among Generation Z artificial intelligence image generator users in East Java. A quantitative correlational method was utilized with a purposive sample of 126 active users. Data were collected through an online questionnaire utilizing a five-point Likert scale and analyzed using the Pearson Product Moment correlation. The findings reveal a strong and significant negative correlation between digital literacy and personal data sharing attitudes ($r = -0.726$, $p = 0.000$). This indicates that higher digital literacy significantly fosters a more protective and cautious attitude toward sharing personal biometric data. Furthermore, the discussion highlights a privacy paradox where users exhibit high affective anxiety toward risks like deepfakes, yet display permissive conative behaviors due to technological determinism and social trends. The study concludes that digital literacy serves as a vital cognitive capacity for managing communication privacy boundaries. The implication of this research emphasizes the necessity for educational institutions and policymakers to design digital literacy programs that go beyond technical access, focusing extensively on critical evaluation and ethical reflection to foster a secure digital ecosystem.

INTRODUCTION

The accelerating integration of Artificial Intelligence (AI) technologies into everyday digital life has fundamentally altered how individuals produce, share, and consume visual content. Among the most socially pervasive manifestations of this shift is the widespread adoption of AI image generators applications, such as Lensa AI, Midjourney, and Stable Diffusion, that allow users to create, stylize, or transform imagery through simple textual prompts or by uploading personal photographs. These platforms have achieved enormous popularity, particularly among Generation Z, driven by motivations ranging from creative self-expression and aesthetic enhancement to social media visibility and participation in viral trends.

However, beneath the surface of these engaging and seemingly innocuous applications lies a profound and largely underappreciated privacy challenge. When users upload facial photographs to an AI image generator, they are, in effect, surrendering biometric data. Unlike a password that can be changed, biometric data derived from facial geometry is permanent and uniquely identifying. Under Indonesian Law No. 27 of 2022 on Personal Data Protection, such data is explicitly classified as "specific personal data," warranting the highest level of regulatory protection. Yet the degree to which users, particularly younger digital natives, appreciate this distinction and adjust their behavior accordingly remains an open empirical question.

The stakes are demonstrably high. The phenomenon of AI-generated deepfakes has evolved from a technical curiosity into a documented social harm. Public cases involving Indonesian national football players, such as Rizky Ridho and Sandy

Walsh, who were compelled to publicly object to unauthorized AI-edited images of themselves shared by fans, illustrate that the misuse of AI image generation is not an abstract threat but an experienced reality. More disturbingly, cases have emerged on social media platforms in which AI-generated facial composites were used to produce and commercially distribute non-consensual intimate imagery, a practice that directly implicates the biometric data submitted by unsuspecting platform users.

Despite this well-documented risk landscape, empirical research suggests that privacy awareness remains alarmingly low. A 2023 Pew Research Center study found that 56% of internet users routinely provide personal data to applications without reading their privacy policies. Research in the Indonesian context has similarly documented limited understanding of digital security risks and data protection mechanisms among young users (Rafi et al., 2025; Zega, 2025). This pattern of behavior that characterized by superficial engagement with platform permissions, impulsive adoption of trending applications, and a general tolerance for data-sharing in exchange for aesthetic rewards represents what scholars have termed the "privacy paradox" by Masur (2020) a persistent gap between stated privacy concerns and actual data-sharing behaviors.

The concept of digital literacy, broadly understood as the capacity to access, analyze, evaluate, and critically reflect upon media in digital environments (Austin & Domgaard, 2024), has been proposed as a key mediating variable in this paradox. The underlying logic is that individuals who possess more refined digital literacy competencies should be better equipped to manage their privacy boundaries when engaging with AI technologies. In the context of AI image generators, digital literacy extends beyond the technical ability to operate the application. It also includes the capacity to critically evaluate the implications of uploading facial images, understand the collection and processing of biometric data, and recognize the long-term privacy risks associated with AI-generated content. Consequently, individuals with stronger digital literacy are expected to make more informed decisions before sharing personal data with AI image generation platforms. Yet empirical tests of this relationship, particularly in the context of AI image generators and biometric data among Indonesian Generation Z users, remain scarce.

