Jurnal Communio : Jurnal Ilmu Komunikasi, Volume 13, No. 2, Juli 2024, hlm 349-359

User Privacy Preservation in AI-Powered Digital Communication Systems

Ilham Gemiharto[1], Dwi Masrina[2]
[1,2]Faculty of Communication Science, Universitas Padjadjaran

ABSTRACT
In an era dominated by AI-powered digital communication systems, concerns about user privacy have taken center stage. This research aims to understand and assess the strategies employed to preserve user privacy in such a system. Specifically, it seeks to identify the range of privacy preservation methods, evaluate the transparency of data collection and usage, and analyze the mechanisms for obtaining user consent. Additionally, the research aims to assess the impact of these strategies on user trust and satisfaction. This research presents a comparative case study to achieve these objectives. A qualitative comparative case study methodology focused on multiple AI-powered digital communication systems, comparing different privacy preservation strategies across various platforms. Data was collected through in-depth interviews with system developers and users, content analysis of privacy policies, and user experience assessments. The in-depth interviews provided insights into the practical challenges and strategies from the perspective of both developers and users. In contrast, the content analysis and user assessments offered a comprehensive understanding of the implemented privacy measures and their perceived effectiveness. The findings reveal diverse approaches to user privacy preservation, ranging from end-to-end encryption to data anonymization. Variations were observed in the transparency of data collection and usage and the mechanisms for user consent. The study also highlighted the impact of these strategies on user trust and satisfaction. This research underscores the importance of a nuanced approach to user privacy preservation, considering both technical and ethical dimensions. It emphasizes the need for transparent communication between users and system developers and the role of legal frameworks and industry standards in shaping privacy practices. In the context of AI-powered digital communication systems, this comparative case study sheds light on the multifaceted landscape of user privacy preservation. It advocates for a holistic approach that combines technical safeguards, ethical considerations, and regulatory measures to ensure user privacy in an increasingly interconnected digital world.

Keywords: AI-powered digital communication systems; Data protection; Privacy strategies; User privacy preservation

Perlindungan Privasi Pengguna dalam Sistem Komunikasi Digital Berbasis AI

ABSTRAK
Di era yang didominasi oleh sistem komunikasi digital bertenaga AI, kekhawatiran tentang privasi pengguna menjadi pusat perhatian. Penelitian ini bertujuan untuk memahami dan menilai strategi yang digunakan untuk menjaga privasi pengguna dalam sistem tersebut. Secara khusus, penelitian ini berusaha untuk mengidentifikasi berbagai metode pelestarian privasi, mengevaluasi transparansi pengumpulan dan penggunaan data, dan menganalisis mekanisme untuk mendapatkan persetujuan pengguna. Selain itu, penelitian ini juga bertujuan untuk menilai dampak dari strategi-strategi ini terhadap kepercayaan dan kepuasan pengguna. Penelitian ini menyajikan studi kasus komparatif untuk mencapai tujuan-tujuan tersebut. Metodologi studi kasus kualitatif yang berfokus pada beberapa sistem komunikasi digital bertenaga AI, membandingkan berbagai strategi pelestarian privasi di berbagai platform. Data dikumpulkan melalui wawancara mendalam dengan pengembang sistem dan pengguna, analisis konten kebijakan privasi, dan penilaian pengalaman pengguna. Wawancara mendalam memberikan wawasan tentang tantangan dan strategi praktis dari perspektif pengembang dan pengguna. Sebaliknya, analisis konten dan penilaian pengguna menawarkan pemahaman yang komprehensif tentang langkah-langkah privasi yang diterapkan dan efektivitas yang dirasakan. Temuan-temuan ini mengungkapkan beragam pendekatan untuk menjaga privasi pengguna, mulai dari enkripsi ujung ke ujung hingga anonimisasi data. Variasi diamati dalam transparansi pengumpulan dan penggunaan data serta mekanisme persetujuan pengguna. Penelitian ini juga menyoroti dampak dari strategi-strategi ini terhadap kepercayaan dan kepuasan pengguna. Penelitian ini menggarisbawahi pentingnya pendekatan yang bernuansa pelestarian privasi pengguna, dengan mempertimbangkan dimensi teknis dan etika. Penelitian ini menekankan perlunya komunikasi yang transparan antara pengguna dan pengembang sistem serta peran kerangka hukum dan standar industri dalam membentuk praktik privasi. Dalam konteks sistem komunikasi digital yang didukung oleh AI, studi kasus komparatif ini menyoroti lanskap pelestarian privasi pengguna yang beragam. Studi ini mengadvokasi pendekatan holistik yang menggabungkan perlindungan teknis, pertimbangan etis, dan langkah-langkah regulasi untuk memastikan privasi pengguna di dunia digital yang semakin terhubung.

