

Digital Transformation in Indonesian Policing: Opportunities and Challenges in the Adoption of Emerging Technologies

Arka Wiratama Pradipta*

Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

arkawiratamapradipta@gmail.com

DOI: <https://doi.org/10.65815/55re7v59>

Submitted: 29-08-2025

Revised: 12-09-2025, 20-11-2025

Accepted: 28-12-2025

*Corresponding Author

Abstract

Digital technologies are increasingly transforming the ways in which police institutions collect information, communicate with citizens, investigate crime, and manage organizational processes. In Indonesia, digital transformation presents opportunities to improve police efficiency and responsiveness while simultaneously creating challenges concerning privacy, accountability, technological capacity, and ethical governance. This study examines the development of digital transformation in Indonesian policing and assesses its institutional implications. Using qualitative policy analysis, the study reviews police digitalisation initiatives and examines the opportunities and challenges associated with the adoption of emerging technologies. Particular attention is given to digital evidence, information management, online public services, data integration, and technology-supported investigation. The study finds that technological adoption can strengthen operational capabilities when accompanied by appropriate institutional governance, professional training, data protection, and accountability mechanisms. However, technological modernisation may also create new risks when regulatory and ethical safeguards fail to develop at the same pace. The study argues that digital transformation should therefore be treated as an institutional reform process rather than merely a technological upgrade. The article contributes to contemporary policing scholarship by examining digital transformation through the Indonesian context and identifying governance principles relevant to technology-enabled policing.

[Teknologi digital semakin mengubah cara institusi kepolisian mengumpulkan informasi, berkomunikasi dengan masyarakat, menyelidiki tindak pidana, dan mengelola proses organisasi. Di Indonesia, transformasi digital menghadirkan peluang untuk meningkatkan efisiensi dan daya tanggap kepolisian, sekaligus memunculkan tantangan terkait privasi, akuntabilitas, kapasitas teknologi, dan tata kelola yang etis. Studi ini mengkaji perkembangan transformasi digital dalam kepolisian Indonesia serta menilai

implikasi kelembagaannya. Dengan menggunakan metode analisis kebijakan kualitatif, studi ini meninjau berbagai inisiatif digitalisasi kepolisian serta menganalisis peluang dan tantangan yang muncul dari penerapan teknologi terkini. Perhatian khusus diberikan pada aspek bukti digital, manajemen informasi, layanan publik daring, integrasi data, dan penyelidikan berbasis teknologi. Hasil studi menunjukkan bahwa penerapan teknologi dapat memperkuat kemampuan operasional jika dibarengi dengan tata kelola kelembagaan yang tepat, pelatihan profesional, perlindungan data, dan mekanisme akuntabilitas. Namun, modernisasi teknologi juga dapat menimbulkan risiko baru apabila pengembangan perangkat perlindungan regulasi dan etika tidak berjalan seiring. Oleh karena itu, studi ini berargumen bahwa transformasi digital sebaiknya dipandang sebagai proses reformasi kelembagaan, bukan sekadar peningkatan teknologi semata. Artikel ini memberikan kontribusi pada kajian kepolisian kontemporer dengan menelaah transformasi digital dalam konteks Indonesia serta mengidentifikasi prinsip-prinsip tata kelola yang relevan bagi kepolisian berbasis teknologi.]

Keywords: digital policing, police technology, digital transformation, data governance, Indonesia

Introduction

Digital transformation has become an increasingly important dimension of contemporary policing because police organizations now operate in an environment where information is generated, transmitted, analyzed, and stored through digital infrastructures. Conventional policing relied heavily on physical records, face-to-face interaction, and geographically bounded information, whereas contemporary policing increasingly incorporates digital evidence, automated surveillance, online reporting, data analytics, geographic information systems, biometric identification, and artificial intelligence. Manning argues that police technology does not merely provide new instruments for existing practices but also influences how police organizations conceptualize information, crime control, and rational decision-making (Manning 2008). Ratcliffe similarly positions technology and data analysis as increasingly important components of intelligence-led policing (Ratcliffe 2016). In Indonesia, this transformation is visible in electronic investigation management, online police services, Electronic Traffic Law Enforcement (ETLE), Digital Korlantas, and the POLRI Super App. These developments indicate that digitalization has moved beyond experimentation toward becoming part of the institutional infrastructure of policing.

