JGSP
Jurnal Greenation Sosial dan Politik
+62 81210467572 https://greenationpublisher.org/JGSP greenation.info@gmail.com
GREENATION PUBLISHER

DOI: https://doi.org/10.38035/jgsp.v3i3

Strengthening Polri Law Enforcement through Digital Identification Systems to Realize Domestic Security Stability (KAMDAGRI)

Wido Dwi Arifiya Zaen[1], Joko Setiono[2], Ilham Prisgunanto[3]
[1]Sekolah Tinggi Ilmu Kepolisian, Indonesia, wido.zaen@gmail.com
[2]Sekolah Tinggi Ilmu Kepolisian, Indonesia, joko_setiono@ymail.com
[3]Sekolah Tinggi Ilmu Kepolisian, Indonesia, prisgunanto@gmail.com

Corresponding Author: wido.zaen@gmail.com[1]

Abstract: Digital transformation is an integral part of the modernization of law enforcement institutions, including Polri, in maintaining domestic security stability (Kamdagri). The utilization of digital technologies such as the Automated Biometric Identification System (ABIS), face recognition, and integration of population data are strategic steps taken by Polri to increase the effectiveness of law enforcement. This study uses a normative juridical method by reviewing relevant legislation, such as Law Number 2 of 2002 on the Indonesian National Police, Law Number 27 of 2022 on Personal Data Protection, and Minister of Communication and Informatics Regulation Number 5 of 2020 on the Implementation of Electronic Systems in the Private Sector. The study's findings show that digital identification systems can enhance the efficiency of crime detection and handling but pose serious legal challenges, such as privacy protection, system accuracy, and potential data misuse. There is a need for a more specific and updated internal legal basis within Polri to regulate the governance of these digital technologies. This journal proposes integrating the principles of transparency, accountability, and human rights protection at every stage of implementing identification technology to ensure synergy between security interests and the protection of civil right.

Keyword: Polri, Law Enforcement, Digital Identification, Kamdagri, ABIS, Personal Data

Abstrak: Transformasi digital merupakan bagian integral dari modernisasi lembaga penegak hukum, termasuk Polri, dalam menjaga stabilitas keamanan dalam negeri (Kamdagri). Pemanfaatan teknologi digital seperti Sistem Identifikasi Biometrik Otomatis (ABIS), pengenalan wajah, dan integrasi data kependudukan merupakan langkah strategis yang diambil oleh Polri untuk meningkatkan efektivitas penegakan hukum. Penelitian ini menggunakan metode yuridis normatif dengan meninjau peraturan perundang-undangan yang relevan, seperti Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Pelaksanaan Sistem Elektronik di Sektor Swasta. Temuan studi menunjukkan bahwa sistem identifikasi digital dapat meningkatkan efisiensi dalam deteksi dan penanganan kejahatan, namun menimbulkan tantangan hukum yang serius, seperti perlindungan privasi, akurasi sistem, dan potensi penyalahgunaan data. Diperlukan landasan hukum internal yang lebih spesifik dan diperbarui di dalam Polri untuk mengatur tata kelola teknologi digital ini. Jurnal ini mengusulkan untuk mengintegrasikan prinsip transparansi, akuntabilitas, dan perlindungan hak asasi manusia pada setiap tahap implementasi teknologi identifikasi guna memastikan sinergi antara kepentingan keamanan dan perlindungan hak sipil.

Kata kunci: Polri, Penegakan Hukum, Identifikasi Digital, Kamdagri, ABIS, Data Pribadi

INTRODUCTION

Digital transformation is an essential part of institutional reform within the Indonesian National Police (Polri) in the modern era (Hasibuan, 2023). Developments in information and communication technology have brought major changes in the way law enforcement agencies operate worldwide, including in Indonesia (Absah, 2024). Polri can no longer rely on conventional methods in carrying out its duties to maintain public security and order. Crime dynamics have become increasingly complex, both in terms of modus operandi and geographic scope, demanding faster, more accurate, and data-driven responses (Supratman, 2020). This underlies the importance of integrating digital systems into the law enforcement process as an effort to enhance the effectiveness and efficiency of police institutional work (Sinaga, 2024).