Kata-kata kunci: *Sistem komunikasi digital bertenaga AI; Perlindungan data; Strategi privasi; Perlindungan data pribadi*

Korespondensi: Ilham Gemiharto. Faculty of Communication Science, Universitas Padjadjaran. Email: ilham@unpad.ac.id

INTRODUCTION

In the current digital landscape, where Artificial Intelligence (AI) exerts an unprecedented influence over various facets of society, user privacy has emerged as a paramount concern. The ubiquity of AI-powered digital communication systems has revolutionized how individuals interact, share information, and conduct transactions. However, this surge in technological advancement has brought forth a pressing need to safeguard the confidentiality and autonomy of users within these systems (Chatterjee et al., 2022; Yeo et al., 2022). The Indonesian digital communication ecosystem is a microcosm of this global paradigm shift. With a populace progressively reliant on digital platforms for communication, commerce, and social interaction, preserving user privacy is critical. This necessitates a comprehensive and nuanced understanding of the strategies and mechanisms employed to protect user data in AI-driven communication systems within the Indonesian context (Fatihah & Saidah, 2021; Sholihah & Irwansyah, 2020).

User privacy preservation in AI-powered digital communication systems is a critical concern, given the sensitive nature of the data involved. Virtual voice assistants like Siri, Google Assistant, Alexa, Bixby, and Celia process voice commands or text inputs to perform tasks and provide information. These assistants implement state-of-the-art encryption techniques, such as Advanced Encryption Standards (AES) and protocols like Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), to ensure data confidentiality and integrity during transit (Ahmad & Hasan, 2021). However, challenges remain in ensuring transparency in data collection and usage, obtaining user consent, and maintaining user trust (Liu et al., 2022; Shariatzadeh et al., 2021).

In Indonesia, the adoption of virtual voice assistants has steadily grown. Localizing these assistants to Bahasa Indonesia enhances cultural relevance and user engagement by allowing interactions in the local language (Gerung et al., 2019). This localization effort addresses not only the linguistic needs of the majority but also the diverse linguistic landscape of Indonesia, acknowledging the nation's rich cultural tapestry and linguistic diversity (Ardiansyah, 2023; Paramesti & Nurdiarti, 2022). This inclusivity is crucial for ensuring that all segments of the population can benefit from the capabilities of virtual assistants. (Sarosa, Kusumawardani, Suyono, & Sari, 2020; Wijaya, Rusli, Syah Rany, & Fryonanda, 2020).

The Indonesian government has made significant strides in data privacy and protection, as evidenced by the enactment of the Personal Data Protection Law (UU PDP) in 2016. This law mandates obtaining informed consent from data subjects before processing their personal information and emphasizes the principles of purpose limitation and data subject rights (Hisbulloh, 2021; Sautunnida, 2018). Additionally, virtual assistant providers must regularly assess and update their security protocols to stay ahead of evolving threats and vulnerabilities. By aligning

with GR 82/2012 mandates, virtual assistant providers play a crucial role in safeguarding user data, thereby contributing to the broader objective of maintaining a secure and trustworthy digital environment in Indonesia (Indriani et al., 2014; Sugeng, 2020).

Efforts to preserve user privacy data in Indonesia face several obstacles and challenges, contributing to the perception that they may be lagging compared to more developed countries. The level of digital literacy and formal education about online privacy in Indonesia is a critical factor. While access to digital technology has grown significantly, comprehensive educational programs regarding online privacy and data protection are still in the early stages. Many individuals may not have received formal training or education on the nuances of safeguarding their personal information online. This gap in knowledge can lead to unintentional oversharing of sensitive data or a lack of awareness about best practices for protecting one's privacy in digital spaces. Cultural norms in Indonesia may also influence perceptions of privacy. Traditionally, Indonesia has a collective culture, where the emphasis is often on community and social cohesion. This can sometimes lead to a more relaxed attitude towards sharing personal information, particularly in online settings. As a result, individuals may not always be as vigilant about safeguarding their persona in cultures where privacy is held in higher regard. This cultural context plays a significant role in shaping attitudes towards privacy and may contribute to the lower level of awareness observed in the general population.