This study addresses this gap by examining the correlation between digital literacy levels and personal data sharing attitudes among Generation Z AI image generator users in East Java. The theoretical framework integrates McLuhan's (1964) Technological Determinism Theory, which contextualizes AI platforms as autonomous agents that shape user behavior through environmental pressures and trend mechanisms, with Petronio's (2002) Communication Privacy Management (CPM) Theory, which conceptualizes individuals as active agents who manage dynamic "privacy boundaries" based on risk-benefit calculations. Within AI image generator platforms, Technological Determinism helps explain how algorithmic recommendations, viral visual trends, and the ease of generating AI-enhanced images encourage users to participate by uploading personal photographs. At the same time, CPM Theory explains how users negotiate the decision to disclose or withhold facial images by weighing perceived creative and social benefits against potential privacy risks. In this context, digital literacy functions as the cognitive capability that enables users to recognize these risks and regulate their privacy boundaries when interacting with AI image generation technologies. Together, these frameworks allow for a nuanced interpretation of how digital literacy functions as the cognitive instrument through which individuals navigate between technological pressure and agentic privacy management.

LITERATURE REVIEW

Digital Literacy

Digital literacy has evolved considerably from its early conceptualization as a set of basic technical competencies for navigating digital interfaces. Contemporary scholarship converges on a broader, more multidimensional understanding of the construct as encompassing the critical cognitive capacities required to engage responsibly and effectively with digital media. Austin & Domgaard's (2024) Media Literacy Theory of Change provides a particularly comprehensive operationalization, identifying four core dimensions: Access (the capacity to locate and effectively utilize diverse media), Analysis (the ability to deconstruct how media systems work and interpret their messages), Evaluation (the ability to critically assess the credibility, intent, and potential impact of media content), and Reflection/Creativity (the ability

to create media messages and reflect on their ethical implications).

This four-dimensional framework is especially pertinent in the context of AI-based platforms, where literacy demands extend beyond conventional media criticism to encompass an understanding of algorithmic operations, data economics, and the consent architectures embedded within platform design. Floridi (2024) argues that in AI ecosystems, personal data is no longer passive information but constitutes the primary "fuel" that powers and refines algorithmic models. Understanding this dynamic requires a form of analysis and evaluation that most general media literacy frameworks do not explicitly address.

The relationship between digital literacy and privacy behavior has been examined in a growing body of research. Masur (2020) demonstrated that online privacy literacy positively and significantly supports individuals' capacity for self-data protection and informational self-determination, establishing a direct empirical link between literacy competencies and protective privacy behaviors. In the AI-specific context, Liu (2025) found that AI literacy served as a critical mitigating factor against both excessive fear of and over-reliance on generative AI tools, suggesting that literacy facilitates a more balanced and reflective engagement with AI affordances. Importantly, studies have consistently found that mere awareness of risks is insufficient without deeper analytical capacity: Rafi et al. (2025) found that Indonesian millennials prioritized application enjoyment over long-term data security even when broadly aware of risks, a pattern that aligns with Masur's (2020) observation that privacy knowledge does not automatically translate into protective behavior.

Attitudes

Attitude, as a construct, is understood within social psychology as a predisposition to respond evaluatively toward an object, person, institution, or behavior (Allport, as cited in Azwar, 2022). Crucially, attitude is distinct from behavior: it reflects a mental readiness to act rather than the act itself. Azwar (2022) operationalizes attitude through the Tricomponent Model, which distinguishes between Cognitive components (beliefs and rational assessments about an object), Affective components (emotional responses and feelings toward an object), and Conative components (behavioral intentions and preparedness to act toward an object). These three components are theoretically coherent: what one believes should align with what one feels, and together these should orient behavioral intentions.

