West Science Social and Humanities Studies
Vol. 02, No. 03, March 2024, pp. 412-422

Analysis of Data Privacy Policy, Data Processing Ethics, and Technology Ethics Awareness on User Privacy Protection in West Java

Arief Budi Pratomo[1], Joko Santoso[2], Anggun Nugroho[3], Rully Fildansyah[4], Arnes Yuli Vandika[5]
[1] STIE Nusa Megarkencana
[2,3] Institut Teknologi dan Bisnis STIKOM Bali
[4] Universitas Nusa Putra
[5] Universitas Bandar Lampung

Article Info

Article history:

Received Mar, 2024
Revised Mar, 2024
Accepted Mar, 2024

Keywords:

Data Privacy Policy
Data Processing Ethics
Technological Ethics Awareness
User Privacy Protection
Quantitative Analysis

ABSTRACT

This study investigates the relationships between data privacy policy adherence, data processing ethics, technological ethics awareness, and user privacy protection in West Java, Indonesia. Utilizing a quantitative research design, data was collected through surveys administered to organizations and individual users. Structural Equation Modeling (SEM) with Partial Least Squares (PLS) analysis was employed to analyze the data. The results reveal significant positive relationships between data privacy policy adherence, data processing ethics, and technological ethics awareness with user privacy protection. The findings underscore the importance of regulatory compliance, ethical data practices, and user awareness in safeguarding user privacy. These insights provide valuable implications for policymakers, organizations, and users seeking to enhance privacy protection efforts in West Java and beyond.

Corresponding Author:

Name: Arief Budi Pratomo
Institution STIE Nusa Megarkencana
Email: budiprato@gmail.com

1. INTRODUCTION

The protection of user privacy in the dynamic context of West Java, Indonesia is a complex issue that requires attention to data privacy policy compliance, data processing ethics, and technology ethics awareness. The widespread use of digital technologies has raised concerns about the collection, processing, and utilization of personal data by organizations and platforms. These concerns are related to privacy, transparency, and accountability [1]. Privacy in computer ethics is crucial and involves ethical considerations such as consent, transparency, and data protection [2]. The high number of digital audiences in Indonesia has led to increased use of digital services and changes in people's lifestyles, highlighting the need for proficient ethical understanding and digital literacy [3]. The impact of technological advancements and digital activities on privacy rights is a global issue, and privacy rights are protected by the 1945 Constitution [4]. To address these challenges, robust policies and practices are needed to ensure the effective protection of data rights and the responsible and ethical use of technology [5].

The emergence of the internet and digital platforms has generated enormous amounts of personal data, raising concerns about privacy and data protection [6], [7]. The use of data-driven technologies such as artificial intelligence and machine learning further amplifies these concerns [8]. The protection of personal data is critical due to the potential for misuse or unauthorised access to this data [9]. The article by Kim suggests adopting a Complex Adaptive System model to handle personal data classification and reduce failures in data protection [10]. The study by Wiefling et al. focuses on the challenges faced by digital ecosystem platform providers in implementing data protection requirements. The article by Spitsyna and Simonova discusses the need for legal regulation and protection of personal data in the digital environment.

In response to data privacy challenges, governments, regulatory bodies, and industry stakeholders have established comprehensive data privacy policies to protect user information and ensure responsible data management. These policies outline the rights and responsibilities of organizations regarding the collection, storage, processing, and sharing of personal data. Adherence to these policies fosters trust between users and organizations and reduces the risk of privacy breaches and data misuse [11]–[14]. These policies aim to maximize the benefits of data openness while protecting the rights of individuals and organizations and taking into account legitimate interests and public policy objectives [15]. They promote ethical data practices, such as minimizing harm, distributing benefits and burdens fairly, and respecting autonomy, transparency, accountability, and inclusion. Compliance with data privacy policies is essential for organizations to avoid penalties, reputational damage, and stakeholder harm.

