

Artificial Intelligence and Predictive Policing in Indonesia: Governance, Ethics, and the Future of Law Enforcement

Choirul Amin*^{ID}

Universitas Pendidikan Indonesia, Bandung, Indonesia
choirulamin@students.upi.ac.id

DOI: <https://doi.org/10.65815/633e4r40>

Submitted: 10-01-2026

Revised: 30-04-2026, 10-06-2026

Accepted: 29-06-2026

*Corresponding Author

Abstract

Artificial intelligence is increasingly being considered for applications in policing, including crime analysis, risk assessment, pattern recognition, and predictive policing. While these technologies may enhance analytical capabilities, their use also raises concerns regarding bias, transparency, privacy, accountability, and the potential expansion of surveillance. This study examines the prospects and governance challenges associated with artificial intelligence and predictive policing in Indonesia. Using qualitative policy and conceptual analysis, the study evaluates the potential applications of AI in law enforcement while considering relevant ethical and institutional safeguards. The analysis argues that technological effectiveness cannot be separated from questions of legitimacy and governance. AI-supported policing systems may reproduce existing institutional biases when trained on incomplete or historically distorted data, while opaque algorithmic decision-making can make accountability difficult. The study therefore proposes that AI adoption should be accompanied by principles of transparency, human oversight, proportionality, data protection, and independent accountability. The article contributes to emerging scholarship on AI and policing by applying international debates concerning algorithmic governance to the Indonesian context. It concludes that responsible adoption requires institutional readiness and a governance framework that places human rights and public accountability at the centre of technological innovation.

[Kecerdasan buatan (AI) semakin dipertimbangkan untuk diterapkan dalam kegiatan kepolisian, termasuk analisis kejahatan, penilaian risiko, pengenalan pola, dan pemolisian prediktif. Meskipun teknologi ini dapat meningkatkan kemampuan analisis, penggunaannya juga menimbulkan kekhawatiran terkait bias, transparansi, privasi, akuntabilitas, dan potensi perluasan pengawasan. Studi ini mengkaji prospek serta tantangan tata kelola yang berkaitan dengan kecerdasan buatan dan pemolisian prediktif di Indonesia. Melalui analisis kebijakan dan konseptual yang bersifat kualitatif, studi ini

mengevaluasi potensi penerapan AI dalam penegakan hukum sembari mempertimbangkan aspek perlindungan etis dan kelembagaan yang relevan. Analisis ini berargumen bahwa efektivitas teknologi tidak dapat dipisahkan dari persoalan legitimasi dan tata kelola. Sistem kepolisian yang didukung AI dapat melanggengkan bias kelembagaan yang sudah ada jika dilatih menggunakan data yang tidak lengkap atau terdistorsi secara historis, sementara pengambilan keputusan algoritmik yang tidak transparan dapat menyulitkan upaya akuntabilitas. Oleh karena itu, studi ini mengusulkan agar penerapan AI dibarengi dengan prinsip-prinsip transparansi, pengawasan manusia, proporsionalitas, perlindungan data, dan akuntabilitas independen. Artikel ini memberikan kontribusi terhadap kajian yang sedang berkembang mengenai AI dan kepolisian dengan menerapkan perdebatan internasional tentang tata kelola algoritmik ke dalam konteks Indonesia. Studi ini menyimpulkan bahwa penerapan yang bertanggung jawab memerlukan kesiapan kelembagaan serta kerangka tata kelola yang menempatkan hak asasi manusia dan akuntabilitas publik sebagai inti dari inovasi teknologi.]

