



DIGITAL TRANSFORMATION AND THE ETHICS OF PROFESSIONAL RESPONSIBILITY: A *MAQĀṢID AL-SHARĪ'AH* PERSPECTIVE

Irfan Udin

Sekolah Tinggi Agam Islam Ki Ageng Pekalongan, Indonesia
irfanudin@staikap.ac.id

ABSTRACT

Digital transformation has reshaped the professional landscape through the increasing use of artificial intelligence, big data, and social media, while simultaneously generating ethical challenges, including technology misuse, privacy violations, and disinformation. This study aims to examine the role of professional codes of ethics in addressing digital ethical challenges through the perspective of *maqāṣid al-sharī'ah*. Employing a qualitative approach, the study combines a literature review with case analysis, including the scandal involving the Community Vocational Training Center (Balai Latihan Kerja Komunitas/BLKK) of the Islamic Scholars Association (PP) in Pekalongan City. The findings indicate that professional codes of ethics function not merely as normative instruments governing professional conduct but also as mechanisms for protecting public welfare in accordance with the objectives of *maqāṣid al-sharī'ah*, particularly *ḥifẓ al-'aql* (protection of intellect), *ḥifẓ al-māl* (protection of wealth), *ḥifẓ al-'ird* (protection of dignity), and *ḥifẓ al-nafs* (protection of life). The implementation of professional codes of ethics through strengthened digital ethics literacy, professional oversight, and technology-responsive regulatory reform can prevent harm, enhance accountability, and sustain public trust. The findings of this study contribute to proposing the integration of professional codes of ethics with *maqāṣid al-sharī'ah* as an adaptive ethical framework for strengthening professionalism in the digital era.

Keywords: *Professional Ethics, Digital Transformation, Maqāṣid al-Sharī'ah*

A. Introduction

Digital transformation has brought about significant changes across various professional fields, including technology, journalism, healthcare, and law (Moh. Irsyad Hanif, 2024). Innovations such as artificial intelligence and data analytics have enhanced efficiency, automation, and data-driven decision-making. In journalism, digital tools facilitate faster reporting while supporting the quality and reliability of information. In other professional sectors, digital technologies have improved work efficiency and enabled online service delivery. Although this transformation presents challenges related to adaptation and data protection, it also creates substantial opportunities for innovation and the development of digital competencies (Shiddiq & Sathori, 2025).

Furthermore, advances in digital technology have significantly influenced public trust, particularly in the provision of public services and interactions between governments and citizens (Stoumpos et al., 2023). The use of technology in public services can facilitate more efficient, transparent, and accessible processes, ultimately enhancing citizen satisfaction and trust in government institutions. Digital platforms and real-time reporting systems enable the public to monitor service delivery, thereby promoting accountability and active civic participation (Sarjito, 2024). Nevertheless, privacy breaches, such as the data leakage incident involving the eHAC application, demonstrate that public trust can be easily undermined in the absence of adequate data protection systems. Therefore, information security and the application of ethical principles in data management are of critical importance. Ethical guidelines are needed to ensure explicit consent, continuous monitoring of digital systems, and the prevention of bias in the use of technologies such as artificial intelligence. Strong regulatory frameworks, enhanced digital literacy, and capacity building for public officials are also necessary to ensure that digital public services remain secure, equitable, and trusted by society (Zebua & Zebua, 2025).

The implementation of digital systems in public services promotes faster, more transparent, and more accessible processes, thereby increasing citizen satisfaction and confidence in government performance (Putri, 2024). The availability of online information portals and real-time reporting mechanisms enables citizens to monitor public services directly, strengthening accountability and public engagement (Mokobombang et al., 2023). Moreover, more open interaction through digital channels can foster more inclusive and responsive relationships between the state and its citizens. However, privacy violations, such as the data breach involving the eHAC application, demonstrate that trust, once established, can rapidly deteriorate without adequate data protection mechanisms. Accordingly, information security and ethical data governance constitute fundamental principles that must be safeguarded (Jumalia Mannayong et al., 2024). In this context, robust ethical standards are required, encompassing

informed consent for data use, systematic oversight of digital systems, and safeguards against potential biases arising from the deployment of advanced technologies such as artificial intelligence. Clear regulations, increased public digital literacy, and continuous training for public officials are essential components in developing digital public service systems that are fair, secure, and trusted across society (Shiddiq & Sathori, 2024).