The Indonesian context is particularly significant because digital transformation occurs within a large, decentralized, and institutionally complex police organization. Law No. 2 of 2002 establishes the Indonesian National Police (Polri) as an institution responsible for maintaining public security and order,

enforcing the law, and providing protection and public services (Republic of Indonesia 2002). Digitalization therefore affects not only investigative functions but also administrative management, public-service delivery, traffic enforcement, complaint handling, and relationships between police officers and citizens. Recent institutional developments demonstrate this broadening scope. The POLRI Super App provides multiple police services through a single digital platform, while Digital Korlantas integrates services such as digital driver's-license administration and other traffic-related functions. In 2026, Polri also expanded online police reports and loss reports through its Super App, illustrating how digital transformation increasingly mediates routine interactions between citizens and police institutions (Indonesian National Police 2026a; Indonesian National Police 2026b).

Previous studies provide substantial conceptual foundations for understanding technology-enabled policing, but important gaps remain when these insights are applied to Indonesia. International scholarship has examined predictive policing, algorithmic decision-making, big-data surveillance, body-worn cameras, and artificial intelligence, often emphasizing tensions between operational efficiency and civil liberties (Ferguson 2017; Brayne 2020; Berk 2021). Meijer and Wessels identify a significant discrepancy between the expectations surrounding predictive policing and the empirical evidence demonstrating its effectiveness (2019). Lum and Isaac further show that predictive systems can reproduce patterns embedded in historical police data rather than simply eliminating human bias (2016). Indonesian scholarship, meanwhile, has increasingly examined electronic investigation management, digital public services, digital evidence, cybercrime enforcement, and technology-supported traffic enforcement. However, much of this literature focuses on individual technologies or specific institutional applications rather than examining digital transformation as a broader organizational and governance process. The research gap therefore lies in connecting technological adoption with institutional capacity, data governance, accountability, legal safeguards, and professional transformation within Indonesian policing.

This study addresses that gap through qualitative policy analysis of the development and implications of digital transformation in Indonesian policing. The analysis examines legal instruments, institutional policy documents, official police digital-service platforms, and relevant academic literature concerning digital policing, digital evidence, predictive technologies, data governance, and police accountability. The method is interpretive rather than statistical: it seeks to identify institutional patterns, opportunities, risks, and governance requirements emerging from the adoption of digital technologies. Particular attention is given to five interconnected dimensions: digital evidence and investigation, integrated information management, online public services, technology-supported enforcement, and emerging data-intensive technologies. This approach is appropriate because digital transformation cannot be adequately evaluated by

technological performance alone. As Meijer, Lorenz, and Wessels argue, algorithmic systems operate within organizational contexts that shape how technologies are implemented and interpreted (2021). Accordingly, the central argument of this paper is that Indonesian police digital transformation should be understood as institutional reform involving technology, organizational capacity, law, professional practice, and accountability simultaneously.

Digital Infrastructure, Evidence, and Operational Transformation

One of the most significant opportunities presented by digital transformation is the improvement of police information management and investigative processes. Traditional investigative administration can involve fragmented documentation, duplicated records, slow information exchange, and difficulties in monitoring case progression. Electronic systems can reduce these limitations by creating standardized workflows and making information available across organizational levels. The Electronic Investigation Management System (E-MP), implemented within Polri since 2017, represents an important example because it connects stages of case management from police reports and personnel assignment to the completion of investigations (Irawan et al. 2026). Earlier evaluation research also identified E-MP as a mechanism for facilitating interaction among investigators, assistant investigators, and supervisors through a common management system (Raslin et al. 2021). Such systems can improve organizational visibility because supervisors can monitor case development more systematically, while investigators can work with standardized digital documentation. Nevertheless, technological infrastructure does not automatically create institutional efficiency. Its effects depend on data quality, system reliability, user competence, interoperability, and organizational willingness to replace informal procedures with digitally standardized practices.