This research endeavors to elucidate the complex dynamics underpinning user privacy protection in West Java, Indonesia, through a quantitative analysis employing survey methods. The primary objectives of this study include assessing the level of adherence to data privacy policies among organizations, examining the ethical considerations in data processing practices, and investigating the awareness of technological ethics among users. By gauging the extent of compliance with established data privacy regulations and guidelines, the research aims to identify potential gaps or areas for improvement in policy implementation and enforcement. Moreover, it seeks to explore the ethical frameworks guiding data processing activities, highlighting practices that uphold principles of fairness, transparency, and accountability. Additionally, by assessing users' knowledge of technological ethics, the study aims to gauge the efficacy of existing education and awareness initiatives and identify opportunities for enhancing user empowerment and advocacy in West Java

2. LITERATURE REVIEW

2.1 Data Privacy Policy

Data privacy policies are essential for governing the collection, use, and protection of personal data by organizations, upholding individuals' privacy rights, and fostering trust in data-driven environments. These policies outline principles, rules, and procedures that organizations must adhere to to ensure the privacy and security of personal data. They address issues such as data access requirements, data preservation and stewardship, standards and compliance mechanisms, data security, privacy and ethical concerns, and data flows. Adherence to these policies is crucial for organizations to effectively manage and protect personal data, especially in the face of increasing technological advancements and cyber threats. By implementing and following data privacy policies, organizations can create a secure environment and promote ethical data practices [12], [16], [17].

2.2 Data Processing Ethics

Ethical considerations in data processing revolve around fairness, transparency, accountability, and respect for individuals' autonomy and rights. Ethical lapses in data processing, such as unauthorized data collection, lack of transparency, and algorithmic bias, can lead to adverse consequences, including privacy breaches and discrimination [12], [18]. To address these ethical concerns, several solutions have been proposed, including the development of ethical guidelines, increased transparency and accountability, and the use of diverse and representative datasets [19]. Additionally, bottom-up models such as data trusts and data cooperatives, solidarity as a touchstone principle, and proactive research ethics processes and committees have emerged as promising innovations in data governance [20]. It is important to have flexible and sustained ethical oversight, and to act proactively instead of reactively, adapting best practices to the local setting and improving them over time [21].

2.3 Technological Ethics Awareness

Educating users about technological ethics is crucial for empowering them to make informed decisions and advocate for their privacy rights. This includes understanding the ethical implications of technology use, such as privacy risks, algorithmic bias, and digital rights. Users need to be aware of the potential threats to their personal information and the importance of protecting their data privacy. They should also be knowledgeable about the ethical considerations surrounding the use of artificial intelligence (AI) technology, particularly in the field of education. The widespread use of AI in education raises concerns about student data privacy, and it is essential to address these ethical risks and ensure the security of student personal information [2], [22]

2.4 User Privacy Protection

User privacy protection encompasses a range of measures aimed at safeguarding individuals' personal information from unauthorized access, misuse, or disclosure. Various methods and systems have been proposed to address this issue. One approach involves the use of an end-user privacy protection system that allows users to set time durations for application access to mobile phone hardware components. When the permitted time duration expires, the system disconnects the hardware components [23]. Another method focuses on the protection of users' personal information in the context of short videos. This includes increasing user awareness of personal privacy protection and strengthening the protection of users' personal information through permissions, protocol security, and industry self-discipline [24]. Additionally, a semantically grounded method has been proposed to generate fake queries that distort users' real profiles, offering more control and efficiency in protecting user privacy [25]. Furthermore, a user privacy protection method involves hiding privacy information associated with an application account if the user is not the corresponding user, thereby avoiding privacy leakage and improving the safety of user privacy information [23]. Lastly, a dynamic iteration fast gradient-based method has been developed to rapidly and effectively hide user information, thereby protecting user privacy [26].

3. METHODS

3.1 Research Design

This study adopts a quantitative research design to systematically examine the variables of interest and their interrelationships. Specifically, we utilize survey methods to collect data from a sample of organizations and individual users in West Java. Surveys offer a structured approach for gathering empirical data and allow for the quantification of variables, facilitating statistical analysis (Bryman, 2016). The research design enables us to assess the levels of data privacy policy adherence, ethical considerations in data processing, technological ethics awareness, and user privacy protection, as well as examine their associations.