Keywords: artificial intelligence, predictive policing, algorithmic governance, police technology, Indonesia

Introduction

The rapid evolution of artificial intelligence (AI) and data analytics is fundamentally reshaping modern public administration, state governance, and security infrastructures globally. Among these technological innovations, predictive policing—the application of analytical, mathematical, and machine learning techniques to identify potential criminal activity, high-risk locations, or victim profiles—has emerged as a prominent tool for modernizing law enforcement organizations. Globally, police departments are increasingly adopting algorithmic systems to optimize resource allocation, enhance crime prevention, and streamline intelligence gathering. In Indonesia, state institutions and the Indonesian National Police (*Kepolisian Negara Republik Indonesia* or *Polri*) have progressively expressed enthusiasm for digital transformation, smart policing initiatives, and data-driven security frameworks. As part of broader national strategic goals toward digital governance and public service modernization, the integration of automated risk assessment tools and machine learning algorithms is viewed as an innovative solution to combat urban crime, manage public order, and address complex transnational security threats across the archipelago.

However, the deployment of artificial intelligence within police operational environments introduces profound ethical, normative, and legal complexities. While algorithmic systems offer higher data processing speeds and pattern recognition capabilities compared to traditional analytical methods, they also carry systemic risks regarding algorithmic bias, mass surveillance, invasion of privacy, and opaque decision-making. Predictive policing algorithms rely heavily on

historical crime datasets to forecast future offending patterns or geographic hotspots. When training data reflect historical over-policing, selective law enforcement, or institutional prejudices, AI models risk reinforcing and amplifying these structural inequities under the guise of technological objectivity. Furthermore, the proprietary and complex nature of algorithmic software often creates a "black box" phenomenon, rendering automated risk scores difficult to audit, contest, or justify within constitutional legal frameworks.

Within the context of post-authoritarian Indonesia, the integration of AI into law enforcement occurs against a backdrop of ongoing institutional reform, evolving data protection regimes, and persistent civil liberties challenges. Indonesia's ongoing democratic consolidation requires state security agencies to operate with strict adherence to human rights, procedural justice, and democratic accountability. The introduction of advanced surveillance networks, facial recognition systems, and predictive algorithms without clear statutory guardrails risks expanding executive power and encroaching upon individual privacy rights guaranteed under the amended 1945 Constitution. Moreover, the recent enactment of Law No. 27 of 2022 on Personal Data Protection (*UU PDP*) establishes new legal obligations regarding automated processing and data subject rights, creating an urgent necessity to align police technological adoption with national privacy standards and international human rights frameworks.

This study critically examines the prospects, risks, and governance challenges of integrating artificial intelligence and predictive policing tools into law enforcement frameworks in Indonesia. Utilizing a qualitative policy and conceptual analysis approach, the paper evaluates how algorithmic tools are conceptualized within Indonesian law enforcement, identifies core ethical and structural vulnerabilities, and outlines a comprehensive governance architecture necessary to ensure responsible technological adoption. Specifically, the analysis explores the balance between technological efficacy and public legitimacy, arguing that AI adoption must be anchored in principles of transparency, human oversight, algorithmic accountability, and robust data protection. By bridging global scholarship on algorithmic governance with the specific legal and socio-political dynamics of Indonesia, this article provides timely insights for policymakers, legal scholars, and civil society advocates seeking to align technological innovation with democratic principles.

Literature Review

The academic discourse on artificial intelligence in policing has grown significantly over the past decade, reflecting both enthusiasm for technological efficiency and deep concern over ethical governance. Early scholarship often framed predictive policing and automated risk assessment as revolutionary advancements capable of transforming law enforcement from reactive responders into proactive public safety managers (Perry et al. 2013). Proponents argue that algorithmic systems process vast volumes of structured and unstructured data—

such as historical crime logs, arrest records, spatial geography, and socio-economic indicators—to identify high-risk locations (*place-based prediction*) or individuals likely to commit or become victims of crime (*person-based prediction*). By optimizing patrol routes and directing preventative police presence to predicted hotspots, police agencies aim to reduce crime rates while maximizing efficiency under budgetary and personnel constraints.