One tangible form of Polri's digital transformation is the implementation of a digital identification system. This system includes the use of biometric technologies such as fingerprint scanning, iris scanning, and facial recognition in the process of identifying perpetrators of crime (Wibowo, 2023). This technology can increase accuracy in identity tracing and speed up case handling time, especially in cases involving multiple parties and cross-regional incidents. Digital identification also plays a crucial role in crime prevention, for instance in early detection systems for individuals on the wanted list or those with a criminal record (Agustoni, 2023). This system supports Polri's broader goal of proactively and precisely maintaining national security stability (Kamdagri).

Stability in Kamdagri serves as a fundamental pillar in preserving national unity, especially in the face of contemporary security threats that are cyber-based, transnational, and even without physical perpetrators (Manafe, 2023). Digital identification expands Polri's monitoring reach without the need for more personnel on the ground, through the use of smart surveillance cameras connected to the national population database (Darmawan, 2024). This creates a situation where security control can be conducted in a layered, swift manner with minimal risk of human error. Kamdagri stability is not merely about responding to criminal incidents but also about the state's ability to build effective detection and prevention systems. In this regard, technology bridges the need for fast information and targeted legal actions (Mubarok, 2023).

From a theoretical perspective, the legal system described by Lawrence Friedman consists of three main elements: structure, substance, and legal culture (Al Kautsar, 2022). The digital transformation of Polri touches all these aspects, from organizational structure adapting to the presence of technology and cyber divisions, to legal substance being required to adjust to digital instruments (Djatiutomo, 2023). Legal culture also changes, both internally within the institution and among the public as users of police services. Society is now accustomed to online reporting, report status tracking, and data-driven perpetrator identification, all of which have become part of a digital legal culture (Cahya, 2024). All three must move in unison so that the system built does not become unbalanced in its field implementation.

Legal effectiveness is not sufficiently measured by the number of solved cases or arrested perpetrators. Legal effectiveness is also reflected in how far the presence of the law can provide a sense of security and legal certainty to the broader public (Orlando, 2022). This is where the strategic value of digital identification lies: it is not merely a technical tool, but part of a legal strategy to strengthen public trust in the police institution. When the public feels that criminals can be immediately and accurately identified, a sense of security arises that becomes a key element of public order. This digital innovation must be viewed as part of legal system reform, not just a modernization of work tools.

Digital identification is also a product of scientific advancement in the field of biometrics. Technologies such as fingerprint scans, iris recognition, and facial recognition are not new, but they have now been refined through integration with big data and artificial intelligence (AI) (Windani, 2023). This combination allows systems to analyze patterns, recognize anomalies, and even predict potential criminal acts based on historical data. In this context, digital identification is not only reactive but also preventive. Systems capable of linking the faces of perpetrators with their digital records across platforms can accelerate investigation processes and minimize law enforcement errors.

Big data serves as the foundation in digital-based public security systems (Nainggolan, 2023). All biometric information collected, including population data, medical records, digital movement data, and legal history, becomes a unified whole that can be automatically processed for security purposes. AI then acts as the ‘brain’ of this system, able to recognize suspicious patterns and provide recommendations to law enforcement officers (Kushariyadi, 2024). This combination creates a surveillance system that is not only real-time but also capable of learning from previous data to improve decision-making quality. In this way, technology not only accelerates processes but also enhances the accuracy and objectivity of police work.

The concept of e-policing emerges as a digital-based policing operational model that brings legal services closer to the public (Negara, 2024). E-policing involves digital reporting systems, integration with national information systems, and the use of software for crime mapping (Ismail, 2023). The public can access police services without having to go to a police station, while officers can manage information in a well-structured and documented manner. This system also helps speed up administrative processes in investigations and public services. In the long term, e-policing creates a more transparent, efficient, and data-based legal environment (Dwilaksanaa, 2020).

Smart policing complements e-policing with a strategic, analytics-based approach (Jaladriyanta, 2020). The focus is not only on service delivery but also on Polri’s anticipatory and responsive capabilities toward security threats. Data from digital identification systems, surveillance cameras, citizen reports, and other sources are analyzed to make more accurate strategic decisions. Smart policing emphasizes the importance of cross-sector collaboration, including with local governments, communities, and the private sector, in maintaining regional security. This makes the security system not merely the domain of officers, but a social ecosystem supported by technology.