3.2 Sampling Strategy

The sampling frame comprises organizations operating across various sectors in West Java and a diverse sample of individual users residing in the region. Given the geographical and demographic diversity of West Java, a stratified sampling technique will be employed to ensure representation from different sectors and population groups. The sample size is estimated to be 120, with approximately 60 organizations and 60 individual users.

3.3 Data Collection

Data will be collected through structured surveys administered to representatives of organizations and individual users. The survey instruments will be designed to capture information on:

Adherence to data privacy policies, including the implementation of privacy protection measures and compliance with regulatory requirements.

Ethical considerations in data processing practices, such as transparency, accountability, and fairness.

Technological ethics awareness among users, including knowledge of privacy risks, digital rights, and ethical use of technology.

User perceptions of privacy protection mechanisms and their effectiveness in safeguarding personal information.

Surveys will be distributed electronically via email and online survey platforms, ensuring ease of access for participants. Participants will be assured of the confidentiality and anonymity of their responses, and informed consent will be obtained prior to survey completion.

3.4 Data Analysis

The collected data will undergo analysis utilizing Structural Equation Modeling (SEM) with Partial Least Squares (PLS) 3, a robust statistical technique renowned for its capability to examine intricate relationships between latent variables and observed indicators (Hair et al., 2019). This method facilitates simultaneous scrutiny of multiple variables and allows for hypothesis testing and model evaluation. The data analysis process comprises several key steps: firstly, data cleaning and preparation will ensure the accuracy and consistency of the collected survey data. Subsequently, the reliability and validity of the measurement model will be assessed to ensure the quality of indicators measuring latent constructs. Following this, the relationships between latent variables will be scrutinized using SEM-PLS, allowing for the identification of direct and indirect effects. Moreover, the goodness-of-fit of the structural model will be evaluated, and hypotheses regarding variable relationships will be rigorously tested. Finally, the results of the SEM-PLS analysis will be interpreted to elucidate the intricate connections between data privacy policy adherence, data processing ethics, technological ethics awareness, and user privacy protection in West Java.

4. RESULT AND DISCUSSION

4.1 Demographic Sample

The demographic sample offers insights into the characteristics of the study participants, reflecting a relatively balanced distribution across gender, with 58.3% male and 41.7% female respondents. Age-wise, the majority fall within the 26-35 years bracket (33.3%), followed by the 18-25 years and 36-45 years groups, each comprising 25.0% of the sample, with the remaining 20.8% aged above

45 years. Educationally, half hold a Bachelor's degree (50.0%), followed by Master's degree holders (25.0%) and those with a High School diploma or below (16.7%), while a smaller proportion possess a Doctoral degree (8.3%). Occupationally, the sample encompasses a diverse mix including students (33.3%), employees (41.7%), entrepreneurs (16.7%), and others (8.3%), showcasing a broad range of perspectives. Moreover, organizations represented in the sample span various sectors, with Information Technology (33.3%) and Finance (25.0%) being predominant, while Healthcare, Manufacturing, and Other sectors are also represented, albeit to a lesser extent.

4.2 Measurement Model Evaluation

The measurement model evaluation involves assessing the reliability and validity of the indicators used to measure latent constructs. In this section, we discuss the loading factors, Cronbach's alpha, composite reliability, and average variance extracted (AVE) for each latent variable in the measurement model.

Table 1. Measurement Model

Variable	Code	Loading Factor	Cronbach's Alpha	Composite Reliability	Average Variant Extracted
Data Privacy Policy	DPP.1	0.890	0.812	0.888	0.727
	DPP.2	0.893			
	DPP.3	0.769			
Data Processing Ethics	DPE.1	0.752	0.811	0.882	0.715
	DPE.2	0.924			
	DPE.3	0.852			
Technology Ethics Awareness	TEA.1	0.785	0.762	0.855	0.664
	TEA.2	0.818			
	TEA.3	0.840			
User Privacy Protection	UPP.1	0.908	0.797	0.881	0.714
	UPP.2	0.875			
	UPP.3	0.741			

Source: Data Processing Results (2024)