Conversely, critical scholars in sociology, criminology, and socio-legal studies caution that predictive policing algorithms frequently automate and institutionalize historical biases (Ferguson 2017). A central critique rests on the concept of dirty data or biased inputs: predictive algorithms do not measure actual crime occurrences, but rather recorded criminal justice data, which heavily reflect past policing choices, discriminatory deployment practices, and selective enforcement (Lum and Isaac 2016). When algorithms are trained on historical arrest records that disproportionately target marginalized communities or low-income urban neighborhoods, the software continuously directs police back to those same areas. This creates a self-fulfilling feedback loop, wherein increased police presence leads to higher detection of minor offenses, generating new data that further validates the initial algorithmic prediction (Eubanks 2018). Far from being neutral or objective, automated systems can thus entrench racial, class, or geographic profiling behind a veneer of mathematical neutrality.

The literature also places heavy emphasis on the challenges of transparency, explainability, and procedural justice within algorithmic governance (Pasquale 2015). The opacity of deep learning models and proprietary software code—frequently protected by commercial trade secrets—prevents defense attorneys, oversight bodies, and affected citizens from scrutinizing how risk scores are calculated. This lack of transparency undermines constitutional principles of due process, as individuals subjected to heightened surveillance, arbitrary stops, or adverse bail and sentencing assessments are denied meaningful opportunities to challenge the underlying algorithmic logic (Zavrnik 2020). Scholars argue that procedural justice is severely compromised when citizens feel subjected to automated classification systems that lack human empathy, contextual reasoning, and transparent justification (Citron 2008).

In developing and transitional democracies, the introduction of predictive surveillance technologies carries additional structural risks regarding state power and civil liberties. Research on digital authoritarianism and technology adoption in the Global South emphasizes that security institutions in transitional regimes often adopt advanced surveillance tools faster than the legal frameworks required to regulate them (Greitens 2020). Without independent oversight mechanisms, strong data protection legislation, and active civil society monitoring, AI technologies can easily be weaponized for political surveillance, dissenting voice suppression, and social control. In the Southeast Asian context, scholars have noted that while police forces eagerly adopt smart city infrastructures and digital surveillance networks, the development of ethical guidelines, algorithmic auditing frameworks, and public

accountability remains lagging (Raza 2021). These literature gaps highlight the critical need for context-specific studies that examine how algorithmic governance can be responsibly structured within Indonesia's unique constitutional and institutional framework.

Methods

This study utilizes a qualitative policy and conceptual research methodology to evaluate the governance, ethical implications, and legal frameworks surrounding artificial intelligence and predictive policing in Indonesia. Qualitative conceptual analysis is particularly suited for examining emerging technological phenomena where empirical deployment is in formative stages, but strategic policies, legislative frameworks, and institutional initiatives are rapidly taking shape. By combining normative legal analysis with policy-oriented conceptual evaluation, this approach facilitates a rigorous assessment of how theoretical principles of algorithmic governance, data protection, and human rights apply to the operational context of the Indonesian National Police.

The data used in this study were collected through comprehensive document analysis and legal desk research, drawing from three primary categories of open-source data published up to 2025. First, national statutory legislation and regulatory frameworks were examined, including the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection (*UU PDP*), Law No. 19 of 2016 amending the Electronic Information and Transactions Law (*UU ITE*), and internal police operational guidelines. Second, policy white papers, strategic planning documents, smart city blueprints, and official statements regarding technology adoption from Polri and relevant ministries were analyzed. Third, extensive secondary literature was synthesized, including peer-reviewed journal articles, international monographs on algorithmic governance, policy briefs from civil society organizations, and reports from human rights monitoring bodies.

The analytical framework was structured around four core thematic axes derived from international standards on ethical AI deployment: legal alignment and constitutional rights, data validity and feedback loops, transparency and procedural due process, and institutional oversight and human-in-the-loop governance. Content analysis techniques were applied to identify structural gaps, legal ambiguities, and potential ethical vulnerabilities between current Indonesian regulatory frameworks and the operational requirements of AI-supported policing technologies. Each thematic area was evaluated by comparing normative standards established in international literature and Indonesian statutory mandates against the practical capabilities and risks associated with predictive software algorithms.