This study aims to analyze the role of professional codes of ethics in strengthening integrity and ethical governance amid digital transformation, particularly in addressing issues of data privacy, misuse of personal information, digital manipulation, disinformation, and the development of artificial intelligence. The study examines professional codes of ethics not merely as regulatory instruments but also as moral frameworks that guide professional practices toward the protection of human dignity, freedom, security, and welfare. The perspective of *maqāṣid al-sharī'ah* is employed as an analytical framework to identify *maṣlaḥah* (benefit) and *mafsadah* (harm) in digital practices through the principles of *ḥifẓ al-ʿird* (protection of dignity and honor), *ḥifẓ al-naḥs* (protection of life), *ḥifẓ al-ʿaql* (protection of intellect), and *ḥifẓ al-māl* (protection of wealth), alongside the values of trustworthiness (*amānah*), justice, transparency, and responsibility. The study employs a qualitative approach combining a literature review and case analysis, including the case of the scandal involving the Community Vocational Training Center (Balai Latihan Kerja Komunitas/BLKK) of PP Pekalongan City. The case is examined to assess the ethical consequences of collecting and utilizing personal data and to compare them with technology governance practices emphasizing transparency, data protection, and accountability. The analysis is directed toward developing a conceptual understanding of how professional codes of ethics can be adaptively reconstructed to respond to the complexities of digital technologies while ensuring that technological innovation remains within the ethical boundaries of integrity, justice, rights protection, and human welfare.

This study is expected to produce a conceptual framework for the ethics of digital public services that is oriented not only toward technological efficiency but also toward the protection of human welfare and dignity. Through the perspective of *maqāṣid al-sharī'ah*, the study seeks to demonstrate that data protection, transparency, bias prevention, accountability, and public participation constitute ethical manifestations of efforts to prevent harm and realize public welfare. The findings are expected to strengthen the understanding that professional codes of ethics must be dynamically developed in response to technological change while remaining firmly grounded in the principles of justice, responsibility, trustworthiness, and the protection of citizens' rights. Accordingly, the integration of professional ethics and *maqāṣid al-sharī'ah* is expected to offer a normative-

philosophical framework for establishing digital public services that are secure, fair, transparent, inclusive, and capable of sustaining public trust

B. Professional Codes of Ethics and Integrity

Professional integrity refers to attitudes and behaviors characterized by honesty, accountability, and a commitment to adhering to ethical standards in the performance of professional duties. Professionals with integrity consistently act honestly, transparently, and responsibly in relation to their decisions and actions. They maintain coherence between their moral values and everyday professional practices. Integrity thus constitutes a fundamental foundation for ensuring that a profession remains trusted and respected by clients and society at large.

Various professions have established codes of ethics that function as moral guidelines and standards of conduct for their members. In journalism, for example, professional codes of ethics require journalists to present information that is truthful, accurate, balanced, and independent. Journalists are also expected to fulfill their social responsibilities, avoid discriminatory reporting, and maintain public trust.

In the medical profession, codes of ethics emphasize the priority of patient safety and well-being, the confidentiality of medical information, honesty and fairness in the provision of healthcare services, and a commitment to continuously improving professional competence. In the field of information technology, ethical codes emphasize the importance of protecting public safety and welfare, maintaining honesty, avoiding conflicts of interest, safeguarding user data confidentiality, and continuously developing both technical and ethical competencies.

Professional codes of ethics function as moral standards and behavioral guidelines that foster integrity and professionalism within a profession. Compliance with ethical codes demonstrates professionals' commitment to the principles of honesty, responsibility, and justice. Such commitment directly contributes to strengthening public trust in the profession. This trust is particularly important because it provides a foundation for healthy relationships between professionals and the clients or communities they serve.

Furthermore, the reputation of a profession is strongly influenced by its members' adherence to ethical standards. Violations of professional codes of ethics may negatively affect the image of the profession, undermine its credibility, and ultimately erode public trust. Conversely, professions that consistently uphold high ethical standards are more likely to gain public respect and maintain a strong position within society. Therefore, codes of ethics serve not only to protect the interests of individual professionals but also to safeguard the dignity, credibility, and long-term sustainability of the profession as a whole.