The evaluation of various constructs within the study reveals promising results. For Data Privacy Policy (DPP), substantial loading factors ranging from 0.769 to 0.893 underscore a strong relationship between observed indicators and the latent construct. Cronbach's alpha coefficient of 0.812 and a composite reliability of 0.888 signify good internal consistency reliability and high reliability in measurement, respectively, while the Average Variance Extracted (AVE) of 0.727 surpasses the recommended threshold, confirming convergent validity. Similarly, Data Processing Ethics (DPE) and Technological Ethics Awareness (TEA) exhibit robust loading factors, internal consistency reliability, and convergent validity. Despite TEA's AVE slightly below the threshold at 0.664, it still indicates convergent validity. Moreover, User Privacy Protection (UPP) demonstrates strong loading factors, internal consistency reliability, and convergent validity, with an AVE of 0.714 exceeding the recommended threshold. These findings collectively underscore the reliability and validity of the constructs under investigation, providing a solid foundation for the subsequent analysis of user privacy protection dynamics.

4.3 Discriminant Validity Analysis

Discriminant validity analysis assesses the extent to which each latent construct is distinct from other constructs in the measurement model. In this section, we discuss the discriminant validity of the constructs of Data Privacy Policy, Data Processing Ethics, Technological Ethics Awareness, and User Privacy Protection based on the correlation matrix provided.

Table 2. Discriminant Validity

	Data Privacy Policy	Data Processing Ethics	Technology Ethics Awareness	User Privacy Protection
Data Privacy Policy	0.853			
Data Processing Ethics	0.484	0.846		
Technology Ethics Awareness	0.221	0.242	0.815	
User Privacy Protection	0.326	0.247	0.566	0.845

Source: Data Processing Results (2024)

The assessment of discriminant validity across constructs reveals promising results. For Data Privacy Policy (DPP), correlations with Data Processing Ethics, Technological Ethics Awareness, and User Privacy Protection are 0.484, 0.221, and 0.326, respectively, all lower than the square root of DPP's AVE (0.853), affirming discriminant validity. Similarly, Data Processing Ethics (DPE) exhibits correlations of 0.326, 0.242, and 0.247 with Data Privacy Policy, Technological Ethics Awareness, and User Privacy Protection, respectively, all lower than the square root of DPE's AVE (0.846), indicating discriminant validity. Technological Ethics Awareness (TEA) demonstrates correlations of 0.221, 0.242, and 0.566 with Data Privacy Policy, Data Processing Ethics, and User Privacy Protection, respectively, all lower than the square root of TEA's AVE (0.815), supporting discriminant validity. Furthermore, User Privacy Protection (UPP) showcases correlations of 0.326, 0.247, and 0.566 with Data Privacy Policy, Data Processing Ethics, and Technological Ethics Awareness, respectively, all lower than the square root of UPP's AVE (0.845), confirming discriminant validity across constructs. These findings collectively reinforce the distinctiveness of each construct, providing confidence in the validity of the study's measures.