To ensure qualitative reliability, analytical rigour, and conceptual validity, the study implemented source triangulation and comparative contextualization. Findings derived from Indonesian legislative texts were cross-analyzed against global best practices and established international guidelines, such as the UNESCO Recommendation on the Ethics of Artificial Intelligence and the European Union

Artificial Intelligence Act framework. Potential researcher bias was mitigated by systematically evaluating both the operational benefits touted by technology developers and the ethical risks highlighted by critical criminologists. This balanced approach ensures that the study provides realistic, actionable, and legally sound policy recommendations tailored to Indonesia's constitutional governance architecture.

Analysis and Discussion

A. Technical Prospects vs. Institutional Realities in the Indonesian Context

The integration of artificial intelligence into law enforcement in Indonesia offers notable analytical prospects, particularly for processing large-scale security data across a vast and geographically fragmented archipelago. Modern police organizations face massive volumes of structured and unstructured information, ranging from emergency call logs and crime reports to traffic sensor feeds, social media activity, and digital surveillance data. Advanced machine learning models, natural language processing, and spatial-temporal pattern recognition software can synthesize these disparate datasets rapidly, enabling intelligence analysts to identify emerging crime series, map high-risk geographic areas, and optimize daily patrol distributions. In major urban centers like Jakarta, Surabaya, and Bandung, where smart city infrastructures and connected CCTV networks are expanding, AI tools can enhance operational responsiveness and assist in managing complex urban crime dynamics, traffic congestion, and public safety incidents.

However, the theoretical effectiveness of AI applications in law enforcement is strictly constrained by institutional readiness, digital infrastructure quality, and data standardization challenges across Indonesia's regional commands. Regional police headquarters (*Polda*) and local police stations (*Polres*) across different provinces exhibit substantial variations in technological capacity, data management protocols, and digital literacy. Many legacy crime databases remain fragmented, unstandardized, or manually populated, leading to inconsistent data quality, missing records, and duplicate entries. Implementing advanced predictive models on top of unreliable or unstandardized data infrastructures risks generating inaccurate risk outputs, thereby compromising operational decision-making and wasting valuable police resources. Without a unified, secure, and standardized national data architecture, the operational benefits of AI technologies will remain highly uneven and vulnerable to systemic error.

Furthermore, technological adoption within police organizations often encounters cultural and structural resistance rooted in legacy administrative practices. Police personnel trained in traditional, intuitive, or reactive methods may either reject algorithmic insights due to a lack of understanding or, conversely, demonstrate automated bias—an uncritical over-reliance on computer-generated outputs without exercising necessary professional discretion. Effective technological integration requires not merely acquiring expensive software systems,

but conducting comprehensive institutional capacity-building, digital skills training, and establishing clear operational protocols that define how algorithmic predictions should inform human field deployment.

To realize the genuine analytical potential of digital technologies while mitigating operational failures, the Indonesian National Police must prioritize foundational institutional consolidation over rapid software procurement. This requires developing robust national data governance standards, establishing centralized data quality auditing units, and modernizing legacy reporting systems to ensure data integrity. Furthermore, technological investments should focus on descriptive and diagnostic analytics that assist human analysts in understanding complex crime trends, rather than relying prematurely on fully automated predictive scoring mechanisms. Aligning technological procurement with institutional capacity ensures that digital tools serve as effective, reliable aids to professional law enforcement rather than unverified sources of operational disruption.

B. Algorithmic Bias, Historical Data Distortion, and Structural Inequities

A critical ethical vulnerability of predictive policing lies in the risk of reproducing and amplifying structural biases embedded in historical crime data. Predictive algorithms rely on historical records—such as past arrests, incident reports, stop-and-frisk logs, and citizen complaints—to learn patterns and forecast future criminal activity. In any society, historical criminal justice data do not reflect an objective, complete measurement of all crimes committed; rather, they reflect where law enforcement officers were deployed and which populations were subjected to heightened scrutiny. In Indonesia, historical policing patterns have been shaped by socio-economic disparities, urban-rural divides, and localized political dynamics. Training machine learning models on historical crime datasets that contain disproportionate focus on low-income informal settlements or specific socio-demographic groups ensures that the software will disproportionately classify those same communities as perpetual high-risk zones.