Comparative studies with other countries show that the implementation of digital identification in law enforcement has become a global trend. Countries such as Japan, the United Kingdom, and the United States have applied facial recognition technology in public spaces to detect perpetrators of crimes or individuals who pose security threats. In Singapore, the integration of smart surveillance cameras with the national database has increased the success rate of crime detection to over 80%. Nevertheless, all these countries still face legal and ethical challenges, particularly related to personal data protection and potential abuse of authority. This serves as an important lesson for Indonesia in designing a similar system that is not only technologically sophisticated but also strong in legal and ethical terms.

METHOD

This research uses a normative juridical method, which is an approach that focuses on analyzing the applicable positive legal norms and legal principles relevant to the issue under discussion. The main focus of this method is on library research, by reviewing legislation, legal documents, academic literature, and other secondary legal sources related to digital identification systems, police authority, and personal data protection in the context of law enforcement. The normative approach is used to examine how law legitimizes the use of digital technology in identification activities by the Indonesian National Police (Polri), while also assessing the extent to which existing legal norms can anticipate potential legal and ethical issues in practice. This study also adopts a conceptual approach to understand relevant legal theories, such as Lawrence Friedman's legal system theory and legal effectiveness theory, to construct a critical framework regarding the role of technology in the legal system. In addition, official documents such as laws, presidential regulations, ministerial regulations, and other institutional policies governing information systems, biometric technology, and data security in Indonesia are also reviewed. By using this method, this research does not merely aim to describe applicable norms but also identify legal voids, inconsistencies among regulations, and provide normative recommendations for strengthening the legal system in the future. The normative juridical approach is considered the most appropriate in this context because the object of study is regulatory in nature and oriented toward legal reform.

RESULT AND DISCUSSION

Legal Basis for the Use of Digital Identification Systems by the Indonesian National Police (Polri)

Law Number 2 of 2002 concerning the Indonesian National Police serves as the main foundation in regulating the duties and authority of the police, including the use of digital identification systems. Article 13 explains that the main duties of the police include maintaining public security and order, enforcing the law, and providing protection, guidance, and service to the community. The implementation of digital systems for identification purposes aligns with this mandate, particularly in efforts to modernize police tools and work strategies. The use of technology becomes one form of actualization in creating responsive and effective services. In this context, technology is not merely a supplement but a primary supporting tool in carrying out institutional functions that are adaptive to the times.

Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP) also provides a basis for the use of data in the investigation and inquiry of criminal acts. KUHAP emphasizes the importance of legal evidence, including expert testimony and indications that can be obtained from digital evidence such as biometric identification results. Digital identification systems contribute to strengthening scientific and structured proof. Facial recognition technology, fingerprints, or iris scans can be used to confirm the identity of suspects in legal processes, as long as they are conducted in accordance with legal procedures. As an investigator, the police must ensure that the use of this technology does not violate the principle of due process of law.

In the context of digital-based law enforcement, Law Number 19 of 2016 as an amendment to the Law on Electronic Information and Transactions (ITE Law) provides an important legal framework. The articles in this law explain the legality of electronic information and documents as valid evidence in legal proceedings. Digital identification based on information technology falls into this category, as long as the system used can guarantee authenticity, integrity, and reliability of the data. The use of AI and big data to identify individuals or analyze crime patterns can be legally justified, as long as it does not violate human rights and is conducted within the corridors of positive law. The presence of the ITE

Law strengthens the position of digital systems as part of Indonesia's modern and adaptive legal ecosystem.

Data protection becomes a very crucial issue in the implementation of digital identification systems. Law Number 27 of 2022 on Personal Data Protection serves as a regulation that governs how individual data, especially sensitive data such as biometrics, must be processed and protected. Biometric data used in identification systems falls into the category of sensitive personal data and requires strict protection standards. The process of collecting, storing, and processing data must be based on legitimate principles, transparency, and limited to certain lawful purposes. The use of data in the identification system by the police must comply with these principles to avoid violations of citizens' privacy rights.

