Journal of Management Studies and Development
Vol. 5, No. 01, pp. 200-210
journal.iistr.org/index.php/JMSD
DOI: 10.56741/IISTR.jmsd.001576

Exploring AI Adoption for Digital Legal Compliance in MSMEs

A Qualitative Study from Karanganyar Regency, Indonesia

[1]Marina Ramadhani*, [1]Arseto Endro Supriyanto, [1]Yayu Sri Rahayu
Corresponding Author: *marinaramadhani80@gmail.com
[1] Muhammadiyah University Karanganyar, Indonesia

ARTICLE INFO

Article history
Received XX July 2022
Revised XX August 2022
Accepted XX August 2022

Keywords
Artificial Intelligence
Digital Legal Compliance
MSMEs
Regulation

ABSTRACT

This study aims to explore the challenges and opportunities of applying Artificial Intelligence (AI) in supporting digital legal compliance among MSMEs in Karanganyar Regency, Indonesia. Using a qualitative approach based on in-depth interviews with MSME actors, technology practitioners, and legal experts, the research findings grouped the main issues into eight themes: low understanding of digital regulations, limited resources, perception of legal sanctions, regulatory fragmentation, the potential of AI for real-time monitoring, technical implementation challenges, consumer trust and privacy issues, and the role of local government in policy intervention. The analysis shows that although AI offers potential solutions to improve compliance, its implementation is still hampered by technical, cultural, and institutional factors. This study concludes that the successful application of AI to SMEs' digital legal compliance is highly dependent on institutional support and affirmative local policies.

This is an open-access article under the CC–BY-SA license.

Introduction

The digital transformation of MSMEs has increased business efficiency, but poses significant challenges in complying with digital laws, particularly regarding personal data protection and electronic transactions. Limited legal literacy and technological capacity make

it difficult for MSMEs to meet increasingly complex regulatory requirements. This situation is even more relevant considering that Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection require every electronic system operator, including MSMEs, to ensure the security and management of consumer personal data [1],[2]. Although this regulatory framework is in place, in practice, many MSMEs still face obstacles in implementing these legal obligations, while the use of artificial intelligence as a supporting instrument for compliance remains understudied in the local MSME context.

Karanganyar Regency, as one of the regencies in Central Java Province, has a strong commitment to promoting the advancement of the MSMEs sector, as reflected in its slogan "Progressive, Competitive, and Harmonious." Through this slogan, the local government continues to strive to create a conducive environment for MSME players to continue to grow, innovate, and compete competitively to strengthen their contribution to the regional and national economy. However, in the process of achieving these goals, MSME actors face various challenges, especially in terms of compliance with ever-evolving digital regulations.

MSME actors in this region find it difficult to keep up with regulatory changes in *real time* and detect potential legal violations before they occur. [3] show that of the total 7,914 MSMEs in 2022, around 3,195 MSMEs (40.4%) have used digital technology, while only 485 MSMEs (15.2%) have utilized technology for information searches, including digital searches for regulations [4]. This figure shows that although many MSMEs already use technology, few actively utilize it to search for and follow developments in the legal regulations governing their business activities.

The low level of technology utilization for searching for digital legal regulations has the potential to worsen the level of MSME compliance with existing legal obligations. This can result in legal risks for MSME players [4] , including legal sanctions that are detrimental to their businesses, such as fines, lawsuits, or loss of customers. As a solution to overcome this problem, the implementation of an Artificial Intelligence-based business management model is needed, which can be a very relevant and effective step in improving compliance with digital legal regulations.

AI-based systems can provide real-time monitoring, incident detection, and control, which can be tailored to regulatory compliance in MSMEs [5]**.** These systems can analyze large amounts of data to identify hidden patterns and predict potential regulatory violations before they occur, helping MSMEs to stay up-to-date with changes without the need for manual monitoring of regulations [6]**.**

Previous research on the application of AI in legal compliance in the SME sector is still limited. Most studies focus on the international context or large companies. For example,

previous findings have found that AI in the European Union and Ukraine can facilitate access to justice, increase transparency and efficiency, and support decision-making by automating routine processes and analyzing big data[7]. AI is effective in improving legal oversight and compliance in the Hainan Free Trade Port (HFTP) [8]. On the other hand, through a normative juridical approach and interviews with legal and technology experts, it was concluded that AI can improve the efficiency of regulatory monitoring and early detection of legal violations [4]. However, most studies still focus on the international context or large companies, while the application of AI for local MSMEs, particularly legal compliance among MSMEs in Karanganyar Regency, is still rarely discussed.