C. Challenges to Professional Integrity in the Digital Era

Membership data over the 2020–2024 period indicate a consistent increase in the number of TABUR financing participants. The growth trend reflects farmers' positive response to the product and suggests a relatively high level of trust in the institution. This trend can be interpreted as evidence that Rahn-based financing addresses practical financing constraints more effectively than informal lending and conventional credit alternatives. (Syahrurromdhoni et al., 2024)

The misuse of digital technologies, particularly through information manipulation such as deepfakes, misinformation on social media, and biased algorithms, has become a serious concern in the contemporary digital era. Deepfake refers to artificial intelligence-based technology capable of generating highly realistic fabricated videos or audio recordings that imitate a person's face or voice. One example of such misuse involved a figure associated with the Community Vocational Training Center (Balai Latihan Kerja Komunitas/BLKK) of PP Pekalongan City, who was digitally portrayed as speaking Mandarin through AI-generated content.

Social media has become a primary medium for the dissemination of false information, a phenomenon further exacerbated by AI-driven algorithms. These algorithms can promote user engagement by reinforcing particular narratives and creating echo chambers in which hoaxes and misinformation are disseminated on a massive scale (Bua & Idris, 2024). This situation presents a significant challenge as deepfake technologies become increasingly accessible. Such misuse has the potential to threaten social stability and democratic integrity, thereby necessitating stronger regulations, improved digital literacy, and more sophisticated technologies for detecting misinformation and manipulated content.

Privacy violations also constitute a major ethical challenge. Technology companies and professionals who neglect ethical principles in managing personal data may generate serious consequences, particularly with regard to public trust. Personal data breaches, whether caused by technical negligence or deliberate misuse, can damage organizational reputations and create a sense of insecurity among members of the public when accessing digital services. Consequently, citizens may become reluctant to participate in government programs or use technology-based public services. In certain circumstances, such distrust may even affect citizens' compliance with state obligations, including tax payments.

Data breaches involving government institutions or major technology companies, such as Facebook, illustrate how public trust can decline dramatically when personal data protection mechanisms fail. Citizens may become skeptical of the competence and good faith of digital service providers, ultimately eroding public confidence. The consequences of data breaches extend beyond trust, affecting organizational reputation and economic conditions. Organizations experiencing data breaches may face extensive negative publicity, declines in

market value, legal sanctions, substantial costs associated with system recovery, and compensation for affected users. Such losses may result in customer attrition and weakened market share. Data breaches can also produce psychological and social consequences, including anxiety, insecurity, and uncertainty, which may undermine social stability and impede the broader process of national digital transformation.

In addition to challenges related to personal data management and privacy, commercial pressures constitute another important factor influencing ethical conduct in business, particularly in marketing. Companies and marketers often face pressure to achieve high sales targets, which may encourage them to disregard ethical principles in pursuit of short-term financial gains. Unethical practices, such as the use of clickbait headlines or misleading content merely to attract consumer attention and generate clicks, may emerge from such pressures. These practices not only harm consumers but may also undermine corporate reputation.

One concrete example of ethical violations in marketing is the use of highly targeted advertising based on consumers' personal data. In practice, personal information such as location, browsing behavior, and user preferences may be collected and analyzed to deliver highly personalized advertisements. However, when such data are collected without clear consent or adequate transparency, these practices may violate users' privacy and create a perception of manipulation. This condition constitutes a serious ethical issue requiring greater attention because it directly concerns consumer rights and public trust (Petra & Christianto, 2024).

Key ethical principles that should be upheld in marketing include honesty and transparency. Companies have a responsibility to provide accurate and non-misleading information about their products and services while transparently explaining how consumer data are collected and used. Social responsibility is also an essential dimension, requiring businesses to carefully consider the social and environmental consequences of their marketing activities. If companies persist in unethical practices such as clickbait and privacy violations, they face substantial risks of reputational damage and loss of consumer trust, as well as potential legal consequences.

D. The Role of Professional Codes of Ethics in Safeguarding Integrity

Professional codes of ethics function as written moral foundations that guide professionals in navigating complex ethical situations, particularly in the development and application of advanced technologies such as artificial intelligence (AI). In this context, codes of ethics articulate moral values and professional responsibilities that must be upheld to ensure that technology is developed and used in ways that are humane, secure, and responsible. One

important reference in AI ethics is the set of principles developed by the Institute of Electrical and Electronics Engineers (IEEE). These guidelines seek to encourage engineers and technology developers to design AI systems that prioritize not only technical advancement but also their broader social consequences. The principles developed by IEEE emphasize the importance of transparency toward the public concerning how AI systems operate and what types of data they utilize (Prasetya et al., 2024). Such transparency is intended to enable users to understand the processes underlying decisions generated by AI systems.