Digital evidence constitutes a second major dimension of transformation because contemporary criminal investigations increasingly involve smartphones, social-media records, electronic transactions, cloud data, location information, video recordings, and other forms of electronically generated information. Indonesian law recognizes electronic information and electronic documents as legally valid evidence, subject to statutory requirements (Republic of Indonesia 2024). This legal recognition creates an important foundation for technology-supported investigation, but admissibility does not eliminate technical and procedural problems. Digital evidence must be authenticated, preserved, documented, and transferred through reliable procedures so that its integrity can be demonstrated. Casey emphasizes that the evidentiary value of digital information depends not merely on its existence but also on forensic processes capable of establishing how evidence was acquired, preserved, and interpreted (Casey 2011). Recent Indonesian legal scholarship similarly identifies chain-of-custody standards, authentication, and disparities in digital-forensic capacity as continuing challenges

(Putra 2026). Consequently, digital transformation requires standardized forensic protocols and trained investigators rather than simply purchasing forensic software and hardware.

The operational value of digital transformation is also apparent in technology-supported traffic enforcement and integrated public-service systems. ETLE illustrates how cameras, sensors, digital records, and automated analytical technologies can transform traffic enforcement from predominantly officer-initiated intervention toward technology-supported detection and documentation. Official Polri information describes ETLE as using cameras, sensors, and artificial intelligence to identify traffic violations and generate electronic records that can support enforcement processes (Korlantas Polri 2026a). Similarly, Digital Korlantas integrates services such as SIM registration and renewal, digital identity functions, biometric authentication, and other traffic-related services (Korlantas Polri 2026b). These systems can reduce administrative friction and create more standardized interactions between citizens and police institutions. However, their institutional significance should not be reduced to convenience. Automated enforcement changes how discretion is exercised, how evidence is generated, and how citizens encounter police authority. The central policy question therefore concerns whether technological standardization is accompanied by transparent procedures for correcting errors, contesting decisions, securing personal data, and maintaining human responsibility for consequential decisions.

Public Services, Data Integration, and Institutional Capacity

Digital transformation can also reshape policing by moving public services from physical offices toward digitally mediated interactions. The POLRI Super App illustrates this transition by consolidating multiple services into a single platform, while the 2026 introduction of online police and loss reports further expands the range of interactions that citizens can conduct digitally (Indonesian National Police 2026a). Such systems have the potential to reduce transaction costs, increase accessibility, provide electronic records of service interactions, and improve administrative monitoring. From an institutional perspective, digitized services can also generate structured data that may help police organizations identify service demand and allocate resources. Yet the creation of more digital interfaces does not automatically produce greater accessibility. Citizens may face unequal access to devices, connectivity, digital literacy, or reliable identification systems. Digital exclusion can therefore reproduce inequalities in a different form. The transformation of public services should consequently be assessed through both efficiency and inclusion. A service that is technically available online but difficult to use, poorly communicated, or inaccessible to digitally disadvantaged groups may increase formal availability without producing equivalent substantive accessibility.

Data integration represents another major opportunity but also one of the most consequential governance challenges. Integrated policing requires information

from different units and systems to become interoperable without compromising security, accuracy, or lawful purpose limitations. Brayne's research demonstrates that data-intensive policing expands the scale of information available to police organizations, enabling connections among datasets that previously remained institutionally separate (Brayne 2020). Ratcliffe similarly emphasizes the importance of information analysis for intelligence-led policing (2016). In Indonesia, however, integration must be considered alongside the Personal Data Protection Law, which establishes a comprehensive legal framework for protecting personal data and recognizing personal-data protection as an important individual right (Republic of Indonesia 2022). The challenge is therefore not whether Polri should integrate data, but under what conditions data may be collected, linked, retained, accessed, shared, and deleted. Effective data governance requires clearly defined purposes, access controls, audit mechanisms, retention policies, cybersecurity standards, and institutional responsibility for misuse. Without these safeguards, interoperability can expand both institutional capability and institutional vulnerability simultaneously.

Institutional capacity is particularly important because digital transformation can create an assimilation gap between technological systems and the personnel expected to use them. Recent research on E-MP involving 14,547 Polri personnel across 12 regional police commands identifies human resources, infrastructure, and system stability as continuing implementation challenges (Irawan et al. 2026). This finding demonstrates that technology adoption is partly a workforce transformation problem. Officers require technical competencies, but they also need the ability to interpret digital information critically, understand evidentiary standards, recognize data-quality problems, and operate within privacy and accountability requirements. Algorithmic systems can create a misleading perception that decisions are objective simply because they are computational. Kroll et al. argue that automated decision systems require mechanisms capable of establishing whether their outputs comply with legal and normative standards (2017). Meijer, Lorenz, and Wessels likewise emphasize that organizational routines shape the effects of algorithmic systems (2021). For Indonesian policing, investment in technology therefore needs to be accompanied by continuous professional education, specialized digital-forensic expertise, data-literacy training, and institutional mechanisms for reviewing technological performance.