This research offers novelty by focusing on the application of an AI-based business management model to improve digital legal regulatory compliance among MSMEs in Karanganyar Regency. The use of AI by MSME players in this region is still very low. This research is important to fill this gap with a combination of qualitative and normative juridical approaches to provide practical solutions that can improve compliance with evolving digital legal regulations, in order to prevent potential violations that are detrimental to MSMEs.

Material and Methods

This study employs a qualitative approach as the primary method, complemented by a normative juridical approach, with the research conducted in Karanganyar Regency. The qualitative approach is used to gain an in-depth understanding of the adoption of digital technology and artificial intelligence by Micro, Small, and Medium Enterprises (MSMEs), particularly in relation to digital legal compliance [9]. Qualitative data were collected through in-depth interviews with purposively selected participants, including:

1. MSME actors in Karanganyar Regency who have adopted digital technologies,
2. Local regulators responsible for supervising and implementing MSME- and digital-related regulations, and
3. Legal and technology experts with expertise in digital law and AI.

The interviews focused on MSMEs' understanding of digital regulations, the extent of AI adoption, and the technical, legal, and institutional barriers to compliance [10]. The normative juridical approach was applied through a literature review of relevant laws, regulations, and legal documents, including Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 27 of 2022 on Personal Data Protection, as well as local regulations governing MSMEs in Karanganyar Regency [1],[2].

Importantly, the normative legal analysis is not limited to background context, but is explicitly integrated into the Results and Discussion to identify regulatory complexity, legal gaps, and compliance challenges faced by MSMEs. Data analysis was conducted using an interpretive approach, combining interview findings and legal analysis to assess how AI-based

management models can support digital legal compliance and to formulate policy-relevant recommendations.

Results

A. Data Analysis

The results of thematic analysis of interviews with MSME actors, legal practitioners, and information technology experts produced eight main themes. These themes provide a comprehensive picture of the structural challenges, capacity limitations, and opportunities for AI-based transformation to strengthen digital legal compliance among MSMEs in Karanganyar.

1. Addressing Digital Legal Literacy and Resource Constraints

The findings indicate that low digital legal literacy and resource constraints constitute structural barriers rather than incidental shortcomings. MSMEs do not merely lack information; they lack the organizational capacity to translate abstract legal norms into concrete operational routines. This is clearly reflected in the narratives of MSME actors. As P1, owner of Markas Pentol, explained,

> "I often hear about digital transaction rules, but when asked for details, I get confused and worry about making mistakes." Similarly, Mrs. Rubiyani noted, "The rules exist, but how to apply them in small businesses like ours is what confuses us."

These accounts illustrate a persistent gap between regulatory texts and day-to-day business practices. Consistent with small-firm regulation literature, MSMEs experience legal requirements as cognitively demanding and administratively burdensome because they lack internal legal or IT specialists [11]. The obligation to simultaneously manage production, marketing, and compliance creates what prior studies describe as compliance fatigue. Consequently, improving compliance cannot rely solely on increasing awareness; it requires reducing interpretive burdens through simplified guidance, standardized procedures, and embedded compliance mechanisms that align with MSMEs' limited resources.

2. Fear-Based Compliance versus Sustainable Compliance Cultures

The dominance of fear as a motivation for compliance highlights a fragile and short-term regulatory equilibrium. As articulated by a legal practitioner (P2),

> "Many business actors comply because they are afraid, not because they understand. Compliance driven by fear easily collapses when supervision weakens."

This observation aligns with compliance theory distinguishing between instrumental compliance (fear-driven) and normative compliance (understanding-driven).

In the MSME context, fear-based compliance may temporarily prevent violations but fails to foster learning or internalization of legal norms. Literature warns that deterrence-heavy approaches can suppress innovation and risk-taking, particularly among small firms already constrained by limited capital and knowledge [12]. The implication is that

sustainable compliance requires a shift toward supportive and educative regulatory approaches that enable MSMEs to perceive legal compliance as an enabler of business continuity rather than a constant threat.