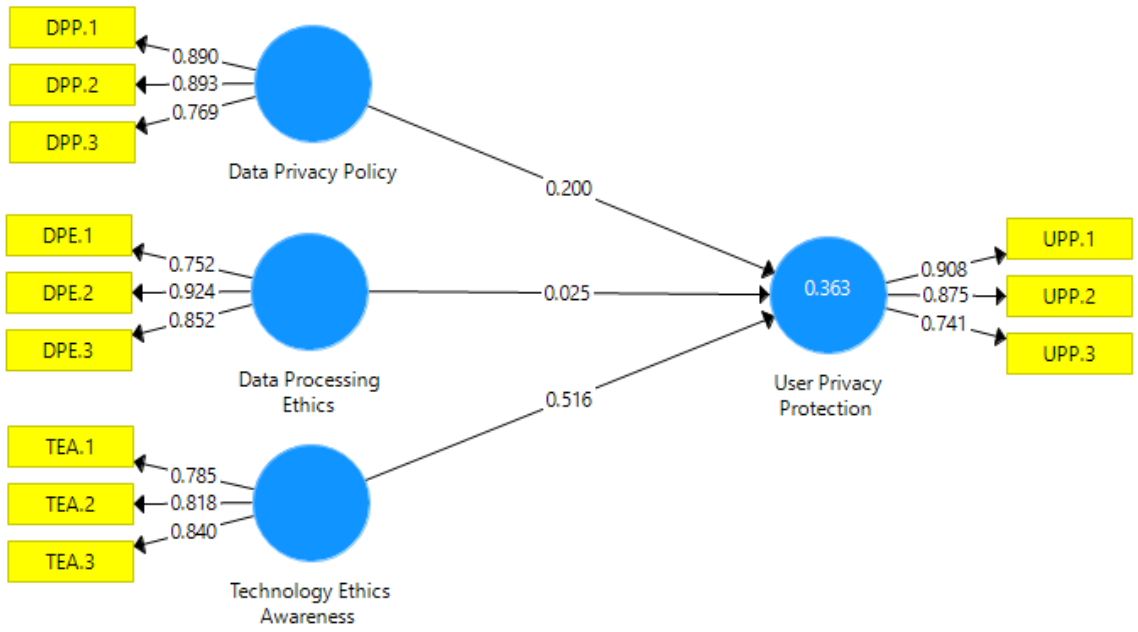

Figure 1. Model Results

Source: Data Processed By Researchers, 2024

4.4 Model Fit Analysis

The model fit analysis assesses the extent to which the hypothesized structural model adequately represents the relationships between observed and latent variables in the data. In this section, we discuss the fit indices for both the Saturated Model (the model where all possible relationships are estimated) and the Estimated Model (the hypothesized model) based on the provided fit indices.

Table 3. Model Fit Results Test

	Saturated Model	Estimated Model
SRMR	0.106	0.106
d_ULS	0.873	0.873
d_G	0.350	0.350
Chi-Square	251.258	251.258
NFI	0.648	0.648

Source: Data Processing Results (2024)

In model fit analysis, researchers typically evaluate multiple fit indices to assess the overall goodness of fit of the structural model to the observed data. The fit indices provided, including the Standardized Root Mean Square Residual (SRMR), Chi-Square, and Normed Fit Index (NFI), serve as measures of discrepancy and incremental fit, respectively. The Saturated Model acts as a baseline, estimating all possible relationships and indicating the best possible fit given the data, while the Estimated Model represents hypothesized relationships based on the research model. In this study, both models demonstrate identical fit indices across all measures, indicating adequate fit to the data. The SRMR, d_ULS, and d_G values fall within acceptable ranges, signifying good fit, and the non-significant Chi-Square value suggests no significant deviation from the observed data. However, the relatively low NFI value (0.648) suggests potential for improving model fit through exploring alternative specifications or modifying hypothesized relationships between variables.

Table 4. Coefficient Model

	R Square	Q2
User Privacy Protection	0.363	0.347

Source: Data Processing Results (2024)

In structural equation modeling (SEM), R-Square (R^2) and Q^2 are pivotal measures used to gauge the explanatory power and predictive relevance of endogenous latent constructs within the model. Specifically focusing on the endogenous latent construct "User Privacy Protection," the R-Square value of 0.363 signifies that approximately 36.3% of the variance in user privacy protection is elucidated by the independent variables (Data Privacy Policy, Data Processing Ethics, and Technological Ethics Awareness) integrated into the model. This metric offers insights into the model's overall explanatory prowess, with higher R-Square values indicating stronger relationships between independent and dependent variables. Additionally, Q^2, representing the cross-validated R-Square, measures the predictive relevance of the endogenous latent variable, showcasing its ability to forecast itself in a cross-validated context. With a Q^2 value of 0.347 for "User Privacy Protection," approximately 34.7% of the variance in user privacy protection is predicted by the model when applied to new data, affirming its validity and utility in predicting user privacy protection outcomes in similar contexts.

4.5 Hypothesis Testing

Hypothesis testing evaluates the statistical significance of the relationships between independent and dependent variables in the structural model. In this section, we discuss the results of hypothesis

testing for the relationships between Data Privacy Policy, Data Processing Ethics, Technological Ethics Awareness, and User Privacy Protection based on the provided sample statistics.