Emerging Technologies, Accountability, and Ethical Governance

The expansion of artificial intelligence and predictive analytics creates opportunities for police organizations to identify patterns that may be difficult to detect through conventional methods. Predictive systems can process historical crime information, geographic patterns, temporal variables, and other datasets to support decisions about resource allocation or preventive strategies. Berk explains that predictive policing can be understood partly as an application of statistical

modeling to crime patterns, while emphasizing persistent concerns regarding accuracy, fairness, and transparency (2021). Meijer and Wessels similarly find that claims concerning predictive policing should be treated cautiously because empirical evidence concerning effectiveness remains less developed than the technological discourse surrounding it (2019). For Indonesia, this distinction is particularly important because predictive systems may appear attractive in contexts where police agencies seek more efficient allocation of limited resources. However, prediction should remain an analytical input rather than an unquestionable determination of risk. Historical police data may reflect previous enforcement priorities, reporting patterns, and institutional biases. Therefore, algorithmic outputs can reproduce existing patterns while presenting them as mathematically neutral.

The problem of algorithmic bias becomes especially important when emerging technologies influence surveillance, targeting, or investigative decisions. Barocas and Selbst demonstrate that data-driven systems can reproduce discrimination because historical datasets may contain patterns generated by earlier human decisions and unequal social structures (2016). Lum and Isaac similarly warn that predictive policing can reproduce the geographic and demographic patterns already present in police records rather than simply forecasting crime independently of prior enforcement (2016). Benjamin's concept of the "New Jim Code" further emphasizes that technological systems can conceal or accelerate inequality while appearing neutral because decisions are mediated through technical infrastructures (2019). These arguments do not establish that every algorithmic police system will necessarily produce discriminatory outcomes; rather, they demonstrate why claims of technological neutrality require empirical testing. In Indonesia, algorithmic policing should therefore involve independent validation, representative data assessment, error analysis, documentation of model limitations, and mechanisms allowing affected persons to challenge consequential decisions. Human oversight should remain meaningful rather than functioning as a symbolic approval layer placed after an automated decision has already been made.

Surveillance technologies present a related governance challenge because digital policing can substantially expand the quantity and granularity of information available to law-enforcement institutions. Facial recognition, automated cameras, location tracking, digital communications analysis, and integrated databases can strengthen investigative capabilities, but they can also change the relationship between citizens and the state by making continuous observation technically easier. Schneier argues that the expansion of data collection creates a fundamental tension between collective security objectives and individual privacy (2015). Brayne similarly demonstrates that data-intensive policing can produce forms of "dragnet surveillance" in which information concerning people who are not directly suspected of wrongdoing becomes incorporated into police databases (2020). Body-worn cameras illustrate the complexity of technology-based accountability: Lum et al. find that their effects on police and citizen behavior are inconsistent across outcomes, while evidence concerning reductions in complaints does not

necessarily demonstrate improved police-community relationships (2020). These findings suggest that surveillance technologies should be governed through necessity, proportionality, purpose limitation, retention rules, access controls, and independent oversight rather than justified solely by their technical capabilities.

The broader implication is that digital transformation requires a shift from technology procurement toward technology governance. Accountability must exist at multiple stages: when a technology is selected, when data are collected, when algorithms are designed or purchased, when outputs influence police decisions, and when citizens seek remedies for errors or misuse. Yeung describes algorithmic regulation as a form of governance in which computational systems continuously collect information, assess conditions, and influence behavior (2018). Kroll et al. similarly argue that conventional accountability mechanisms may be inadequate for automated systems because responsibility can become distributed across programmers, vendors, institutions, and decision-makers (2017). In Indonesia, the Personal Data Protection Law provides an important legal foundation for regulating personal-data processing, while the Electronic Information and Transactions Law establishes the legal recognition of electronic information and documents (Republic of Indonesia 2022; Republic of Indonesia 2024). Nevertheless, formal legal recognition must be complemented by operational governance: algorithm registers, audit trails, cybersecurity standards, procurement requirements, impact assessments, clear retention periods, and mechanisms for human review. Digital policing becomes institutionally sustainable when technological power is matched by traceable responsibility.