This dynamic creates a destructive algorithmic feedback loop that reinforces spatial and social stigmatization. When a predictive model identifies a low-income urban neighborhood as a predicted hotspot based on historical arrest records for minor offenses, police commanders deploy additional patrols to that targeted area. Increased police presence inevitably leads to higher rates of officer-initiated stops, arrests for minor infractions, and field inquiries, generating new data points that confirm the algorithm's initial prediction. Meanwhile, crimes committed in higher-income residential areas or non-spatial offenses like white-collar corporate crime, corruption, and cybercrime remain systematically uncaptured by spatial predictive models. Consequently, predictive policing risk tools can transform historical over-policing and institutional biases into self-validating mathematical facts, further marginalizing vulnerable populations under the guise of technological objectivity.

Addressing algorithmic bias in Indonesia is further complicated by the lack of technical mechanisms for auditing data representative quality and model fairness. Machine learning algorithms operating as complex deep neural networks or proprietary software often lack explainable decision logic, making it difficult for technical teams to detect whether specific variables—or proxy variables like geographic location, socio-economic status, or age—are generating discriminatory outcomes. Without rigorous pre-deployment auditing of training datasets, police agencies risk deploying software that violates constitutional non-discrimination guarantees under Article 28I of the 1945 Constitution, exposing law enforcement institutions to legal challenges and severe public reputational damage.

Mitigating algorithmic bias requires establishing strict data auditing protocols and fairness metrics prior to deploying any analytical model in public safety contexts. Law enforcement agencies must conduct comprehensive data hygiene reviews to identify and remove historically distorted, incomplete, or proxy-biased variables from training datasets. Furthermore, predictive software must be evaluated using independent algorithmic impact assessments (AIAs) that measure whether predicted risk outputs disproportionately impact specific demographic groups or geographic regions. Integrating technical fairness standards into software development ensures that technological tools do not perpetuate historical inequities, safeguarding citizen rights and reinforcing public trust in law enforcement integrity.

C. Transparency, Privacy, and the Legal Framework for Data Protection

The deployment of AI-powered predictive policing and automated risk scoring systems poses significant challenges to individual privacy rights, public transparency, and procedural due process. Predictive policing systems rely heavily on continuously collecting, aggregating, and processing vast amounts of personal data from multiple sources, including biometric identifiers, facial recognition feeds, vehicle license plate readers, and digital communication logs. In the absence of strict statutory limitations, the continuous, automated collection of personal data creates an pervasive surveillance environment that infringes upon the constitutional right to personal privacy (*hak atas perlindungan diri pribadi*) guaranteed under Article 28G of the 1945 Constitution. Mass automated surveillance threatens to produce a chilling effect on public life, discouraging citizens from exercising fundamental freedoms of assembly, movement, and peaceful expression in public spaces.

The legal landscape governing data protection in Indonesia was fundamentally transformed with the passage of Law No. 27 of 2022 on Personal Data Protection (*UU PDP*). The PDP Law establishes strict statutory principles regarding data processing legality, purpose limitation, data minimization, and the explicit rights of data subjects. Crucially, Article 50 of the PDP Law recognizes the

right of individuals to object to automated decision-making processes that produce legal consequences or significantly affect their lives. Applying these statutory principles to law enforcement AI systems creates a legal requirement for police agencies to establish clear lawful bases for processing personal data, maintain strict access controls, and provide mechanisms for individuals to seek redress if automated risk profiling leads to arbitrary police interventions, unlawful detentions, or inaccurate criminal classification.

Transparency and procedural due process are further compromised by the "black box" nature of many commercial predictive policing platforms. When police agencies purchase proprietary software from private vendors, the underlying code, weighting factors, and mathematical algorithms are frequently protected as commercial trade secrets. In a constitutional criminal justice system, individuals subjected to police action—such as targeted stops, searches, or heightened risk classification—have a fundamental right to know the legal and factual basis of the state's suspicion. If an officer's suspicion is generated by an opaque, proprietary algorithm that cannot be explained, audited, or cross-examined in a court of law, the citizen's right to due process and a fair defense is fundamentally undermined.