Table 5. Hypothesis Testing

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics	P Values
Data Privacy Policy -> User Privacy Protection	0.400	0.494	0.097	4.059	0.000
Data Processing Ethics -> User Privacy Protection	0.325	0.349	0.077	2.323	0.001
Technology Ethics Awareness -> User Privacy Protection	0.516	0.515	0.066	7.823	0.000

Source: Process Data Analysis (2024)

The hypothesis testing results unveil significant relationships between various constructs and User Privacy Protection. Data Privacy Policy demonstrates a substantial positive influence on User Privacy Protection, evidenced by a t-statistic of 4.059 and a p-value of 0.000, indicating statistical significance. Similarly, Data Processing Ethics exhibits a significant positive effect on User Privacy Protection, albeit with a slightly smaller t-statistic of 2.323 and a p-value of 0.001. Moreover, Technological Ethics Awareness demonstrates a highly significant relationship with User Privacy Protection, supported by a notable t-statistic of 7.823 and a p-value of 0.000. These findings confirm the hypothesized relationships within the structural model and emphasize the critical role of organizational policies, ethical data processing practices, and user awareness initiatives in promoting and preserving user privacy.

Discussion

In this chapter, we delve into the implications of the study findings, discuss their significance, and explore avenues for future research. The discussion encompasses the relationships between data privacy policy adherence, data processing ethics, technological ethics awareness, and user privacy protection, as well as their broader implications for stakeholders in West Java, Indonesia, and beyond.

Understanding the Relationships

The study's findings underscore the significant positive relationships between data privacy policy adherence, data processing ethics, and technological ethics awareness with user privacy protection. These results highlight the multifaceted nature of privacy protection, indicating that regulatory compliance, ethical data practices, and user awareness collectively contribute to fostering a secure and trustworthy digital environment.

The study's findings highlight the importance of data privacy policy adherence, ethical data practices, and user awareness in promoting user privacy protection [27], [28]. These factors collectively contribute to creating a secure and trustworthy digital environment. Regulatory compliance ensures that companies safeguard customer data and comply with data protection laws [12]. Ethical data practices, such as transparency, accountability, and fairness, are essential for protecting personal information and building trust between customers and service providers [29], [30]. User awareness plays a crucial role in understanding privacy issues and making informed decisions about providing personal information. By considering these multifaceted aspects of privacy protection, organizations can foster a digital environment that prioritizes user privacy and promotes ethical data practices.

Implications for Policymakers

For policymakers, the study findings emphasize the importance of enacting and enforcing robust data privacy regulations. By prioritizing regulatory compliance and

providing clear guidelines for organizations, policymakers can promote a culture of accountability and transparency in data handling practices. Additionally, policymakers should invest in public education campaigns to raise awareness about privacy rights and empower users to make informed decisions about their personal data.

Considerations for Organizations

Organizations play a pivotal role in safeguarding user privacy through ethical data processing practices. The study highlights the need for organizations to prioritize transparency, accountability, and fairness in their data-handling procedures. By implementing privacy-by-design principles and adopting ethical data processing frameworks, organizations can enhance user trust and mitigate privacy risks.

Empowering Users

User empowerment is central to privacy protection efforts, as highlighted by the positive relationship between technological ethics awareness and user privacy protection. Advocacy groups, educational institutions, and industry stakeholders should collaborate to promote digital literacy and empower users to assert their privacy rights. By equipping users with the knowledge and tools to navigate digital environments safely, stakeholders can foster a culture of privacy-conscious behavior.

Future Research Directions

While the study provides valuable insights into privacy protection dynamics, there are several avenues for future research. Longitudinal studies could explore the long-term impact of data privacy policies and ethical data practices on user privacy outcomes. Additionally, qualitative research methods could provide deeper insights into the underlying mechanisms driving privacy-related behaviors and attitudes among stakeholders.