The Indonesian experience therefore suggests that successful digital transformation should be evaluated according to institutional integration rather than the number of applications or technologies introduced. Research on Digital Korlantas has identified progress in digital public services while also highlighting the need for improved integration, data-processing efficiency, security management, and infrastructure (Raslin et al. 2024). Recent developments in Polri's digital ecosystem, including the Super App, Digital Korlantas, E-MP, ETLE, and integrated complaint-management initiatives, demonstrate a movement toward interconnected digital policing rather than isolated technological projects. At the same time, the existence of multiple systems increases the importance of interoperability standards and centralized governance. The policy challenge is consequently to prevent digital fragmentation, where separate applications produce disconnected databases and duplicated administrative processes. An effective architecture should define which datasets are authoritative, who may access them, how systems communicate, and how citizens can understand and contest decisions made through digital processes. Digital maturity should thus be measured through institutional coherence, service quality, security, accountability, and professional capacity rather than technological novelty alone.

Conclusion

Digital transformation is fundamentally reshaping Indonesian policing by changing how police organizations collect evidence, manage investigations, provide public services, enforce regulations, and use information for operational decision-making. The analysis demonstrates that digital technologies provide substantial opportunities for improving administrative efficiency, information availability, investigative capacity, service accessibility, and consistency of enforcement. E-MP illustrates how digital systems can structure investigative workflows, while Digital Korlantas and the POLRI Super App demonstrate the expansion of digital public services. ETLE further illustrates how technological systems can transform evidence production and enforcement practices. Nevertheless, these opportunities are conditional rather than automatic. Technological systems require reliable infrastructure, interoperable databases, skilled personnel, standardized digital-forensic procedures, and institutional capacity to interpret digital information critically. The evidence from Indonesian studies indicates that human-resource capacity, infrastructure, system stability, integration, and security remain important implementation concerns. Digital transformation should therefore be understood not as a replacement of police work by technology but as a reconfiguration of police organizations around digitally mediated information and services.

The central challenge for Indonesian policing is consequently to align technological modernization with legal protection, ethical governance, and institutional accountability. Emerging technologies such as artificial intelligence, predictive analytics, biometric systems, and large-scale surveillance can increase analytical capabilities, but they can also amplify existing data-quality problems, create new privacy risks, and obscure responsibility for consequential decisions. Indonesia's Personal Data Protection Law and amended Electronic Information and Transactions Law provide important legal foundations, but effective governance requires implementation mechanisms capable of translating legal principles into operational practice. The future of digital policing should therefore emphasize privacy-by-design, data minimization, cybersecurity, independent auditing, transparent procurement, human oversight, professional digital training, and accessible mechanisms for contesting technological decisions. The Indonesian case contributes to broader policing scholarship by demonstrating that digital transformation is not principally a technological upgrade; it is an institutional reform process in which technology, organizational capacity, legal regulation, professional practice, and public accountability must develop together. The sustainability of digital policing will ultimately depend on whether technological capability is matched by governance capability.