Indonesia's journey in enacting data protection laws reflects a commendable effort to adapt to the rapidly evolving digital landscape. The legislative framework has evolved significantly with the introduction of critical regulations like the Personal Data Protection Law (UU PDP) in 2016. However, it is essential to acknowledge that the regulatory landscape is still maturing. The UU PDP, while a crucial step forward, may require further refinements and amendments to address emerging challenges in data protection. As technologies continue to advance, it becomes imperative for the regulatory framework to evolve in tandem, ensuring that it is active and relevant in safeguarding user privacy. Enforcing data protection regulations poses unique challenges, particularly in a diverse and geographically expansive country like Indonesia. The enforcement mechanisms and resources available to regulatory authorities may not be as extensive as those in more developed countries. This can result in variations in the rigor with which data protection laws are implemented and enforced across different regions. Additionally, the sheer volume of businesses, both large and small, operating in Indonesia adds complexity to regulatory oversight. Striking a balance between encouraging compliance and avoiding undue burden on businesses requires careful calibration of enforcement strategies. These challenges can contribute to gaps in user privacy preservation measures, highlighting the need for

ongoing efforts to strengthen regulatory enforcement and implementation capabilities.

This research seeks to understand and assess the strategies employed to preserve user privacy in AI-powered digital communication systems. The specific objectives of the study are to (1) Identify the range of privacy preservation methods used in AI-powered digital communication systems; (2) Evaluate the transparency of data collection and usage practices in these systems; (3) Analyze the mechanisms for obtaining user consent within these platforms; and (4) Assess the impact of privacy preservation strategies on user trust and satisfaction.

This comparative case study focuses on multiple AI-powered digital communication systems, comparing different privacy preservation strategies across various platforms. Data was collected through in-depth interviews with system developers and users, content analysis of privacy policies, and user experience assessments. The findings reveal diverse approaches to user privacy preservation, ranging from end-to-end encryption to data anonymization, and highlight the variations in transparency and user consent mechanisms. This research underscores the importance of a nuanced approach to user privacy preservation, considering both technical and ethical dimensions. It advocates for a holistic approach that combines technical safeguards, ethical considerations, and regulatory measures to ensure user privacy in an increasingly interconnected digital world.

RESEARCH METHOD

This research utilizes a case study approach, employing qualitative techniques within an exploratory paradigm. Case studies are particularly valuable in providing rich, detailed insights into complex phenomena within their real-life contexts (Creswell, 2017). This methodology allows for a deep exploration of the strategies implemented to safeguard user privacy in AI-powered digital communication systems. The qualitative nature of the study emphasizes flexible and open research methods that facilitate inductive analysis, enabling a nuanced understanding of the research subject (Bungin, 2017; Moleong, 2018).

The research employs a qualitative comparative case study methodology, focusing on multiple AI-powered digital communication systems. This approach enables an in-depth examination and assessment of the strategies employed to preserve user privacy. The research subjects encompass various digital communication platforms utilizing AI technologies, providing a comprehensive view of the privacy preservation landscape.

Data collection is conducted through a comprehensive process involving in-depth interviews with system developers and users, content analysis of privacy policies, and evaluations of user experiences. By engaging both system developers and users, the study ensures a holistic perspective on the issue of user privacy preservation in AI-powered digital communication systems.

The analysis of the collected data reveals a spectrum of approaches to user privacy preservation, ranging from robust measures such as end-to-end encryption to subtler techniques like data anonymization. One of the significant insights derived from this research pertains to the transparency of data collection and usage, as well as the mechanisms for obtaining user consent. These variations directly impact user trust and satisfaction, highlighting the intricate relationship between privacy practices and user experience.

The study underscores the need for a nuanced approach that considers both the technical and ethical dimensions of privacy preservation. It emphasizes the importance of transparent communication between users and system developers, as well as the role of legal frameworks and industry standards in shaping privacy practices within this evolving landscape.