Personal data sharing attitudes, in the context of this study, refer to users' evaluative orientations toward the act of submitting biometric data to AI image generator platforms. Research on this domain has consistently documented the privacy paradox: a systematic disconnection between high levels of stated privacy concern and persistently permissive data-sharing behaviors (Masur, 2020; Rafi et al., 2025). Chesney & Citron (2019) further documented the chilling psychological effects of deepfake technology on users' sense of security, showing that fear of non-consensual facial misuse is both widespread and emotionally intense, yet it does not consistently suppress uploading behavior.

The privacy calculus model (Masur, 2020) provides a useful framework for understanding this paradox: individuals weigh perceived benefits (aesthetic enhancement, social recognition, trend participation) against perceived risks (identity theft, biometric exploitation, privacy violations) when deciding whether to share data. When benefits are immediate, concrete, and socially reinforced, and risks are abstract, temporally distant, and poorly understood, the calculus systematically favors data disclosure even among individuals who express genuine concern about privacy.

Technological Determinism Theory

Mcluhan's (1964) Technological Determinism Theory posits that technological media are not neutral conduits for human expression but active forces that reshape perception, behavior, and social norms. Encapsulated in his famous proposition that "the medium is the message," this framework foregrounds the structural properties of media over the content they carry. In the context of AI image generators, technological determinism manifests in the design architectures of these platforms, which create powerful incentive structures that systematically push users toward data disclosure. The concept of "hard determinism" describes scenarios in which these pressures so overwhelm individual agency that users effectively cede control of their data-sharing decisions to the platform's logics, while "soft determinism" acknowledges that informed, agentic individuals can resist these pressures through deliberate reflection.

Digital literacy, in this study, is theorized as the primary instrument of soft determinism: the cognitive capacity that enables users to critically evaluate and selectively resist deterministic pressures

Communication Privacy Management Theory

Petronio's (2002) Communication Privacy Management (CPM) Theory provides the primary analytical lens for understanding how individuals navigate privacy decisions in digital contexts. CPM conceptualizes privacy management through the metaphor of dynamic "privacy boundaries" that individuals actively regulate based on evolving rule systems. When information crosses a personal boundary, the recipient becomes a "co-owner" of that information, bound by implicit norms of management. In AI contexts, the act of uploading a facial photograph transfers biometric co-ownership from the user to the platform developer, a process with potentially irreversible consequences given the nature of machine learning model training.

Five core principles structure CPM's account of privacy management. Private Information Ownership establishes that individuals believe themselves to be the legitimate sole owners of their personal data. Private Information Control operationalizes this ownership as the right to determine the flow of that information. Privacy Rule Foundations describes how individuals develop rule systems for managing disclosure based on risk-benefit calculations, the stage at which digital literacy plays a foundational role by determining the sophistication of these calculations. Boundary Coordination and Co-ownership explains how shared information transitions into a co-owned relational resource, a principle directly applicable to platform data ecosystems. Finally, Privacy Turbulence describes the disruption that occurs when privacy rules are violated by co-owners, manifesting in the context of AI as fear of deepfake misuse and other non-consensual applications of biometric data.

Hypothesis

Drawing on the theoretical frameworks outlined above, this study proposes the following directional hypothesis. Based on CPM's formulation of digital literacy as the cognitive foundation for privacy rule formation, and on Technological Determinism's account of AI platforms as structurally deterministic forces that require literate resistance, it is hypothesized that there exists a significant negative correlation between digital literacy levels and personal data sharing attitudes. That is, higher digital literacy should be associated with more protective and cautious (i.e., lower) dispositions toward sharing biometric data with AI image generator platforms.

Given that this study hypothesizes a linear relationship between two continuous variables digital literacy scores and personal data sharing attitude scores the proposed relationship is tested using the Pearson Product Moment correlation, which is appropriate for examining the strength and direction of linear associations between interval-level variables.

H_a: There is a significant negative correlation between digital literacy level and personal data sharing attitudes among Generation Z AI image generator users in East Java.