This law requires a clear legal basis for every act of personal data collection by public institutions. The police, as a state institution authorized in public security, must demonstrate legal standing for the processing of biometric data collected. Citizens must be adequately informed of their rights to their data, including the right to know, access, and even request data deletion under certain conditions. The implementation of digital identification systems will require the integration of security interests and the protection of individual rights. The main challenge is to build a system that is not only technically secure but also legally and ethically sound.

Ministerial Regulation of the Ministry of Communication and Information Technology (Permenkominfo) Number 5 of 2020 on the Implementation of Private Scope Electronic Systems in conjunction with Permenkominfo No. 10 of 2021 provides technical guidelines on how electronic systems should be implemented, although initially intended for the private sector. However, many principles in this regulation can be referred to by state institutions, including the police, in designing and operating digital systems. System security standards, data management, and information system governance are relevant aspects in building a robust digital identification system. This regulation also emphasizes that system operators must ensure availability, integrity, authenticity, and confidentiality of the data being processed. The police can adapt these principles in developing their internal digital systems to meet national and international security standards.

Meanwhile, Presidential Regulation Number 39 of 2019 on One Data Indonesia serves as a reference for data integration among state institutions. The digital identification system of the police is closely related to population data managed by the Directorate General of Population and Civil Registration (Dukcapil) and other institutions. This presidential regulation stipulates that data exchange between agencies must be carried out with the principles of interoperability, standardized data, and transparent governance. System integration between the police and other institutions allows for faster and more accurate identity data validation in law enforcement processes. This regulation is an important foundation to prevent data duplication, ensure accuracy, and maintain the efficiency of the identification system.

Data integration across institutions certainly requires a strong coordination system to prevent authority conflicts or legal violations. In its implementation, clear Memorandums of Understanding (MoUs) and Standard Operating Procedures (SOPs) are needed regarding how data is used, stored, and who has access to it. Transparency in data usage is key to maintaining public trust, especially in the context of law enforcement involving citizens' rights. The police have a major responsibility to ensure that technology is not misused to violate privacy or conduct profiling without legal grounds. Collaboration with data supervisory institutions and human rights protection agencies becomes crucial to balance between security interests and individual rights protection.

The digital identification system by the police is a progressive step in responding to the challenges of modern law enforcement. However, without a strong legal foundation, this system could become a double-edged sword that creates human rights violations. The regulations mentioned earlier are juridical foundations that must be thoroughly internalized in digital policing policies and practices. Every step of technological innovation must be based on caution and respect for the principles of the rule of law. The police are not only required to act swiftly in maintaining security, but also to adhere to the supremacy of law in every use of their digital power.

Implementation of Digital Identification Technology by the Indonesian National Police and Its Challenges

The digital identification system used by the Indonesian National Police (Polri) has undergone significant development through the utilization of the Automatic Biometric Identification System (ABIS). This system enables the automatic and rapid matching of biometric data such as fingerprints, facial features, and irises. The implementation of ABIS is highly beneficial in the process of identifying suspects or crime victims, especially in situations that require high speed and accuracy. This technology also supports cross-data matching in a much shorter time compared to conventional methods. However, its application still depends heavily on the quality of data and the supporting systems used by Polri.

Cross-agency collaboration is an integral part of the implementation of digital identification systems. Polri cooperates with the Directorate General of Population and Civil Registration (Ditjen Dukcapil) of the Ministry of Home Affairs in accessing population data, and with the Directorate General of Immigration to monitor cross-border human movement. Moreover, international cooperation, such as with Interpol, becomes crucial in handling transnational cases like human trafficking, terrorism, and cybercrime. Connections with global networks allow for the biometric data matching of perpetrators crossing national borders. Such collaborations require solid interoperability systems and formal agreements regarding data exchange and use across jurisdictions.

The presence of algorithms in digital identification technology opens the door to new issues, especially those related to accuracy and algorithmic bias. Facial recognition systems, for instance, have shown less accurate results in some international studies when applied to certain racial or gender groups. Such identification failures can have serious consequences for law enforcement processes, as they may lead to wrongful arrests or misidentification. These risks are not merely technical issues but also concern the legitimacy of law enforcement agencies. This challenge demands regular evaluations of the algorithms used and the involvement of independent experts in system audits.