3. Regulatory Fragmentation and the Problem of Legal Complexity

Regulatory fragmentation significantly amplifies compliance risks for MSMEs. Frequent regulatory changes and overlapping legal mandates create an environment of uncertainty that small firms are ill-equipped to navigate. As noted by P3,

> "The rules keep changing, but there is very little socialization. MSMEs are confused about which ones to follow."

This finding reinforces regulatory complexity theory, which argues that ambiguity and instability disproportionately burden smaller firms due to their limited monitoring capacity. In the digital governance context, rapid technological evolution further accelerates regulatory change, deepening uncertainty [13]. Without consolidated guidance or coherent interpretive frameworks, digital regulations risk becoming symbolic artifacts rather than actionable rules for MSMEs.

4. AI as an Instrument for Preventive and Embedded Compliance

The study reveals a clear expectation that AI could transform compliance from a reactive to a preventive process. An IT expert (P4) emphasized that AI could act as a "digital assistant" capable of detecting potential violations early, noting that "the main challenge lies in representative training data and adaptation to the local MSME context."

This aligns with emerging scholarship on compliance-by-design, where legal requirements are embedded directly into business processes [14]. For MSMEs, such systems could reduce dependence on external consultants and lower monitoring costs. However, the findings also caution against direct transplantation of enterprise-level AI systems. Without simplification and localization, AI risks reinforcing digital inequality rather than mitigating it. Therefore, AI-based compliance tools must be affordable, intuitive, and tailored to MSMEs' operational realities.

5. Trust and Explainability in AI-Based Compliance Tools

Trust and explainability emerged as decisive factors shaping AI acceptance. MSME actors expressed reluctance toward opaque systems, echoing concerns raised in explainable AI (XAI) literature. As one academic expert (P5) stated,

> "SMEs will find it difficult to accept systems that are perceived as black boxes. Algorithm transparency is crucial for building trust."

For MSMEs, explainability serves not only as a technical feature but also as a crucial governance mechanism. Understanding how and why a recommendation system enables business owners to justify decisions, conduct critical assessments, and maintain human control (human-in-the-loop) over legally sensitive processes. In the context of digital

regulation, this capability plays a crucial role in reducing information asymmetries between technology systems and users, while minimizing the risk of unnoticed errors. These findings strengthen the argument in the literature that explainability should be treated as a core compliance feature that supports accountability, transparency, and legitimacy of AI-based decisions, rather than simply an optional technical enhancement [15].

6. Consumer Trust, Data Protection, and Relational Business Models

Concerns about consumer data protection underscore the deeply relational nature of MSME business models, where economic transactions are embedded in personal trust and repeated social interactions rather than formal contracts. As P1 noted,

> "If customer data leaks, we could lose trust and repeat purchases."

It indicates that data misuse is perceived not merely as a legal violation but as a direct threat to business survival.

Unlike large firms that can absorb reputational shocks through branding or legal remediation, MSMEs depend heavily on localized reputational capital. From a theoretical perspective, privacy and trust literature suggests that data protection compliance functions as a signaling mechanism that communicates reliability and ethical conduct to consumers, thereby reinforcing long-term relational ties [16]. In this context, AI-based compliance tools must do more than ensure backend legal conformity; they must visibly demonstrate responsible data handling practices—such as clear consent mechanisms and transparent data use explanations—so that compliance strengthens, rather than erodes, existing trust norms within MSME–consumer relationships.

7. Institutional Support and Policy Alignment

The findings further highlight the pivotal role of local governments as institutional intermediaries between national digital regulations and MSME operational realities. As emphasized by P3,

> "The success of this system depends heavily on policy alignment between central government, local governments, and supporting institutions."

This reflects a broader institutional challenge in multilevel governance systems, where uniform national regulations often fail to account for local capacity variations.

Policy alignment theory posits that innovation-oriented regulation is effective only when regulatory objectives, implementation instruments, and user capabilities are mutually reinforcing [17]. In the MSME context, local governments are uniquely positioned to operationalize this alignment by translating abstract legal norms into actionable tools, providing financial and technical support for compliance technologies, and coordinating pilot initiatives with universities and technology providers. Without such localized

institutional mediation, AI-based compliance initiatives risk remaining technically viable but socially disconnected, thereby limiting adoption and reinforcing existing digital and regulatory inequalities among MSMEs.