METHOD

This study employed a quantitative correlational design, aimed at testing the hypothesized relationship between two psychologically measured variables: digital literacy (Variable X) and personal data sharing attitudes (Variable Y). Correlational methods are appropriate for establishing the direction and magnitude of association between constructs without manipulation of variables (Sugiyono, 2013). Statistical inference was conducted using Pearson Product Moment Correlation because both variables were measured as composite scores derived from multiple five-point Likert-scale items, which were treated as continuous variables after summation. In addition, preliminary assumption testing indicated that the data satisfied the requirements for parametric correlation analysis, including normality and linearity, making Pearson Product Moment more appropriate than non-parametric alternatives such as Spearman's rank correlation. Statistical inference was conducted using Pearson Product Moment Correlation, with all classical assumptions checked prior to analysis.

Operational Definitions and Variabel Measurement

Digital literacy (Variable X) was operationalized as the capacity to access, analyze, evaluate, and critically reflect upon AI image generator media, adapted from Austin & Domgaard's (2024) four-dimensional Media Literacy Theory of Change framework: (1) Access, basic technical competency in operating AI application features and prompting; (2) Analysis, depth of understanding of AI's machine learning mechanisms and data collection practices; (3)

Evaluation, critical capacity to assess privacy risks before granting data access; and (4) Reflection, ethical awareness of long-term digital footprint consequences. A higher score on Variable X indicates a higher and more critical level of digital literacy.

Personal data sharing attitudes (Variable Y) were operationalized following Azwar's (2022) Tricomponent Model of Attitude across three dimensions: (1) Cognitive, beliefs about the safety, benefits, and risks of submitting facial photographs to AI platforms; (2) Affective, emotional responses (comfort, anxiety, pride, fear) evoked by data-sharing contexts; and (3) Conative, behavioral intentions regarding data submission, platform permissions, and terms of service compliance. A higher score on Variable Y indicates a more permissive attitude toward sharing personal data.

Both variables were measured via a five-point Likert scale (Strongly Agree = 5; Agree = 4; Neutral = 3; Disagree = 2; Strongly Disagree = 1). Items identified as unfavorable were reverse-scored prior to analysis. The initial instrument for Variable X comprised 20 items, and for Variable Y, 15 items.

Population, Sample, and Sampling Procedure

The target population consisted of all Generation Z individuals (born between 1997 and 2012) residing in East Java who had actively used at least one AI image generator application within the preceding six months. Exact population size could not be determined due to the absence of an official sampling frame; the population was therefore treated as infinite. Using the Lemeshow formula at a 95% confidence level and a 10% margin of error, the minimum required sample size was calculated at 97 participants. To exceed this threshold, and following Roscoe's (as cited in Sugiyono, 2013) guidelines for correlational research, a final sample of 126 respondents was secured.

Participants were recruited through non-probability purposive sampling via online questionnaire distribution across multiple social media platforms (TikTok and WhatsApp) during March 2026. Eligibility was confirmed through screening questions verifying Generation Z birth year range, East Java residence, and recent AI image generator use. All 126 respondents who completed the questionnaire and met all eligibility criteria were retained for analysis.

Instrument Validity and Reliability

Prior to the main analysis, all instrument items underwent validity and reliability testing. Validity was assessed using Pearson Product Moment Correlation, with items declared valid if Sig. < 0.05. Reliability was assessed using Cronbach's Alpha coefficient, with instruments declared reliable at $\alpha \geq 0.60$ (Sugiyono, 2013). Following item-level validity testing, seven items from Variable X (X1, X2, X3, X9, X11, X13, X16) were removed due to non-significant correlation with their respective construct totals, yielding a 13-item instrument for Variable X. All 15 items of Variable Y were retained.

Table 1. Validity and Reliability Results for Both Variables

Variable	Cronbach's Alpha	Status
Digital Literacy (X)	0.724	Reliable
Personal Data Sharing Attitude (Y)	0.900	Reliable

RESULTS

Respondent Profile

Of the 126 respondents, 97 (77.0%) identified as female and 29 (23.0%) as male. This gender distribution likely reflects the higher engagement of young women with AI image generators' visual aesthetic, features such as artistic avatar creation and portrait enhancement, which are strongly associated with feminine self-presentation practices on Indonesian social media. This pattern is consistent with Mcluhan's (1964) observation that platform design affordances are not neutral but actively shape the demographics of user engagement.