To align AI adoption with national data protection legislation and constitutional due process standards, Indonesia must establish clear legal boundaries governing police data processing and algorithm transparency. Police agencies must be legally prohibited from utilizing fully opaque, un-auditable "black box" algorithms for operational decision-making. Software procurement mandates should require full code access, technical explainability, and open documentation for independent review. Furthermore, police data processing protocols must comply strictly with *UU PDP* mandates, ensuring that personal data collected for security purposes are subject to purpose limitation, secure storage, and strict oversight by the National Personal Data Protection Authority.

D. Governance, Human Oversight, and Independent Accountability Architecture

Developing a responsible, democratic AI policing regime requires constructing a robust governance framework founded on human oversight, institutional accountability, and continuous independent supervision. A fundamental principle of ethical algorithmic governance is the requirement of "human-in-the-loop" decision-making. Automated systems, no matter how sophisticated, should function strictly as supportive analytical tools rather than autonomous decision-makers. In law enforcement contexts, an algorithmic risk prediction or spatial hotspot map must never serve as sole legal grounds for executing arrests, conducting searches, or initiating coercive police measures. Every operational action must require meaningful, contextualized evaluation by a trained human officer who remains fully accountable under public law for the legality and proportionality of the resulting intervention.

Designing an effective governance architecture for police technology in Indonesia requires establishing clear external oversight and auditing mechanisms. Current oversight bodies—such as the National Police Commission (*Kompolnas*), the National Human Rights Commission (*Komnas HAM*), and the National Ombudsman—must be equipped with specialized technical capacity and statutory authority to monitor police technology adoption. This includes establishing a dedicated Algorithmic Oversight Committee composed of data scientists, legal experts, human rights advocates, and civil society representatives. This independent body should be empowered to conduct mandatory pre-deployment algorithmic impact assessments, perform routine code and data audits, inspect data storage security, and investigate public complaints regarding algorithmic discrimination or automated abuse.

Furthermore, clear institutional mechanisms for command responsibility and legal liability must be established to prevent accountability gaps when technology fails. When an algorithmic system generates a false positive that leads to wrongful detention, property damage, or civil rights violations, accountability must not be deflected onto the software vendor or the computer system itself. Legal liability must rest clearly with the police leadership that authorized the software's deployment and the field commanders who executed the operational decision. Establishing explicit legal chains of command ensures that police officials maintain rigorous supervision over technological tools, preventing the erosion of professional standards and preserving public accountability.

Finally, public participation, ethical transparency, and multi-stakeholder dialogue must be embedded into the lifecycle of police technology governance. Before deploying automated surveillance, facial recognition, or predictive analytics in public spaces, police agencies should be required to conduct public consultations and publish plain-language summaries of the technology's scope, purpose, legal basis, and privacy safeguards. Open public engagement demystifies security technology, allows civil society to highlight localized risks, and fosters collaborative trust between communities and law enforcement. By anchoring technological innovation in human rights, public transparency, and independent accountability, Indonesia can harness the analytical power of artificial intelligence while safeguarding its democratic institutions and constitutional values.

Conclusion

The integration of artificial intelligence and predictive analytical tools into law enforcement represents a transformative frontier for police governance and public safety management in Indonesia. As the nation advances its digital governance infrastructure and smart policing initiatives, automated analytics and predictive models offer genuine opportunities to process complex data, enhance situational awareness, and optimize strategic resource allocation across the archipelago. However, as demonstrated throughout this study, technological efficacy cannot be isolated from questions of democratic legitimacy, human rights, and constitutional

law. The operational deployment of AI tools carries profound risks of automating historical biases, creating feedback loops of over-policing in vulnerable communities, eroding individual privacy rights, and obscuring state accountability behind opaque algorithmic systems.