5. CONCLUSION

In conclusion, this study contributes to the understanding of factors influencing user privacy protection in the digital era, particularly in the context of West Java, Indonesia. Through quantitative analysis, we have demonstrated the significant positive relationships between data privacy policy adherence, data processing ethics, technological ethics awareness, and user privacy protection. These findings highlight the crucial role of regulatory compliance, ethical data practices, and user education in fostering a safe and trustworthy digital environment. Policymakers, organizations, and users must collaborate to prioritize privacy protection measures and promote responsible data handling practices. By addressing these key factors, stakeholders can work towards enhancing user privacy outcomes and building trust in digital interactions. Moving forward, continued research and concerted efforts are needed to address emerging privacy challenges and ensure a privacy-respecting digital ecosystem for all users.

REFERENCES

[1] V. P. Shehu and V. Shehu, "Human rights in the technology era–Protection of data rights," *… Journal of Economics, Law and Social Sciences*. sciendo.com, 2023. doi: 10.2478/ejels-2023-0001.

[2] M. Zostant and R. Chataut, "Privacy in computer ethics: Navigating the digital age," *Comput. Sci. Inf. Technol.*, vol. 4, no. 2, pp. 183–190, 2023.

[3] V. Katiandagho, D. D. Putong, and I. J. Melo, "Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia," *J. Huk. to-ra Huk. Untuk Mengatur dan Melindungi Masy.*, vol. 9, no. 1, pp. 106–114, 2023.

[4] E. Krisnaningsih, S. Dwiyatno, A. D. Jubaedi, and A. Shafitri, "Increasing Ethical Understanding of the Use of Information Technology Through Digital Literacy Proficiency Training," *Din. J. Pengabdi. Kpd. Masy.*, vol. 7, no. 3, pp. 789–801, 2023.

[5] E. A. P. Manurung, "The right to privacy based on the Law of the Republic of Indonesia number 27 of 2022," *J. Digit. Law Policy*, vol. 2, no. 3, pp. 103–110, 2023.

[6] G. Harinath, "Does personal data protection matter in data protection law? A transformational model to fit in the digital era," *Handb. Big Data Res. Methods 0*, 2023, [Online]. Available: https://books.google.com/books?hl=en&lr=&id=9gPEEAAAQBAJ&oi=fnd&pg=PA267&dq=personal+data+protection+in+the+digital+age&ots=ikgF61cekO&sig=JhPfL-foIY6R8mkM2R5jkPQPwUs

[7] S. Wiefling, J. Tolsdorf, and L. Lo Iacono, "Data Protection Officers' Perspectives on Privacy Challenges in Digital Ecosystems," in *European Symposium on Research in Computer Security*, Springer, 2022, pp. 228–247.

[8] N. Fedocenko and H. Spitsyna, "Current issues of international legal regulation of the protection of personal data of employees," *Anal. Comp. Jurisprud.*, pp. 204–208, Jun. 2023, doi: 10.24144/2788-6018.2023.02.34.

[9] S. Simonova, "Data processing on digital platforms: topical issues of improving legislation and practice," *Vestn. Yarosl. Gos. Univ. im. P. G. Demidova. Seriya Gumanit. Nauk.*, vol. 16, p. 642, Dec. 2022, doi: 10.18255/1996-5648-2022-4-642-649.

[10] R. Romansky, "Digital age and personal data protection," *… Journal on Information Technologies &Security*. researchgate.net, 2022. [Online]. Available: https://www.researchgate.net/profile/Radi-Romansky/publication/362695987_DIGITAL_AGE_AND_PERSONAL_DATA_PROTECTION/links/62fa34f5e3c7de4c345c4233/DIGITAL-AGE-AND-PERSONAL-DATA-PROTECTION.pdf

[11] M. Cuquet, G. Vega-Gorgojo, H. Lammerant, and R. Finn, "Societal impacts of big data: challenges and opportunities in Europe," *arXiv Prepr. arXiv1704.03361*, 2017.

[12] M. S. McCoy *et al.*, "Ethical responsibilities for companies that process personal data," *Am. J. Bioeth.*, vol. 23, no. 11, pp. 11–23, 2023.

[13] S. Matagi and S. Kaneko, "Challenges and opportunities on data protection and privacy in healthcare," *Int. J. Sci. Res. Updat.*, vol. 5, pp. 23–41, Jan. 2023, doi: 10.53430/ijsru.2023.5.1.0001.