Furthermore, the implementation of digital identification technology also faces significant challenges in terms of the right to privacy. Biometric data is highly sensitive because it is permanent and cannot be changed like passwords. When such data is leaked or misused, the impact can be long-lasting and difficult to remedy. Problems arise when there is a lack of transparency about how this data is collected, stored, and used by the police. The absence of strict internal regulations governing data processing makes room for violations.

The use of digital technology in police systems often precedes the available regulations. The lack of comprehensive internal regulations for the governance of digital identification systems renders existing policies temporary or patchwork solutions. The absence of standard operating procedures also makes it difficult for officers to operate the system correctly and consistently. Additionally, without clear rules, supervision and accountability for system misuse are weak. In such situations, the potential for violations of the principles of legality and procedural justice becomes even greater.

Operational constraints are also significant obstacles in the implementation of this system. Human resources (HR) within Polri still face challenges in mastering the complex digital technologies. Not all members have technical backgrounds or a deep understanding of the technologies being used. Limited training and inadequate technical assistance have led to suboptimal system operation. This condition also creates dependency on external technology vendors, which could become a long-term issue.

Uneven technological infrastructure is another barrier to the implementation of digital identification systems across Indonesia. Many police regions in remote areas still lack adequate internet access or supporting hardware. This inequality creates gaps in service and law enforcement effectiveness between central and regional areas. Moreover, hardware maintenance and system updates require large budgets that have not yet been fully and sustainably prepared. This situation makes it difficult for some regions to fully adopt the system.

Technical issues also involve the cybersecurity of the systems used. Digital identification systems store large volumes of data, making them attractive targets for cyberattacks. When systems are not built with high information security standards, the risk of data breaches is always present. Many internal systems still use basic security protocols and lack early detection mechanisms for potential hacking. Dependence on digital systems without adequate security preparedness can become a serious threat to Polri's credibility as a law enforcement institution.

The overall implementation of digital identification systems by Polri reflects the spirit of modernization but is not free from major challenges that must be addressed structurally and sustainably. Technology can be a powerful tool when supported by a strong legal, ethical, and managerial framework. A comprehensive evaluation of the technical, legal, and human resource aspects is crucial to ensure that the technology truly serves as a solution, not a source of additional problems. This challenge is not solely the responsibility of Polri but also requires cross-sector support to build an identification system that is fair, accurate, and trusted by the public.

CONCLUSION

The enhancement of law enforcement by Polri through the use of digital identification systems is a strategic step in responding to increasingly complex, rapidly changing, and technology-based domestic security dynamics. Advances in information and communication technology have pushed the police institution to undergo a digital transformation to make identification, investigation, and legal action processes more efficient. Digital identification systems based on biometrics, such as the Automatic Biometric Identification System (ABIS), have become the backbone in verifying the identities of criminal perpetrators, victims, and witnesses more quickly, accurately, and in a documented manner. The integration of this system with population data from Dukcapil, immigration data, and even Interpol's system demonstrates significant progress in cross-sector and international cooperation. However, the implementation of this technology also raises several important issues that cannot be ignored, such as the lack of internal regulation, weak ethical understanding among officers, and limited digital infrastructure in many regions. On the other hand, the risks of identification errors, potential algorithmic bias, and violations of personal data privacy are serious challenges that could undermine public trust in the police if not anticipated early through strict policies and oversight. Polri must recognize that digital transformation is not merely about procuring equipment and systems, but involves a comprehensive change in working methods, value systems, and accountability patterns that must be developed systematically, transparently, and accountably.

To ensure the effectiveness and sustainability of the digital identification system used by Polri, earnest efforts are needed to design a comprehensive internal regulatory framework that prioritizes the protection of human rights, especially in managing biometric data. This regulation should not only govern technical and operational aspects but must also include information security standards, independent oversight mechanisms, citizens' rights to access and correct their data, as well as ethical audit procedures for the use of algorithms and big data.

In addition, strengthening the capacity of Polri's human resources in information technology and digital ethics is an urgent need to ensure that the technology is utilized proportionally, fairly, and responsibly. Every use of the digital identification system must comply with the principles of legality, proportionality, and accountability to prevent abuses of power that could violate the principle of due process of law. Polri must also open a dialogue with civil society, academics, and oversight institutions so that the system built is not only effective in preventing and combating crime, but also able to maintain public trust in the police institution. Thus, the digital transformation carried out by Polri can serve as the foundation for establishing a modern, inclusive, and just law enforcement system aimed at achieving sustainable domestic security.