RESULTS AND DISCUSSION

RESULTS

Developed countries have often had a head start in building advanced technological infrastructures. This encompasses a wide range of elements, including high-speed internet access, robust data centers, and sophisticated cybersecurity systems. The pace at which these infrastructures were developed has allowed for the seamless integration of state-of-the-art privacy preservation measures. In contrast, Indonesia, while making significant progress in improving its digital infrastructure, may face particular challenges in catching up to the level of technological advancement seen in more developed nations. Overcoming these challenges requires sustained investment, strategic planning, and coordination between public and private sectors.

One of the unique challenges faced by Indonesia is the need to bridge digital divides, particularly in terms of internet accessibility. While urban areas and major cities may have relatively advanced technological infrastructures, rural and remote regions may still lack access to high-speed internet and modern digital services. This disparity in connectivity can pose challenges in ensuring consistent and uniform implementation of privacy preservation measures across the entire country. Efforts to expand internet access and improve connectivity in underserved areas are crucial steps toward narrowing this gap and fostering a more inclusive digital environment.

There are several areas in Indonesia where internet connection and network infrastructure continue to be significant obstacles and challenges. Many remote and rural areas across Indonesia, particularly those located on various islands, often have limited access to reliable and high-speed internet. The challenging geographical terrain and lack of necessary infrastructure make it difficult to establish stable network connections in these regions. Islands in the eastern part of Indonesia, such as parts of Maluku, Papua, and Nusa Tenggara, face notable connectivity challenges. The scattered nature of these islands, combined with their relatively lower population densities, makes it economically challenging for telecommunication companies to invest in robust

network infrastructure. Areas with mountainous or hilly terrain, like parts of Sumatra and Sulawesi, often face difficulties in establishing consistent network coverage. The rugged landscape poses challenges in deploying and maintaining the necessary network infrastructure. Outer islands and regions near international borders, such as those in Kalimantan, Sulawesi, and Papua, can encounter network connectivity issues. Ensuring reliable internet access in these areas involves overcoming logistical and regulatory hurdles.

Even in urban centers like Jakarta, Surabaya, and Bandung, there can be challenges related to network congestion, especially during peak usage times. The high population density and intense demand for data services can strain existing network infrastructure. Specific communities in Kalimantan and Papua remain relatively isolated, often lacking reliable internet connectivity. These areas may require specialized solutions to bridge the connectivity gap. Areas prone to natural disasters, such as earthquakes, tsunamis, and floods, face additional challenges in maintaining consistent network connectivity. Infrastructure damage during disasters can disrupt internet services. Efforts are being made by the Indonesian government, telecommunications companies, and non-governmental organizations to address these challenges and expand internet access to underserved areas. Initiatives such as infrastructure development projects and the utilization of satellite technology are being explored to improve connectivity in these regions.

Indonesia's cultural diversity is one of its greatest strengths, but it also presents unique considerations for privacy preservation. Different regions and communities within Indonesia may have distinct privacy norms and expectations. Understanding and respecting these cultural nuances is crucial when designing privacy policies and practices. What may be considered acceptable in one community might differ in another. For instance, some communities may place a higher value on collective sharing, while others may prioritize individual privacy. Striking the right balance between respecting cultural norms and implementing effective privacy measures requires careful consideration and cultural sensitivity. With over 700 spoken languages and dialects, Indonesia boasts a rich linguistic tapestry. This linguistic diversity can pose challenges in ensuring that privacy policies and practices are accessible and easily understood by all segments of the population. It is essential to provide privacy information in multiple languages, particularly in areas where specific dialects are prevalent. Additionally, clear and simple language should be used to convey privacy-related information, ensuring that it is comprehensible to a broad audience. By addressing linguistic diversity, organizations can make significant strides in creating inclusive privacy policies that resonate with all members of the Indonesian population.

Based on the results of interviews with AI-Powered Digital Communication System service providers such as representatives of Apple, Google, Amazon, Samsung, and Huawei in Indonesia, a

common thread can be drawn that they implement a combination of encryption protocols, data anonymization, and access controls to safeguard user data. They have strict policies in place regarding data access and use by their team and employ a straightforward and user-friendly consent process. When users first interact with their system, they are presented with a detailed privacy policy outlining what data is collected and how it is used. Users have the option to opt in or out of specific data processing activities. The system implements a range of security measures to safeguard user data. This includes the application of encryption protocols, data anonymization techniques, and access controls. These measures collectively contribute to the confidentiality and integrity of user information. Additionally, the system maintains stringent policies governing data access and usage by the team. This ensures that data is handled with care and only accessed for legitimate purposes.