Discussion

The findings of this study reveal that digital legal compliance among MSMEs is shaped by a complex interaction between structural capacity constraints, regulatory design, and socio-technical trust dynamics. Compliance gaps observed at the operational level do not primarily stem from resistance or neglect, but from a misalignment between the assumptions embedded in digital regulations and the actual organizational realities of MSMEs. Low digital legal literacy is therefore better understood as an institutional capacity deficit rather than an informational problem. MSMEs are exposed to regulatory norms, yet lack the cognitive, administrative, and technological infrastructure required to translate abstract legal provisions into routinized business practices. This reinforces arguments in small-firm regulation literature that uniform regulatory frameworks tend to privilege larger organizations while systematically disadvantaging smaller firms through disproportionate compliance costs [11].

The predominance of fear-based compliance further illustrates how regulatory environments oriented toward deterrence can unintentionally undermine sustainable compliance cultures. While sanction-oriented enforcement may generate short-term conformity, it discourages learning, experimentation, and internalization of legal norms. In resource-constrained MSMEs, fear-driven compliance amplifies risk aversion and reinforces perceptions of regulation as an external burden rather than a strategic asset. This finding extends compliance theory by demonstrating that instrumental compliance is particularly fragile in digitally evolving sectors, where adaptive learning is essential [12]. Sustainable compliance requires a regulatory shift toward supportive, educative, and capacity-building mechanisms that enable MSMEs to integrate legal considerations into business decision-making processes [13].

Regulatory fragmentation and legal complexity further exacerbate these vulnerabilities. Rapid regulatory changes, overlapping mandates, and limited socialization mechanisms create legal uncertainty that MSMEs lack the capacity to monitor and interpret independently. In the digital governance context, this complexity is intensified by technological dynamism, rendering static compliance strategies ineffective [14]. Without consolidated interpretive frameworks or adaptive guidance tools, digital regulations risk becoming symbolic rather than operational, widening the gap between formal legality and actual practice. This study thus reinforces regulatory complexity theory by highlighting how legal instability interacts with technological change to disproportionately burden small firms [11].

Within this constrained environment, AI emerges as a potentially transformative but deeply contingent compliance instrument. Participants' expectations of AI reflect a shift toward preventive and embedded compliance, where legal requirements are integrated directly into operational workflows. Such an approach aligns with the concept of compliance-by-design and offers the possibility of reducing dependence on external consultants while lowering long-term monitoring costs [15]. However, the findings caution that AI is not inherently democratizing. When designed for large enterprises and transferred uncritically, AI systems risk reinforcing digital inequality by imposing technical, financial, and cognitive demands beyond MSMEs' capacities. AI-based compliance tools must therefore be intentionally simplified, localized, and scaled to MSME realities to function as enabling rather than exclusionary technologies.

Trust and explainability emerge as central mediating variables in the adoption of AI-based compliance systems. For MSMEs, explainability performs a dual role: it supports technical usability and functions as a governance mechanism that preserves human oversight in legally sensitive processes. The ability to understand and contest algorithmic recommendations reduces information asymmetries between technology and users, strengthens accountability, and mitigates the risk of unnoticed compliance errors [16]. This finding contributes to explainable AI literature by situating explainability not merely as a design preference, but as a core legal compliance requirement in small-business contexts [17].

Concerns over consumer data protection further underscore the relational embeddedness of MSME business models. Unlike large firms, MSMEs depend heavily on localized trust and reputational capital, making data protection compliance inseparable from business sustainability [18]. Privacy compliance thus operates as a signaling mechanism that communicates ethical conduct and reliability to consumers. AI-based compliance tools must therefore visibly demonstrate responsible data practices to reinforce, rather than disrupt, existing trust relationships.

The findings position local governments as critical institutional intermediaries capable of aligning national digital regulations with MSME capacities. Policy alignment is essential to ensure that regulatory objectives, implementation instruments, and user capabilities evolve in tandem. Through simplified operational guidance, subsidized compliance technologies, and collaborative pilot programs with universities and technology providers, local governments can translate abstract legal norms into actionable practices. Without such institutional mediation, AI-based compliance initiatives risk remaining technically viable but socially inaccessible, ultimately reinforcing existing regulatory and digital divides.

Based on these findings, this study proposes a conceptual framework for AI-based compliance support for MSMEs that emphasizes the interaction between three key elements:

AI tools, government support, and MSME capacity building. AI tools participate in regulation and reduce compliance burdens, government support bridges national policies with local practices through subsidies and mentoring, while MSME capacity building ensures the critical and responsible use of AI. This framework views it as an ongoing socio-technological process, where the effectiveness of AI depends heavily on the alignment between technology design, institutional support, and user capabilities.