References

- Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparate Impact." *California Law Review* 104 (3): 671–732. <https://doi.org/10.15779/Z38BG31>.
- Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity.
- Berk, Richard A. 2021. "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement." *Annual Review of Criminology* 4: 209–237. <https://doi.org/10.1146/annurev-criminol-051520-012342>.
- Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press. <https://doi.org/10.1093/oso/9780190684099.001.0001>.
- Casey, Eoghan. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Waltham, MA: Academic Press.
- Ferguson, Andrew G. 2017. "Policing Predictive Policing." *Washington University Law Review* 94 (5): 1109–1189.
- Indonesian National Police. 2026a. "Polri Luncurkan Layanan Laporan Polisi Online, Super App Polri Kini Semakin Lengkap dan Transparan." April 14, 2026.
- Indonesian National Police. 2026b. "KPRP Outlines Six Strategic Pillars for National Police Institutional Reform." May 6, 2026.
- Irawan, Dhanny, A. Widihandoko, Rachmat Taufik Hidayatulloh, and Moch. Nurhasim. 2026. "Strategi Pemberdayaan SDM Polri Guna Mendukung Penerapan Sistem Elektronik Manajemen Penyidikan (EMP)." *Jurnal Litbang Polri* 29 (1). <https://doi.org/10.46976/litbangpolri.v29i1.364>.
- Korlantas Polri. 2026a. "Teknologi ETLE Perkuat Penegakan Hukum Lalu Lintas Berbasis Digital." May 15, 2026.
- Korlantas Polri. 2026b. *Digital Korlantas POLRI*.
- Kroll, Joshua A., Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. 2017. "Accountable Algorithms." *University of Pennsylvania Law Review* 165 (3): 633–705. <https://doi.org/10.2307/4049111>.
- Lum, Cynthia, Christopher S. Koper, David B. Wilson, Megan Stoltz, Michael Goodier, Elizabeth Eggins, Angela Higginson, and Lorraine Mazerolle. 2020. "Body-Worn Cameras' Effects on Police Officers and Citizen Behavior: A Systematic Review." *Campbell Systematic Reviews* 16 (3): e1112. <https://doi.org/10.1002/cl2.1112>.
- Lum, Kristian, and William Isaac. 2016. "To Predict and Serve?" *Significance* 13 (5): 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.

- Manning, Peter K. 2008. *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press.
- Meijer, Albert J., Lotte Lorenz, and Martijn Wessels. 2021. "Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems." *Public Administration Review* 81 (5): 837–846. <https://doi.org/10.1111/puar.13391>.
- Meijer, Albert, and Martijn Wessels. 2019. "Predictive Policing: Review of Benefits and Drawbacks." *International Journal of Public Administration* 42 (12): 1031–1039. <https://doi.org/10.1080/01900692.2019.1575664>.
- Ngatmo, Ngatmo. 2025. "Advancing Law Enforcement Efficiency Through Integrated Technological Innovation Systems." *Jurnal Scientia Indonesia* 9 (2). <https://doi.org/10.15294/scientia.v9i2.37972>.
- Nurizki, Andhika Raka, Chairul Muriman Setyabudi, and Solikhah Yuliatiningtyas. 2026. "Governing Disinformation Through Preventive Digital Policing: Technology, Legitimacy, and Social Implications in Indonesia." *International Journal of Science and Society* 8 (1). <https://doi.org/10.54783/ijssoc.v8i1.1609>.
- Putra, Gilang Rizki Aji. 2026. "Kedudukan Bukti Digital dalam Sistem Peradilan Pidana Indonesia: Rekonsepsi Pengaturan dan Penguatan Chain of Custody di Era Cyber-Enabled Crime." *BULETIN ADALAH* 8 (7). <https://doi.org/10.15408/adalah.v8i7.51879>.
- Raslin, Harvin, Endro Sulaksono, Whisnu Argo Bintoro, Mohamad Yunus, and Mulyanto. 2021. "Efektivitas Penggelaran Sistem Elektronik Manajemen Penyidikan (E-MP) Reskrim dalam Mewujudkan Pelayanan Prima Polri." *Jurnal Litbang Polri* 24 (1). <https://doi.org/10.46976/litbangpolri.v24i1.139>.
- Raslin, Harvin, Septi Astuti, Annisa Yusuf, Suryadi, and Yana Taryana. 2024. "Evaluasi Kualitas Aplikasi Digital Korlantas Polri guna Mendukung Tugas Kepolisian dalam Rangka Penguatan Pelayanan Publik." *Jurnal Litbang Polri* 27 (3): 191–215. <https://doi.org/10.46976/litbangpolri.v27i3.245>.
- Ratcliffe, Jerry H. 2016. *Intelligence-Led Policing*. 2nd ed. London: Routledge.
- Republic of Indonesia. 2002. *Law Number 2 of 2002 concerning the Indonesian National Police*. Jakarta: Government of Indonesia.
- Republic of Indonesia. 2022. *Law Number 27 of 2022 concerning Personal Data Protection*. Jakarta: Government of Indonesia.
- Republic of Indonesia. 2024. *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*. Jakarta: Government of Indonesia.
- Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505–523. <https://doi.org/10.1111/rego.12158>.

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

N/A