The system places a strong emphasis on user consent and transparency. When users first engage with the platform, they are presented with a comprehensive privacy policy. This document outlines the types of data collected, the purposes for which it is gathered, and how it will be utilized. Users are given the option to exercise control over specific data processing activities, aligning with their preferences and comfort levels. Such a user-centric approach not only empowers individuals but also establishes a foundation of trust. The system is designed to operate effectively within Indonesia's diverse linguistic and cultural landscape. It is equipped to understand and respond in various regional languages and dialects, ensuring interactions are accurate and culturally relevant. However, this linguistic diversity does present challenges in refining language processing capabilities. To address this, ongoing efforts are made to enhance models and better capture nuances. Moreover, the system adheres to Indonesian data protection laws and regulations, including the Personal Data Protection Law (UU PDP), to ensure compliance with established standards. This underscores the commitment to responsible data handling practices in the context of digital communication systems.

Furthermore, sources from the Ministry of Communication and Information of the Republic of Indonesia stated that The UU PDP provides a comprehensive legal framework for the protection of personal data. It outlines the principles and requirements for processing personal data, including consent, purpose limitation, and data subject rights. The law defines the roles and responsibilities of data controllers and processors. This includes obligations to implement technical and organizational measures to protect personal data, as well as reporting data breaches when they occur. The UU PDP emphasizes the importance of obtaining explicit consent from individuals for data processing activities. This aligns with global best practices for ensuring transparency and empowering individuals to have control over their

personal information. The law grants individuals various rights over their data, such as the right to access, rectify, erase, or object to the processing of their data. This empowers individuals to have a say in how their data is handled. The law addresses cross-border data transfers by requiring data controllers to ensure that personal data transferred out of Indonesia receives an adequate level of protection. The law establishes the role of the Personal Data Protection Agency (Badan Perlindungan Data Pribadi or "BPDP") to oversee and enforce compliance with data protection regulations. The BPDP is tasked with monitoring data processing activities and handling complaints.

DISCUSSION

In the AI-based digital communications sector, compliance with the UU PDP is of paramount importance. Companies and platforms that utilize AI for communication purposes must ensure that they have robust privacy measures in place. This includes obtaining explicit and informed consent for data processing, implementing encryption and anonymization techniques, and providing accessible mechanisms for users to exercise their data rights. Implementing the UU PDP in the AI-based digital communications sector can be complex due to the dynamic nature of technology and evolving AI applications. Companies may face challenges in fine-tuning their systems to align with data protection requirements. Ongoing efforts are needed to adapt to emerging technologies and address any potential gaps in compliance.

In the realm of digital communication science theory, the findings presented in this paragraph underscore the critical importance of robust data protection measures within AI-Powered Digital Communication Systems. The providers, representing major tech companies, have implemented a multifaceted approach that encompasses encryption protocols, data anonymization, and access controls. These measures collectively function as a safeguard to preserve user data integrity and confidentiality. Furthermore, the emphasis on user consent and transparency is a cornerstone of their approach. This user-centric philosophy is evident in the comprehensive privacy policy presented to users upon their initial interaction with the platform. This policy elucidates the nature of data collection, its purpose, and the methods through which it will be utilized. The provision of user-controlled options regarding data processing activities not only empowers individuals but also establishes a bedrock of trust between the user and the platform.

The recognition and accommodation of Indonesia's diverse linguistic and cultural landscape demonstrate a keen understanding of the socio-cultural context in which these systems operate. The system's capacity to understand and respond in various regional languages and dialects ensures that interactions are not only accurate but also culturally relevant. However, it is acknowledged that linguistic diversity presents a challenge in refining language processing capabilities. Ongoing efforts are directed towards enhancing models to capture linguistic nuances better, reflecting a commitment to continuous

improvement. Importantly, adherence to Indonesian data protection laws and regulations, including the Personal Data Protection Law (UU PDP), is a testament to the platform's dedication to responsible data handling practices. This regulatory compliance underscores the platform's commitment to upholding established standards in the context of digital communication systems.

Overall, these findings align with digital communication science theories that emphasize the significance of privacy, transparency, and cultural sensitivity in shaping effective and responsible digital communication systems, particularly within the Indonesian context. The multifaceted approach adopted by the providers reflects a holistic understanding of the complexities inherent in preserving user privacy and trust in the digital realm.