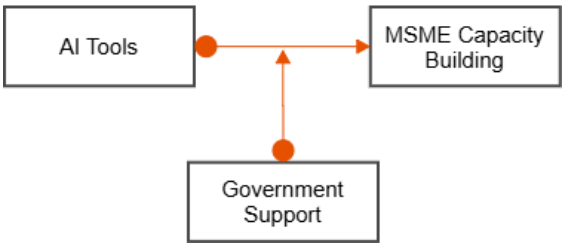


Fig. 1. Proposed Research Framework Model

Conclusion

This study demonstrates that digital legal compliance among MSMEs is not merely a technical or behavioral issue, but a structural and institutional challenge shaped by limited organizational capacity, regulatory complexity, and trust in digital technologies. Compliance gaps largely arise from the misalignment between uniform regulatory designs and the practical realities of MSMEs, leading to fear-based and fragile compliance practices rather than sustainable legal integration. While AI offers significant potential to support preventive and embedded compliance, its effectiveness depends on simplified, explainable, and context-sensitive design, as well as strong data protection to preserve consumer trust. The findings underscore the crucial role of local governments as policy intermediaries in aligning regulations, technology, and MSME capabilities through capacity building, institutional support, and collaborative innovation. An integrated approach that combines AI-based tools, supportive governance, and MSME empowerment is therefore essential to transform digital legal compliance from a regulatory burden into a foundation for sustainable and trustworthy digital business practices.

Limitation and Suggestions

This study has several limitations. First, empirical data was obtained from a limited number of informants, so it does not fully represent the diversity of MSME experiences in various sectors. Second, the analysis still focuses on the perspectives of business actors, technology practitioners, and lawyers, without directly involving regulators. Third, the qualitative approach in this study does not allow for broad generalization, although the findings provide relevant insights for similar contexts. Future research should involve a broader range of MSMEs across sectors and regions and include the perspectives of regulators

and consumers to strengthen contextual validity, while quantitative studies are needed to test the relationship between governance quality, AI adoption, and digital legal compliance. From a policy perspective, the findings call for targeted interventions, including the development of simplified visual compliance checklists that translate key provisions of the Personal Data Protection Law and the ITE Law into practical steps for MSMEs, as well as technology voucher schemes to subsidize access to affordable and explainable AI-based compliance tools. In addition, digital literacy programs should shift from general awareness to hands-on compliance simulations and sector-specific applications, supported by collaboration between local governments, universities, and technology providers to pilot user-friendly AI compliance solutions aligned with MSMEs' operational needs.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008, "tentang Informasi dan Transaksi Elektronik", doi: file:///C:/Users/User/Downloads/UU%20Nomor%2011%20Tahun%202008.pdf.

[2] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022, "tentang Perlindungan Data Pribadi", doi: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

[3] B. K. Karanganyar, "Profil Industri Mikro dan Kecil Kabupaten Karanganyar Tahun 2022," 2022, doi: https://karanganyarkab.bps.go.id/id/publication/2023/12/29/731350e6cdc0061cb90c9e7c/profil-industri-mikro-dan-kecil-kabupaten-karanganyar-2022.html.

[4] D. Wintara and Aan Fitriani, "Implementasi Model Manajemen Bisnis Berbasis Kecerdasan Buatan dalam Kepatuhan terhadap Regulasi Hukum Digital," *Journal of Digital Cyberlaw*, vol. 01, no. 01, pp. 7–12, 2025.

[5] M. El Hajj and J. Hammoud, "Unveiling the Influence of Artificial Intelligence and Machine Learning on Financial Markets: A Comprehensive Analysis of AI Applications in Trading, Risk Management, and Financial Operations," *Journal of Risk and Financial Management*, 2023, doi: 10.3390/jrfm16100434.

[6] K. Lipianina-Honcharenko, N. Maika, S. Sachenko, L. Kopania, and M. Soia, "A Cyclical Approach to Legal Document Analysis: Leveraging AI for Strategic Policy Evaluation," *CEUR Workshop Proceedings*, vol. 3736, pp. 201–211, 2024.