To ensure that the adoption of police technologies reinforces rather than undermines democratic consolidation, Indonesia must establish a comprehensive, human-rights-centered governance framework. Technological tools must never replace human context, professional judgment, or legal standards of reasonable suspicion; they must function strictly under meaningful human oversight. Adherence to the Personal Data Protection Law (*UU PDP*), statutory bans on opaque "black box" commercial algorithms, and mandatory pre-deployment algorithmic impact assessments are essential legal requirements to prevent arbitrary state surveillance and protect due process. Furthermore, empowering independent oversight bodies like *Kompolnas* and *Komnas HAM* with technical auditing capabilities will ensure that algorithmic systems remain transparent, fair, and publicly accountable.

Ultimately, the future of law enforcement in Indonesia depends not on the uncritical procurement of advanced software, but on the institutional commitment to align technological innovation with democratic values. Artificial intelligence should serve as an instrument to enhance justice, procedural fairness, and public protection for all citizens, rather than a mechanism for expanded state control. By placing human dignity, constitutional rights, and robust independent accountability at the center of technological strategy, Indonesia can build a modern, professional, and democratically accountable law enforcement system equipped to meet the security challenges of the digital age.

References

- Aspinall, Edward, and Marcus Mietzner. 2019. "Southeast Asia's Troubling Elections: Nondemocratic Pluralism in Indonesia." *Journal of Democracy* 30 (4): 104–118.
- Citron, Danielle Keats. 2008. "Technological Due Process." *Washington University Law Review* 85 (6): 1249–1313.
- Diprose, Rachael, Dave McRae, and Vedi R. Hadiz. 2019. "Two Decades of Reformasi in Indonesia: Its Illiberal Turn and Other Trajectories." *Journal of Contemporary Asia* 49 (5): 691–712.
- Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.
- European Union. 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels: Official Journal of the European Union.

- Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
- Greitens, Sheena Chestnut. 2020. "Dealing with Demand: The Domestic Politics of Chinese Surveillance Technology Exports." *Global China*, Brookings Institution Report, November 2020.
- Lum, Kristian, and William Isaac. 2016. "To Predict and Serve? Analyzing the Bias in Predictive Policing Models." *Significance* 13 (5): 14–19.
- National Human Rights Commission (Komnas HAM). 2023. *Kajian Hak Asasi Manusia Terhadap Penggunaan Teknologi Pengawasan dan Intelijen Digital di Indonesia*. Jakarta: Komnas HAM.
- National Police Commission (Kopolnas). 2022. *Laporan Strategis Modernisasi Teknologi Informasi dan Pelayanan Publik Polri*. Jakarta: Kopolnas.
- Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
- Perry, Walter L., Brian McInnis, Carter C. Price, Susan C. Smith, and John S. Hollywood. 2013. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation.
- Power, Thomas. 2018. "Jokowi's Authoritarian Turn and Indonesia's Democratic Decline." *Bulletin of Indonesian Economic Studies* 54 (3): 307–338.
- Raza, Aamir. 2021. "Smart Cities, Big Data, and Surveillance in Southeast Asia: Governance and Civil Liberties in the Digital Age." *Asian Journal of Political Science* 29 (3): 289–307.
- Republic of Indonesia. 1945. *The 1945 Constitution of the Republic of Indonesia*. Jakarta: State Gazette.
- Republic of Indonesia. 2002. *Law No. 2 of 2002 concerning the Indonesian National Police*. Jakarta: State Gazette No. 2.
- Republic of Indonesia. 2016. *Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE)*. Jakarta: State Gazette No. 257.
- Republic of Indonesia. 2022. *Law No. 27 of 2022 concerning Personal Data Protection (UU PDP)*. Jakarta: State Gazette No. 227.
- UNESCO. 2021. *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization.
- Warburton, Eve. 2020. "Deepening Polarization and Democratic Backsliding in Indonesia." *Asian Survey* 60 (1): 18–40.
- Zavrnik, Aleš. 2020. "Criminal Justice, Artificial Intelligence, and Big Data in the Surveillance Society." *Frontiers in Psychology* 11: 1942–1953.

This page is intentionally left blank

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