Variable X Distribution

Table 2 presents the mean scores for each dimension of Variable X. The overall pattern reveals that respondents scored highest on the Reflection and Analysis dimensions, indicating strong ethical awareness and conceptual understanding of AI mechanisms, while scoring markedly lower on the Access dimension, suggesting that technical operational proficiency remains limited.

Table 2. Distribution of Digital Literacy Variable (X)

Dimension	Mean	Mean Min.	Mean Max.
Access	2.68	2.61 (X4)	2.75 (X5)
Analysis	3.83	2.63 (X10)	4.32 (X7)

Evaluation	3.20	2.67 (X14)	4.10 (X12)
Reflection	3.80	3.21 (X20)	4.51 (X17)

Source: Primary data processed (2026)

Within the Analysis dimension (mean = 3.83), 92.0% of respondents acknowledged that uploaded photographs are processed and analyzed by the AI system (X7, mean = 4.32), and 84.1% understood that AI applications collect user data for algorithmic training (X8). However, a significant proportion (57.2%) simultaneously endorsed the misconception that AI operates "magically" without recording facial data (X10, mean = 2.63), revealing an internal inconsistency that Masur (2020) characterizes as the privacy paradox at the cognitive level.

Within the Evaluation dimension (mean = 3.20), 81.7% of respondents reported considering biometric data security risks before granting gallery access (X12, mean = 4.10). Yet 54.0% acknowledged downloading viral AI applications without verifying security credentials (X14, mean = 2.67), and 50.0% reported never having considered that uploading a photograph to a free AI application could constitute a privacy threat (X15). These findings demonstrate that the capacity for risk evaluation, while present in principle, is systematically suppressed by trend pressures.

The Reflection dimension (mean = 3.80) yielded the most socially normative results in the entire study: 92.9% recognized that editing another person's photograph with AI without consent is ethically wrong (X17, mean = 4.51), and 84.1% reported consistently considering the long-term digital footprint implications of sharing visual data (X18). These strong ethical orientations suggest that Generation Z has internalized normative frameworks around others' privacy even while remaining individually vulnerable.

The Access dimension recorded the lowest overall mean (2.68), reflecting that many respondents could only use pre-built AI templates rather than composing manual prompts (X5, mean = 2.75), and frequently experienced confusion when navigating new application features (X4, mean = 2.61). This pattern is theoretically significant: insufficient operational mastery renders users more susceptible to platform determinism (Mcluhan, 1964) by limiting their capacity to navigate applications on their own terms.

Variable Y Distribution

Table 3 presents the mean scores across the three components of Variable Y, revealing a pronounced pattern consistent with the privacy paradox: high affective anxiety coexisting with moderately permissive behavioral intentions.

Table 3. Distribution of Personal Data Sharing Attitudes Variable (Y)

Component	Mean	Mean Min.	Mean Max.
Cognitive	2.86	1.82 (Y4)	3.94 (Y3)
Affective	2.63	1.79 (Y10)	3.28 (Y6)
Conative	2.66	1.61 (Y14)	3.58 (Y11)

Source: Primary data processed (2026)

The Cognitive component (mean = 2.86) exhibited notable internal contradictions. On one hand, 80.1% of respondents recognized that sharing facial photographs with AI poses significant identity theft risks (Y4, mean = 1.82), and 81.0% acknowledged the potential for third-party misuse of uploaded photographs (Y5). On the other hand, 47.7% still considered sharing facial photographs "normal and safe" (Y1), and 54.8% trusted AI developers to maintain adequate data security systems (Y2). Additionally, 75.4% expressed confidence in obtaining high-quality aesthetic results from AI processing (Y3, mean = 3.94). This simultaneous holding of contradictory beliefs typifies the cognitive structure of the privacy paradox as identified by Masur (2020).