[7] V. I. Teremetskyi and Kovalchuk. O. Ya, "Artificial Intelligence As a Factor in the Development of Human Capital," *Forum Prava*, vol. 78, no. 1, pp. 106–115, 2024, doi: https://orcid.org/0000-0001-6490-9633.

[8] Y. Li, S. Wang, and M. B. Khaskheli, "Integrating Artificial Intelligence into Service Innovation, Business Development, and Legal Compliance: Insights from the Hainan Free Trade Port Era," *Systems*, vol. 12, no. 11, pp. 1–28, 2024, doi: 10.3390/systems12110463.

[9] M. N. Huda, A. Nurmandi, and S. Saefudin, "A Bibliometric Analysis Of Research On Digital Maturity: Research Streams, Influential Works And Future Research Paths," *Journal of Governance and Development*, vol. 21, no. 1, pp. 40–53, 2025, doi: 10.32890/ jgd2025.21.1.3 A.

[10] A. I. Hamzani, T. V. Widyastuti, N. Khasanah, and M. H. M. Rusli, "Implementation approach in legal research," *International Journal of Advances in Applied Sciences*, vol. 13, no. 2, pp. 380–388, 2024, doi: 10.11591/ijaas.v13.i2.pp380-388.

[11] D. Chambers, P. A. Mclaughlin, and T. Richards, "Regulation , entrepreneurship , and firm size," *Journal of Regulatory Economics*, vol. 61, no. 2, pp. 108–134, 2022, doi: 10.1007/s11149-022-09446-7.

[12] T. Wang and F. R. Trejo-macotela, "Revolutionizing biotech and pharmaceutical education with adaptive learning," *Frontiers in Education*, pp. 1–17, 2025, doi: 10.3389/feduc.2025.1679222.

[13] J. Mohan, M. Singh, and K. Rajeev, "Identification and investigation into the barriers to Green Lean Six Sigma implementation : a micro small and medium enterprises perspective," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 18, no. 8, pp. 6161–6175, 2024, doi: 10.1007/s12008-023-01551-x.
[14] Z. Kong, Q. Bian, and B. Fan, "How does digital transformation affect compliance performance : evidence from listed corporations in China," *Journal of Financial Reporting and Accounting*, 2025, doi: 10.1108/JFRA-01-2025-0010.
[15] R. Christiaanse and J. Hulstijn, "Control Automation to Reduce Costs of Control," *International Journal of Information System Modeling and Design*, vol. 4, no. 4, pp. 27–47, 2013, doi: 10.4018/ijismd.2013100102.
[16] H. Yang, D. Li, and P. Hu, "Technology in Society Decoding algorithm fatigue : The role of algorithmic literacy , information cocoons , and algorithmic opacity," *Technology in Society*, vol. 79, pp. 1–12, 2024, doi: 10.1016/j.techsoc.2024.102749.
[17] S. Sapienza and M. Palmirani, "Algorithmic Knowability: A Unified Approach to Explanations in the AI Act," in *Communications in Computer and Information Science*, 2025. doi: 10.1007/978-3-032-08317-3.
[18] M. F. Cabrera and Y. A. Peña, "Incidence of trust in corporate value generated by ICT in commerce and services microbusinesses," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 8, pp. 1–19, 2024.

Authors



Marina Ramadhani is a lecturer in Business Law at Muhammadiyah University of Karanganyar. She earned her Bachelor of Laws degree from Sriwijaya University, Palembang, and her Master of Laws in Business Law from Gadjah Mada University, Yogyakarta. Her expertise lies in Business Law, particularly Intellectual Property Rights. She has been actively involved in legal research and academic activities related to digital law and regulatory compliance. (email: marinaramadhani80@gmail.com).



Arseto Endro Supriyanto is a lecturer in Business Law at Muhammadiyah University of Karanganyar. He holds a Master of Laws degree with a concentration in Business Law from Sebelas Maret University. His academic and professional expertise includes business law, energy law, and mining law. He has contributed to research and teaching in the legal aspects of industry and natural resources governance. (email: supriyantoendroseto@gmail.com).



Yayu Sri Rahayu is a lecturer in Computer Engineering at Muhammadiyah University of Karanganyar. She obtained her Master's degree in Computer Science from Gadjah Mada University. Her expertise includes database systems, programming, and decision support systems. She has extensive experience in applying information technology to solve practical problems and support organizational decision-making processes. (email: rahayu1972@gmail.com).