[14] N. Scope, A. Rasin, B. Lenard, K. Heart, and J. Wagner, "Harmonizing privacy regarding data retention and purging," in *Proceedings of the 34th International Conference on Scientific and Statistical Database Management*, 2022, pp. 1–12.

[15] L. Golightly, K. Wnuk, N. Shanmugan, A. Shaban, J. Longstaff, and V. Chang, "Towards a Working Conceptual Framework: Cyber Law for Data Privacy and Information Security Management for the Industrial Internet of Things Application Domain," in *2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC)*, IEEE, 2022, pp. 86–94.

[16] R. J. Sancon, "Data Privacy Best Practices of A Local Higher Educational Institution: A Model for Governance," *Int. Multidiscip. Res. J.*, Jun. 2023, doi: 10.54476/ioer-imrj/688585.

[17] P. Yadav, S. Tiwari, P. Kumari, and S. Mittal, "Business Policies and Practices for Ensuring Data Security: An Exploratory Study," *J. IoT Secur. Smart Technol.*, vol. 2, pp. 9–14, Feb. 2023, doi: 10.46610/JISST.2023.v02i01.002.

[18] S. Parthasarathy, P. K. Panigrahi, and G. H. Subramanian, "A framework for managing ethics in data science projects," *Eng. Reports*, p. e12722, 2023.

[19] S. Shubham and S. Saloni, "Data and science engineering: The ethical dilemma of our time-exploring privacy breaches, algorithmic biases, and the need for transparency," *World J. Adv. Res. Rev.*, vol. 18, no. 1, pp. 762–768, 2023.

[20] M. Levine, R. Philpot, S. J. Nightingale, and A. Kordoni, "Visual digital data, ethical challenges, and psychological science.," *Am. Psychol.*, vol. 79, no. 1, p. 109, 2024.

[21] N. Tempini, "The ethics of data self-reporting: important issues and best practices," *F1000Research*, vol. 12, p. 485, 2023.

[22] V. Gerasimenko, "Digital Ethics of Artificial Intelligence Application in Business: Awareness of New Opportunities and Risks," *Sci. Res. Fac. Econ. Electron. J.*, vol. 15, pp. 37–54, Apr. 2023, doi: 10.38050/2078-3809-2023-15-1-37-54.

[23] N. K. S. KUMAR, "End user privacy protection system and method thereof." Google Patents, Dec. 08, 2022.

[24] H. Wang, "Short Video Users' Personal Privacy Leakage and Protection Measures," in *Intelligent Computing Theories and Application: 17th International Conference, ICIC 2021, Shenzhen, China, August 12–15, 2021, Proceedings, Part I 17*, Springer, 2021, pp. 317–326.

[25] M. Rodriguez-Garcia, M. Batet, D. Sánchez, and A. Viejo, "Privacy protection of user profiles in online search via semantic randomization," *Knowl. Inf. Syst.*, vol. 63, pp. 2455–2477, 2021.

[26] Z. Qu, Y. Tang, G. Muhammad, and P. Tiwari, "Privacy protection in intelligent vehicle networking: A novel federated learning algorithm based on information fusion," *Inf. Fusion*, vol. 98, p. 101824, 2023.
[27] H. H. H. Aldboush and M. Ferdous, "Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust," *Int. J. Financ. Stud.*, vol. 11, no. 3, p. 90, 2023.
[28] C. U. Ingole, M. Bandela, D. Tanna, S. K. Solanki, P. Dhotre, and R. Patil, "Privacy Awareness and Online Behavior of Indian Users: An Analytical Study," 2023.
[29] J. Sah and S. Jun, "The role of consumers' privacy awareness in the privacy calculus for iot services," *Int. J. Human–Computer Interact.*, pp. 1–12, 2023.
[30] D. Susanto, "Protection of Personal Data in Business: An Overview of the Perspective of Business Ethics and Its Implications for Regulatory Compliance," *Indones. J. Contemp. Multidiscip. Res.*, vol. 2, no. 2, pp. 109–120, 2023.