The Affective component recorded the lowest overall mean (2.63), indicating the most protective emotional orientation. Notably, 82.6% expressed anxiety about the possibility of deepfake misuse of their uploaded photographs (Y9), and 83.3% reported fear of their faces appearing in unauthorized online content (Y10, mean = 1.79). These figures represent the strongest protective signals in the entire dataset. Yet the highest mean in this component (Y6, mean = 3.28) reflected that 50.8% of respondents felt no hesitation when AI applications requested gallery access, suggesting that even in emotionally loaded moments of data disclosure, ambient deterministic pressures soften protective responses.

The Conative component (mean = 2.66) revealed the most striking behavioral paradox of the study. While 88.1% stated their intention to immediately delete any AI application confirmed to have

experienced a data breach (Y14, mean = 1.61), and 84.2% expressed willingness to deny excessive permission requests (Y15), these reactive protective intentions coexisted with markedly permissive prospective behaviors: 60.4% admitted to immediately clicking "Agree" on terms and conditions without reading them (Y11, mean = 3.58), and 49.2% intended to continue adopting trending AI applications regardless of their privacy policies (Y13). This pattern indicates that protective conative responses are predominantly reactive and conditional, rather than proactively and systematically applied.

Normality Test

Prior to hypothesis testing, the Kolmogorov–Smirnov test confirmed that the data residuals were normally distributed, satisfying the parametric assumption required for Pearson correlation analysis.

Table 4. Kolmogorov-Smirnov Normality Test

Test	Significant Value	Status
Kolmogorov-Smirnov	0.200	Normally Dostributed

Source: Primary data processed (2026)

The significance value of 0.200 substantially exceeds the critical threshold of 0.05, confirming that the data meet the normality assumption with confidence.

Pearson Product Moment Correlation

Table 5 presents the results of the Pearson Product Moment Correlation analysis.

Table 5. Results of Pearson Product Moment Correlation

Pearson Correlation (r)	Sig. (2-tailed)	N
-0.726	0.000	126

Source: Primary data processed (2026)

The analysis yielded a Pearson correlation coefficient of r = −0.726 at a two-tailed significance level of p = 0.000. Based on Sugiyono's (2013) interpretive scale, the absolute value of |r| = 0.726 falls within the 0.60–0.799 range, indicating a strong correlation. The negative sign of r confirms that the relationship is inverse in direction. Given that Sig. (2-tailed) = 0.000 < 0.05, the null hypothesis is rejected and the alternative hypothesis (Ha) is accepted. The study concludes that there is a statistically significant, strong, negative correlation between digital literacy levels and personal data sharing attitudes among Generation Z AI image generator users in East Java: as digital literacy increases, personal data sharing attitudes become more protective and cautious.

DISCUSSION

The strong negative correlation (r = −0.726, p = 0.000) found in this study confirms the central theoretical proposition: digital literacy functions as a vital cognitive instrument for managing privacy boundaries in AI mediated communication environments. The findings extend and complement existing literature in several important ways, closely aligning with broader empirical studies. Masur (2020) established the foundational link between privacy literacy and self-protective behavior; the present study extends this finding specifically to the biometric data context of AI image generators. Liu (2025) found that AI literacy mitigated excessive dependence and unfounded anxiety, while Zega (2025) documented limited privacy security awareness among Indonesian social media users, which is consistent with this study's identification of significant knowledge gaps at the behavioral level despite widespread surface awareness.

Technological Determinism and Soft Determinism Agency

The study provides empirical evidence of technological determinism mechanisms as described by Mcluhan (1964). AI image generator platforms are not passive tools but structurally deterministic environments that reward biometric disclosure through viral aesthetics and social validation. The data highlighted that 49.2% of respondents intended to continue trying new trending AI applications regardless of privacy policies (Y13), and 50.0% felt pride when receiving social media praise for their AI-generated photos (Y8). This demonstrates how platforms are designed to provide instant social rewards, utilizing viral filters to gain community validation, which McLuhan describes as the medium autonomously forming social norms through its structure.

Despite these deterministic pressures, the research strongly supports a soft determinism perspective, proving that human agency remains significant when balanced by adequate digital literacy. The strong

ethical orientations in the reflective dimension of digital literacy act as a powerful shield. Specifically, 92.9% of respondents recognized that editing others' faces without permission is unethical (X17), and 84.1% consistently considered the long-term consequences of their digital footprint (X18). This demonstrates that when digital literacy is sufficiently developed, individuals retain the agentic capacity to resist deterministic pressures.