CONCLUSION

The research highlights significant challenges in user privacy preservation in Indonesia, particularly in the context of AI-powered digital communication systems. The level of digital literacy and formal education regarding online privacy emerges as a critical factor. While access to digital technology has grown, comprehensive educational programs on online privacy and data protection are still nascent. This knowledge gap leads to inadvertent oversharing of sensitive data and a lack of awareness about best practices in safeguarding one's privacy online. Cultural norms, rooted in Indonesia's collective culture, influence perceptions of privacy. This can result in a more relaxed attitude towards sharing personal information online, especially in a communal context. This cultural backdrop contributes to a lower level of awareness about privacy among the general population. The enactment of the Personal Data Protection Law (UU PDP) in 2016 signifies Indonesia's commendable efforts to adapt to the evolving digital landscape. However, the regulatory framework is still evolving and may require further refinements to address emerging data protection challenges. Challenges in enforcement, particularly in a geographically expansive country like Indonesia, add complexity to regulatory oversight. This may lead to variations in the rigor with which data protection laws are implemented across different regions. Moreover, Indonesia faces infrastructure challenges, with limited access to reliable and high-speed internet, especially in remote and rural areas. This connectivity gap poses hurdles in implementing consistent privacy preservation measures nationwide. Efforts to expand internet access are pivotal in fostering a more inclusive digital environment.

Indonesia's rich cultural diversity presents both strengths and challenges in privacy preservation. Recognizing and respecting diverse privacy norms is essential in designing effective privacy policies and practices. The linguistic diversity, with over 700 spoken languages and dialects, necessitates clear and accessible privacy information for all segments of the population. In conclusion, addressing these challenges requires a concerted effort from various stakeholders, including educational institutions, regulatory

bodies, technology providers, and infrastructure developers. By prioritizing privacy education, refining regulatory frameworks, and investing in digital infrastructure, Indonesia can make substantial strides toward robust user privacy preservation in the digital age.

REFERENCES

Ahmad, N., & Hasan, S. M. R. (2021). A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator. *Microelectronics Journal*, *117*, 105255. https://doi.org/10.1016/j.mejo.2021.105255

Ardiansyah, A. (2023). Pendampingan Perancangan Chatbot Sebagai Media Interaktif Dalam Menghadapi Tantangan Era Digitalisasi. *Lamahu: Jurnal Pengabdian Masyarakat Terintegrasi*, *2*(1), 44–55. https://doi.org/10.34312/ljpmt.v2i1.18078

Bungin, B. (2017). *Metodologi Penelitian Kualitatif*. (B. Bungin, Ed.) (2nd ed.). Jakarta: PT Rajagrafindo Persada. Retrieved from https://www.rajagrafindo.co.id/produk/metodologi-penelitian-kualitatif-burhan-bungin/

Chatterjee, S., Chaudhuri, R., & Vrontis, D. (2022). AI and digitalization in relationship management: Impact of adopting AI-embedded CRM system. *Journal of Business Research*, *150*, 437–450. https://doi.org/10.1016/j.jbusres.2022.06.033

Creswell, J. W. (2017). *Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed*. (S. Z. Qudsy, Ed.) (3rd ed.). Yogyakarta, Indonesia: Pustaka Pelajar. Retrieved from https://opac.perpusnas.go.id/DetailOpac.aspx?id=1213690

Elita Natalia Sugianto, Jessica Aurelia Sujangga, Delvia, N., Verdiana Ayustika, & Agus Cahyo Nugroho. (2022). Pengembangan Chatbot "Ciovita" Virtual Assistant Cioccolato Brownie Semarang Dengan Metode Waterfall. *Journal of Applied Computer Science and Technology*, *3*(2), 179–185. https://doi.org/10.52158/jacost.v3i2.348

Fatihah, D. C., & Saidah, I. S. (2021). Model Promosi Marketplace Berbasis Artificial Inteligence (AI) di Indonesia. *JMBI UNSRAT (Jurnal Ilmiah Manajemen Bisnis Dan Inovasi Universitas Sam Ratulangi).*, *8*(3). https://doi.org/10.35794/jmbi.v8i3.35908