Ethical awareness cannot be adequately developed through professional experience alone. Continuous education and training are necessary to ensure that professionals remain sensitive to ethical dilemmas and are capable of making responsible decisions amid the complexities of modern technology. Structured training programs can cultivate values such as integrity, social responsibility, and respect for users' privacy rights. Organizations are therefore expected to provide continuous learning opportunities as an integral component of an ethical organizational culture.

Alongside the growing importance of professional responsibility and ethical awareness in information technology management, there is an urgent need to update professional codes of ethics so that they remain aligned with increasingly complex technological developments. Digital transformation and the emergence of AI have generated new ethical challenges that are not fully accommodated by conventional codes of ethics. Accordingly, professional codes must be continuously adapted to preserve their relevance and effectiveness in guiding professional conduct in the digital era.

Emerging technologies have introduced distinctive ethical concerns, including algorithmic bias, privacy violations, limited system transparency, and data security risks. In this context, the revision of professional codes of ethics should incorporate principles of fairness, accountability, security, and respect for human rights. In AI development, for example, professionals must ensure that systems do not produce discriminatory outcomes, that data are collected and processed ethically, and that AI-generated decisions can be adequately explained to users in a transparent and comprehensible manner.

E. Protecting Personal Data and Professional Integrity: Reconstructing Digital Ethics through the Lens of *Maqāṣid al-Sharī'ah*

One concrete example of a violation of professional ethics in the digital era is the scandal involving the Community Vocational Training Center (Balai Latihan Kerja Komunitas/BLKK) of PP Pekalongan City. In this case, BLKK PP Pekalongan City allegedly accessed Facebook users' personal data without obtaining direct consent from the data subjects. The information reportedly collected included user profiles, social connections, and personal preferences, which were subsequently

utilized to construct psychological profiles of users. The consequences of such a violation can be substantial. Public trust in social media platforms, particularly Facebook, may decline significantly when users perceive that their privacy has been compromised. Many users may become uncomfortable using digital platforms due to concerns regarding how their personal information could be accessed or utilized without their knowledge or control. Consequently, users may reduce their online activities because of heightened concerns about digital data protection.

The case may also have broader political and social implications. The use of personal data to manipulate voters' perceptions can undermine the integrity of democratic processes. Manipulative political microtargeting may generate information asymmetries, contribute to social polarization, and potentially threaten political and social stability. Concerns about external interference and covert influence in electoral processes may become more pronounced when such manipulative data practices are exposed.

Conversely, several technology companies have demonstrated efforts to implement principles of digital ethics. Google and Microsoft, for instance, have developed artificial intelligence governance and ethical frameworks that emphasize transparency in algorithmic systems and safeguards against potential bias. They also publish transparency reports and other governance disclosures intended to inform the public about how data and digital systems are managed and protected. Such measures reflect an institutional commitment to social responsibility and professional accountability in the management of user data. From the perspective of *maqāṣid al-sharī'ah*, personal data protection should not be understood merely as a matter of technical cybersecurity but also as an effort to safeguard human dignity, freedom, security, and welfare. At its core, *maqāṣid al-sharī'ah* is oriented toward the realization of *maṣlaḥah* (benefit or welfare) and the prevention of *mafsadah* (harm). Accordingly, access to and utilization of personal data should take into account data subjects' rights, the purpose of data processing, the degree of potential benefit, and the risks of harm resulting from its use.

First, accessing personal data without consent can be analyzed through the principle of *ḥifẓ al-ʿird* (protection of honor and human dignity). Personal data, including profiles, social relationships, preferences, and psychological characteristics, represent important dimensions of an individual's identity and private life. When such information is collected without the knowledge or consent of the data subject, it may constitute an intrusion into personal privacy and human dignity. In the digital context, safeguarding honor extends beyond protection from direct insult or defamation; it also involves preventing personal information from being covertly exploited to construct perceptions of individuals or influence their behavior.

Second, such practices are relevant to *ḥifẓ al-nafs* (protection of life and personal well-being). The exploitation of psychological data for manipulation or political microtargeting may generate psychological pressure, insecurity, fear, and social anxiety. When individuals lose a sense of security within digital spaces, technologies intended to facilitate human activities may instead become sources of psychological vulnerability. Therefore, the principle of *ḥifẓ al-nafs* requires digital technologies to be developed and utilized with due regard for users' safety, psychological well-being, and overall welfare.