However, an important contribution of this study lies in its differentiation between reactive and proactive privacy protection, showing that the effectiveness of this agency is situational. The data demonstrate that Generation Z respondents are capable of strong reactive protection when confronted with demonstrated harms, such as 88.1% expressing intent to uninstall an application proven to have data leaks (Y14), but remain highly vulnerable to prospective, permissive trends, like downloading new viral apps blindly (Y13). This proves that technological determinism is most potent at the initial point of adoption. This distinction has direct implications for digital literacy program design: effective education must not only teach users what risks exist but also equip them with the capacity to project those risks concretely into the prospective moments of daily platform interaction, precisely where deterministic pressures are strongest.

Digital Literacy and Communication Privacy Management (CPM)

The findings robustly confirm Petronio's (2002) Communication Privacy Management theory, wherein individuals actively manage their privacy boundaries through rules formed by calculating a risk-benefit ratio. The research establishes that digital literacy acts as the critical cognitive capacity determining the quality and sophistication of individuals' privacy rule systems. This is most clearly illustrated by the discrepancy between analytical knowledge and cognitive belief. While 92.0% of respondents recognized that their photos are processed by AI (X7), 57.2% still held the cognitive misconception that AI operates magically without recording facial data (X10). The coexistence of accurate surface-level awareness and inaccurate deep-level understanding confirms that knowing about a risk differs fundamentally from truly understanding it and that only the latter translates into protective privacy behavior.

Furthermore, the principle of Boundary Coordination is evident in the gap between risk evaluation and actual conative action. Although 81% of respondents claimed to consider security risks before providing gallery access (X12), a staggering 60.4% admitted to directly clicking 'Agree' on terms and conditions without reading them (Y11). Within the CPM framework, the act of giving consent automatically opens the personal privacy boundary, instantly transforming the application developer into a co-owner of the biometric data. The lack of awareness regarding this permanent transition is a direct impact of suboptimal digital literacy. Consequently, while respondents anticipate Privacy Turbulence, evidenced by their high affective anxiety toward deepfakes (82.6%) and fear of data misuse (83.3%), their lack of deep literacy prevents this abstract anxiety from converting into systematic, protective conative actions. This structural gap also points to the need for complementary privacy governance and regulatory measures, including clearer platform disclosure requirements and consent architecture redesign, since reliance on informed consent mechanisms is insufficient when the population lacks the literacy competencies to make genuinely informed decisions.

The Complexity of the Tri-Component Attitude and Provacy Paradox

An analysis using Azwar's (2022) Tri-Component model reveals a complex reality that deviates from theoretical idealism, where cognitive, affective, and conative elements should align perfectly. The cognitive component displayed significant internal tension. Respondents recognized the severe risks (80.1% acknowledged identity theft danger, Y4), yet paradoxically, 54.8% simultaneously trusted the developers' security systems (Y2), and 47.7% believed sharing photos was generally safe (Y1). This incoherence is the hallmark of the privacy paradox, where users intellectually acknowledge risks but irrationally believe they will personally remain unharmed.

Affectively, fear and anxiety heavily dominated the responses. Although this emotional signal should theoretically drive protective behavior, the conative component showed a fractured response. Protective intentions were strong only in extreme, reactive

scenarios (uninstalling compromised apps or rejecting excessive camera access). However, in mundane, everyday interactions with the technology, permissive behaviors prevailed (bypassing privacy policies). This illustrates that the conative component operates selectively, becoming active only when threats are explicit and immediate, while remaining passive against abstract risks masked by convenience.

The strong negative correlation coefficient (r = -0.726) confirms that digital literacy is the crucial variable that bridges these three components coherently. Analytical understanding of AI mechanisms solidifies cognitive beliefs about real risks; reflective awareness of long-term consequences validates affective concerns; and mature risk evaluation provides the foundation for consistent, proactive conative protection. Therefore, digital literacy is a holistic capacity that empowers individuals to resist the deterministic currents of technology, maintain control over their privacy boundaries, and cultivate a highly protective data sharing attitude.