Gerung, R. A., Fadilah, K., Wardani, Y., Dwiyaniti, M., & Mulyadi, W. H. (2019). Aplikasi Asisten Virtual sebagai Perintah Suara pada Sistem Otomatisasi Rumah Tinggal. *ELECTRICES*, *1*(1), 9–14. https://doi.org/10.32722/ees.v1i1.1890

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119. https://doi.org/10.26532/jh.v37i2.16272

Indriani, M., Arafah, A. R., & Islamy, F. N. (2014). Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cybercrime Dalam Sistem Transaksi Elektronik. *Yuridika*, *29*(3). https://doi.org/10.20473/ydk.v29i3.375

Kopalle, P. K., Gangwar, M., Kaplan, A., Ramachandran, D., Reinartz, W., & Rindfleisch, A. (2022). Examining artificial intelligence (AI) technologies in marketing via a global lens: Current trends and future research opportunities. *International Journal of Research in Marketing*, *39*(2), 522–540. https://doi.org/10.1016/j.ijresmar.2021.11.002

Lesmana, C. T., Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *3*(2), 1–6. https://doi.org/10.52005/rechten.v3i2.78

Liu, Y., Wang, L., Qouneh, A., & Fu, X. (2022). Enabling PIM-based AES encryption for online video streaming. *Journal of Systems Architecture*, *132*, 102734. https://doi.org/10.1016/j.sysarc.2022.102734

Moleong, J. L. (2018). *Qualitative Research Methodology* (8th ed.). Bandung: Remaja Rosdakarya. Retrieved from https://opac.perpusnas.go.id/DetailOpac.aspx?id=1133305

Paramesti, A. R., & Nurdiarti, R. P. (2022). Penggunaan Pseudonym di Second Account Instagram dalam Perspektif Etika Digital. *Jurnal Communio : Jurnal Jurusan Ilmu Komunikasi*, *11*(1), 89–102. https://doi.org/10.35508/jikom.v11i1.5184

Perdana, R. P., & Irwansyah, I. (2019). Implementasi Asisten Virtual Dalam Komunikasi Pelayanan Pelanggan (Studi Kasus Pada Layanan Pelanggan Telkomsel). *Jurnal Komunikasi*, *11*(2), 183. https://doi.org/10.24912/jk.v11i2.5491

Putra, J. C., Rohman, M. M., & Rizqi, M. (2021). Kecerdasan Buatan Virtual Assistant Pada Permainan Menggunakan Metode Finite State Machine. *Journal of Animation and Games Studies*, *7*(2), 85–100. https://doi.org/10.24821/jags.v7i2.4184

Sarosa, M., Kusumawardani, M., Suyono, A., & Sari, Z. (2020). Implementasi Chatbot Pembelajaran Bahasa Inggris menggunakan Media Sosial. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *6*(3), 317. https://doi.org/10.26418/jp.v6i3.43191

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159

Shariatzadeh, M., Rostami, M. J., & Eftekhari, M. (2021). Proposing a novel Dynamic AES for image encryption using a chaotic map key management approach. *Optik*, *246*, 167779. https://doi.org/10.1016/j.ijleo.2021.167779

Sholihah, E., & Irwansyah, I. (2020). Pemanfaatan Informasi dari Big Data oleh Underwriter pada Peer to Peer Lending. *Jurnal Manajemen Komunikasi*, *5*(1), 60–77. https://doi.org/https://doi.org/10.24198/jmk.v5i1.27524

Sugeng, S. (2020). Aspek Hukum Digital Lending di Indonesia. *Jurnal Legislasi Indonesia*, *17*(4), 437. https://doi.org/10.54629/jli.v17i4.639

Wijaya, T., Rusli, M., Syah Rany, E., & Fryonanda, H. (2020). Membangun Aplikasi Chatbot Berbasis Web Pada CV. Unomax Indonesia. *KALBISCIENTIA Jurnal Sains Dan Teknologi*, *6*(2), 110. https://doi.org/10.53008/kalbiscientia.v6i2.45

Yeo, S. F., Tan, C. L., Kumar, A., Tan, K. H., & Wong, J. K. (2022). Investigating the impact of AI-powered technologies on Instagrammers' purchase decisions in digitalization era–A study of the fashion and apparel industry. *Technological Forecasting and Social Change*, *177*, 121551. https://doi.org/10.1016/j.techfore.2022.121551