REFERENCES

Absah, M. M. (2024). Pengaruh globalisasi terhadap pembaharuan hukum pidana di Indonesia. *Hukum Dinamika Ekselensia, 6(3).*

Agustoni, R. (2023). Optimalisasi Penyidik Satuan Reskrim Dalam Pemanfaatan Aplikasi E-Manajemen Penyidikan di Polres Banyumas. *Police Studies Review, 7(8)*, 185-242.

Al Kautsar, I. &. (2022). Sistem hukum modern Lawrance M. Friedman: Budaya hukum dan perubahan sosial masyarakat dari industrial ke digital. *Sapientia Et Virtus, 7(2)*, 84-99.

Cahya, A. N. (2024). Transformasi Budaya Hukum dalam Era Digital (Implikasi Penggunaan AI dalam Perkembangan Hukum Di Indonesia). *IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora, 8(2)*, 361-373.

Darmawan, K. S. (2024). Implementasi Peran Bareskrim Dalam Melindungi Masyarakat Pada Era Society 5.0. *Jurnal Salam Presisi, 2(01)*, 49-61.

Djatiutomo, T. J. (2023). Strategi inovasi services digital Korlantas Polri untuk peningkatan kinerja organisasi. *JEMBA: JURNAL EKONOMI, MANAJEMEN, BISNIS DAN AKUNTANSI, 2(6)*, 897-910.

Dwilaksanaa, C. (2020). Design and Application of E-Policing: Police practice Management Through the use of Information Technology in Indonesia. *International Journal of Innovation, Creativity and Change, 13(4)*, 1-11.

Hasibuan, E. S. (2023). Reformasi Polri: Menilik Keberhasilan Program Presisi Polri. *KRTHA BHAYANGKARA, 17(3)*, 515-524.

Ismail, M. (2023). Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian untuk Mencegah Kejahatan Siber (Cybercrime). *Jurnal Ilmu Kepolisian, 17(3)*, 15.

Jaladriyanta, S. (2020). Polri Menuju Smart Police. *Jurnal Ilmu Kepolisian, 14(2)*, 12-12.

Kushariyadi, K. A. (2024). *Artificial Intelligence: Dinamika Perkembangan AI Beserta Penerapannya*. Jambi: PT. Sonpedia Publishing Indonesia.

Manafe, C. F. (2023). Implementasi konsep Keamanan Nasional Dalam Upaya Menghadapi Ancaman Siber Di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 10(4)*, 2063-2073.

Mubarok, R. F. (2023). Model Pengasuhan Taruna Akademi Kepolisian Berbasis Teknologi Informasi: Analisis Pada Lembaga Pendidikan dan Pelatihan Polri Tahun 2022. *JIM: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah, 8(4)*, 5448-5456.

Nainggolan, N. S. (2023). Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital. *Jurnal Jurnal Sains Dan Teknologi (JSIT), 3(2)*, 253.

Negara, L. G. (2024). E-Policing dan Implikasi Kebijakan Pengelolaan Keamanan Publik. *Jurnal Syntax Admiration, 5(12)*, 5764-5771.

Orlando, G. (2022). Efektivitas Hukum dan Fungsi Hukum di Indonesia. *Tarbiyah bil Qalam: Jurnal Pendidikan Agama dan Sains, 6(1).*

Sinaga, B. B. (2024). Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0. *Padjadjaran Law Review*, *12(1)*, 71-82.

Supratman, A. N. (2020). Menyoal Sikap Kejahatan Di Indonesia Di Era Industri 4.0 (Suatu Perspektif Kriminologi). *Leg. J. Perundang Undangan dan Huk. Pidana Islam*, 27-42.

Wibowo, A. W. (2023). *Pemolisian digital dengan artificial intelligence*. Depok: PT. RajaGrafindo Persada-Rajawali Pers.

Windani, C. A. (2023). Strategi dan Tantangan Predictive Policing di Era Big Data bagi Masyarakat Modern. *Deviance Jurnal Kriminologi*, *7(2)*, 101-120.