CONCLUSION

This study investigated the correlation between digital literacy levels and personal data sharing attitudes among Generation Z AI image generator users in East Java, Indonesia. The analysis of 126 respondents using Pearson Product Moment Correlation revealed a strong, statistically significant negative correlation ($r = -0.726$, $p = 0.000$), confirming the study's central hypothesis: higher digital literacy is associated with more protective and cautious attitudes toward sharing personal biometric data with AI platforms.

The findings establish digital literacy not merely as a technical skill set but as a multidimensional cognitive capacity that enables individuals to navigate the complex privacy landscape of AI-mediated environments. This capacity encompasses the ability to move from surface-level awareness of risks to a deep, mechanistic understanding of how those risks materialize, proactive privacy rule systems as conceptualized by CPM Theory. The study also identifies a significant privacy paradox: despite high affective anxiety about deepfake risks, respondents exhibited persistently permissive conative behaviors attributable to platform-generated deterministic pressures, particularly in prospective rather than reactive scenarios.

These findings carry important practical implications. Privacy protection initiatives targeting Generation Z must move beyond awareness campaigns to deeper literacy development that builds the analytical capacity to translate abstract risk knowledge into concrete protective behavior at the critical moments of platform adoption and data permission granting. Educational programs should integrate AI-specific privacy literacy modules such as covering the mechanisms of algorithmic data collection, the implications of terms-of-service agreements, and the irreversibility of biometric data disclosure into both formal and informal educational settings. Platform developers and policymakers are similarly encouraged to complement literacy based approaches with structural interventions, including consent architecture redesign and stronger biometric data governance frameworks, to address the structural asymmetries inherent in current AI platform designs.

Future research should consider employing mixed-methods approaches to more deeply examine the psychological and social mechanisms underlying the privacy paradox, particularly the conditions under which affective concern fails to translate into protective behavioral intention. Longitudinal studies tracking changes in digital literacy and privacy behavior following targeted educational interventions would further strengthen the evidence base for the causal mechanisms proposed in this study.

Author contribution

Author: Conceptualisation and Research Design, Data Collection, Methodology, Supervision, Writing Entire Paper, Conceptualisation, Data Collection and Analysis, Editing and Layouting. All Authors have read the final version of the paper.

Declaration of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to thank the anonymous referees for their helpful comments and suggestions.

References

Austin, E. W., & Domgaard, S. (2024). *The media literacy theory of change and the message*. *August*, 167–177.

Azwar, S. (2022). *Sikap Manusia: Teori dan Pengukurannya* (3rd ed.). Pustaka Pelajar.

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Floridi, L. (2024). *The Ethics of Artificial Intelligence: exacerbated problems, renewed problems, unprecedented problems*. https://doi.org/https://dx.doi.org/10.2139/ssrn.4801799

Liu, J. (2025). When Usefulness Fuels Fear: The Paradox of Generative AI Dependence and the Mitigating Role of AI Literacy. *International Journal of Human-Computer Interaction*, *0*(0), 1–22. https://doi.org/10.1080/10447318.2025.2544006

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Mcluhan, M. (1964). *Understanding Media The Extension of Man*.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.

Rafi, M., Pane, S., Wilson, E., Awfa, Q., & Karim, A. (2025). Pemahaman Keamanan Dan Perlindungan Privasi Menurut Pandangan Generasi Milenial. *Portal Riset Dan Inovasi Sistem Perangkat Lunak*, *3*(1), 39–44. https://doi.org/10.59696/prinsip.v3i1.81

Sugiyono. (2013). *Metode Penelitian Kuantitatif, Kualitatif dan R&D* (19th ed.). Penerbit Alfabeta.

Zega, F. J. (2025). Analisis Kesadaran dan Perilaku Pengguna dalam Menjaga Keamanan Informasi Pribadi Media Sosial. *Jurnal Komunikasi Digital-DIGICATION*, *1*(1).