Third, the case can be examined through *ḥifẓ al-'aql* (protection of intellect). This dimension becomes particularly significant when personal data are used to construct psychological profiles and selectively deliver political information to specific groups. Manipulative microtargeting can potentially influence individuals' reasoning processes and decision-making by tailoring information to their vulnerabilities, preferences, or psychological tendencies. From a *maqāṣid* perspective, the freedom to think and the capacity to make rational and autonomous decisions constitute forms of human welfare that must be protected. Consequently, technology should not be employed to exploit individuals' psychological conditions for particular political or economic interests.

Fourth, the collection and utilization of personal data without authorization can also be associated with *ḥifẓ al-māl* (protection of wealth and property). In the digital economy, personal data possess considerable economic value. Data may be used for commercial purposes, targeted marketing, behavioral analysis, and the generation of economic benefits for particular actors. When individuals lose control over data that possess economic value, questions arise concerning the fairness of benefit distribution and the ownership of the value generated from such data. From the perspective of *maqāṣid*, the utilization of economic resources should be conducted fairly, transparently, proportionately, and without exploitation.

Fifth, the issue also involves *ḥifẓ al-dīn* (protection of religion), particularly when digital ethics are understood as an application of Islamic moral values. Islam emphasizes truthfulness (*ṣidq*), trustworthiness (*amānah*), justice (*'adl*), and the prohibition of causing harm to others as fundamental ethical principles. The covert collection and manipulative use of personal data are inconsistent with the principle of *amānah*, because parties granted access to personal information bear a moral responsibility to use such data only for legitimate, transparent, and properly authorized purposes.

Thus, the central ethical issue does not lie in the use of technology or personal data per se, but rather in how data are obtained, processed, utilized, and subjected to accountability. Data practices that are transparent, proportionate, consent-based, purpose-specific, and protective of users' rights are more consistent with the principle of *maṣlaḥah*. Conversely, covert and manipulative

data practices tend to conflict with the objectives of *maqāṣid al-sharī'ah* because they may generate broader forms of harm and undermine human dignity, autonomy, security, and public trust

F. Conclusion

This study concludes that professional codes of ethics in the digital era function not merely as normative rules for regulating professional conduct but also embody a *maqāṣid al-sharī'ah* dimension oriented toward safeguarding human welfare. The development of artificial intelligence, big data, and social media necessitates a broader understanding of professional integrity, extending beyond mere compliance with established rules toward a form of moral responsibility that protects human dignity, autonomy, security, and the rights of technology users. Within the framework of *maqāṣid al-sharī'ah*, transparent and responsible data governance can be associated with *ḥifẓ al-'ird* (protection of honor and dignity), *ḥifẓ al-nafs* (protection of life and well-being), *ḥifẓ al-'aql* (protection of intellect), and *ḥifẓ al-māl* (protection of wealth and property). Conversely, data misuse, privacy violations, information manipulation, and disinformation, as illustrated by the cases examined in this study, constitute forms of *mafsadah* because they may undermine individual autonomy, erode public trust, and generate social injustice and instability. Accordingly, professional codes of ethics can be positioned as instruments of *ḥifẓ al-maṣlaḥah* that bridge technological advancement with the humanitarian objectives of Islamic law.

The implications of these findings suggest that strengthening professional integrity in the digital era should focus on developing an ethical ecosystem that extends beyond the formulation of professional codes of ethics. Such an ecosystem requires continuous ethics education and training, institutional oversight, transparency in technology governance, and the continuous revision of professional standards to remain responsive to developments in AI and other digital technologies. The *maqāṣid al-sharī'ah* perspective emphasizes that technological innovation gains ethical legitimacy insofar as it generates *maṣlaḥah* and minimizes *mafsadah*. In this regard, the legal-ethical maxim *dar'u al-mafāsīd muqaddam 'alā jalb al-maṣāliḥ*—preventing harm takes precedence over securing benefits—provides an important foundation for professional decision-making. Therefore, professional integrity amid digital transformation should not be oriented solely toward efficiency, productivity, or regulatory compliance, but toward establishing technology governance grounded in trustworthiness, justice, transparency, and respect for human dignity. This framework further demonstrates the conceptual relevance of *maqāṣid al-sharī'ah* as a paradigm for digital ethics that understands technology not as an end in itself, but as an instrument for realizing sustainable human welfare.

References

- Anita Sinaga, N. (2020). Kode etik sebagai pedoman pelaksanaan profesi hukum yang baik. *Jurnal Ilmiah Hukum Dirgantara*, 10(2). <https://doi.org/10.35968/jh.v10i2.460>
- Bahari, P. K., Marianah, D., Sumarni, T., Mas'ula, S., & Pristiani, R. (2025). Mengintegrasikan etika keilmuan dalam pendidikan: Implikasi bagi penulisan karya tulis ilmiah modern. *Jurnal Pendidikan Dasar Perkhasa: Jurnal Penelitian Pendidikan Dasar*, 11(1), 213–. <https://doi.org/10.31932/jpdp.v11i1.4317>
- Bua, I. T., & Idris, N. I. (2024). Analisis kebijakan keamanan siber di Indonesia: Studi kasus kebocoran data nasional pada tahun 2024.
- Hanif, M. I. (2024). Aspek hukum pengaruh transformasi digital terhadap praktik telemedicine di Indonesia. *Parlementer: Jurnal Studi Hukum dan Administrasi Publik*, 1(2), 55–64. <https://doi.org/10.62383/parlementer.v1i2.48>
- Mannayong, J., Rizal S., M., Herling, & Faisal, M. (2024). Transformasi digital dan partisipasi masyarakat: Mewujudkan keterlibatan publik yang lebih aktif. *Jurnal Administrasi Publik*, 20(1), 53–75. <https://doi.org/10.52316/jap.v20i1.260>
- Mokobombang, W., Syafaruddin, S., Syafaruddin, A. R. A., Khaeriyah, K., & Natsir, N. (2023). Dampak perubahan layanan publik yang disebabkan oleh teknologi dan media sosial. *Journal of Business, Finance, and Economics (JBFE)*, 4(1), 348–359. <https://doi.org/10.32585/jbfe.v4i1.4180>
- Petra, G. C., & Christianto, N. C. (2024). *Etika pemasaran: Membangun kepercayaan dan keberlanjutan di masyarakat*.
- Prasetya, R. N., Kusdiyanto, A., Radiana, U., & Wicaksono, L. (2024). Etika dalam pengembangan artificial intelligence: Tinjauan pedoman dan penerapannya. *Juwara: Jurnal Wawasan dan Aksara*, 4(1), 240–253. <https://doi.org/10.58740/juwara.v4i1.271>
- Putri, N. (2024). *Etika di era digital: Tantangan teknologi informasi modern*.
- Sandi, A., Wijayanti, A., Arafah, G. H. I., Milati, S. K., & Bifadillah, P. (2022). Bentuk pelanggaran kode etik serta sanksi pelanggaran kode etik profesi hakim tindak pidana korupsi. *Moderation: Journal of Islamic Studies Review*, 2(1), 119–128. <https://doi.org/10.63195/moderation.v2i1.40>
- Sarjito, A. (2024). Hoaks, disinformasi, dan ketahanan nasional: Ancaman teknologi informasi dalam masyarakat digital Indonesia. 5(2).
- Shiddiq, M. I., & Sathori, A. (2024). *Transformasi digital profesi hukum: Peran dan kontribusi profesi hukum pada masyarakat modern di era digitalisasi*.
- Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital transformation in healthcare: Technology acceptance and its applications. *International Journal of Environmental Research and Public Health*, 20(4), 3407. <https://doi.org/10.3390/ijerph20043407>

- Syahda, F. L., Nur'aisyah, Y., & Rachman, I. F. (2024). Pentingnya pendidikan etika digital dalam konteks SDGs 2030. *Perspektif: Jurnal Pendidikan dan Ilmu Bahasa*, 2(2), 66–80. <https://doi.org/10.59059/perspektif.v2i2.1259>
- Wardani, V. G., Santosa, H. P., & Setyabudi, D. (n.d.). *Pengaruh terpaan berita kebocoran data penduduk dan terpaan negative e-word of mouth di media sosial terhadap tingkat kepercayaan masyarakat pada pemerintah pusat dalam menangani kasus kebocoran data.*
- Zaelany, F. A., & Putranti, I. R. (2023). Pelanggaran privasi dan ancaman terhadap keamanan manusia dalam kasus BLKK PP Kota Pekalongan. *Journal of International Relations Diponegoro*, 9(1), 125–137. <https://doi.org/10.14710/jirud.v9i1.37259>
- Zebua, D. Y., & Zebua, A. P. (2025). Tantangan etika dalam profesi teknologi informasi. *Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, 2(1), 35–44. <https://doi.org/10.70134/identik.v2i1.162>