**Indonesian Journal *of* Digital Crime *and* Criminal Justice**
Vol. 1 No. 1. January 2025. pp. 85-124
E-ISSN: XXXX-XXXX| P-ISSN: XXXX-XXX
**Original Research Article**

# Algorithmic Policing and Due Process Rights: Balancing Efficiency and Fairness in Criminal Justice in Indonesia

**Hans Ari Saputra** [1]*
[1] Central Java Police Department, Semarang, Indonesia
* Corresponding author: hans_saputra@gmail.com

## ABSTRACT

The integration of algorithmic systems in policing has transformed criminal justice administration by enhancing predictive capabilities and operational efficiency. However, the deployment of algorithmic policing raises critical concerns regarding due process rights, transparency, and potential bias. This article examines the implications of algorithm-driven law enforcement practices in Indonesia, focusing on the tension between technological efficiency and fundamental legal safeguards. Using normative legal research combined with comparative insights from jurisdictions such as the United States and the European Union, the study evaluates whether existing Indonesian legal frameworks adequately regulate algorithmic decision-making in policing. The findings indicate that while algorithmic tools may improve crime detection and resource allocation, they also risk reinforcing structural biases embedded in training data, leading to discriminatory outcomes. Furthermore, the lack of transparency and explainability in algorithmic systems undermines the principles of fair trial and accountability. The article argues that Indonesia's criminal justice system requires regulatory intervention to ensure algorithmic accountability, including mandatory impact assessments, transparency obligations, and judicial oversight mechanisms. It concludes that balancing efficiency and fairness necessitates a rights-based regulatory approach to algorithmic policing.

**KEYWORDS:** Algorithmic Policing, Due Process, Criminal Justice Indonesia, Artificial Intelligence, Fair Trial, Digital Governance

## INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed contemporary law enforcement practices across the globe.

Available online at https://journal.criminallawinstitute.org/JDCCJ/article/view/18, since January 15, 2026
Submitted: November 11, 2024 ■ Reviewed: November 27, 2024 ■ Revised: January 5, 2026 ■ Accepted: January 15, 2025

Traditional policing models, which largely relied on human observation, investigative experience, and reactive responses to criminal incidents, are increasingly being supplemented by data-driven approaches that leverage artificial intelligence (AI), machine learning, and big data analytics. This transformation reflects broader developments in digital governance, where public institutions adopt computational technologies to enhance efficiency, predictability, and evidence-based decision-making (Yeung 2018). Within the criminal justice sector, algorithmic systems are increasingly employed to identify crime patterns, allocate police resources, assess risks, and support investigative processes (Ferguson 2017).

The emergence of big data has significantly contributed to this shift. Modern policing institutions now collect and process vast amounts of information derived from surveillance systems, social media platforms, criminal records, geospatial data, and other digital sources. Through sophisticated analytical tools, these datasets can be utilized to identify correlations and generate predictive insights regarding potential criminal activities (Brayne 2021). Consequently, law enforcement agencies increasingly rely on algorithmic technologies to improve operational effectiveness and optimize resource allocation in environments characterized by limited personnel and growing security challenges.

Predictive policing represents one of the most prominent manifestations of algorithmic governance in criminal justice. Predictive policing systems employ statistical models and machine learning techniques to forecast where crimes are likely to occur, identify individuals considered at elevated risk of criminal involvement, or determine areas requiring intensified police presence (Perry et al. 2013). Advocates argue that such technologies enhance crime prevention capabilities, improve efficiency, and reduce operational costs. However, critics contend that predictive systems may reproduce historical biases embedded within training datasets, thereby generating discriminatory outcomes that disproportionately affect marginalized communities (Lum and Isaac 2016).

The increasing reliance on algorithmic technologies reflects a broader transition toward automated decision-making in public administration.

While technological innovation promises enhanced institutional performance, it simultaneously raises fundamental questions regarding accountability, transparency, and the protection of individual rights. These concerns are particularly significant within criminal justice systems, where state actions directly affect personal liberty, equality before the law, and procedural fairness.

The deployment of algorithmic policing technologies has evolved into a significant global legal and policy issue. In the United States, law enforcement agencies have experimented extensively with predictive policing platforms such as PredPol and risk assessment algorithms designed to support criminal justice decision-making (Ferguson 2017). These systems emerged from the belief that data analytics could enhance crime prevention and improve public safety outcomes. Nevertheless, empirical studies have revealed substantial concerns regarding algorithmic bias and racial disparities. Research demonstrates that predictive policing systems frequently rely on historical arrest data, which may reflect existing patterns of discriminatory policing rather than objective measures of criminal behavior (Lum and Isaac 2016).

The controversy surrounding algorithmic policing in the United States has generated extensive scholarly debate concerning constitutional protections and due process rights. Legal scholars argue that opaque algorithmic systems challenge fundamental procedural safeguards because individuals affected by algorithmic decisions often lack meaningful opportunities to understand, contest, or scrutinize the basis of such determinations (Citron and Pasquale 2014). The so-called "black box" nature of many AI systems creates significant obstacles to accountability, particularly when algorithmic outputs influence law enforcement interventions, surveillance practices, or prosecutorial decisions.

In Europe, concerns regarding algorithmic governance have prompted a more rights-oriented regulatory response. The European Union has increasingly emphasized transparency, explainability, and human oversight in the deployment of AI systems. Regulatory initiatives such as the Artificial Intelligence Act reflect efforts to establish legal safeguards against high-risk AI applications that may adversely affect fundamental rights (Veale and

Borgesius 2021). European human rights institutions have similarly highlighted the importance of ensuring that algorithmic decision-making remains compatible with principles of legality, proportionality, and non-discrimination.

Beyond the United States and Europe, algorithmic policing technologies are expanding across diverse jurisdictions, including Asia, Latin America, and Africa. Governments increasingly view AI-driven law enforcement as an essential component of smart city initiatives and digital governance strategies (Završnik 2021). However, the global diffusion of algorithmic policing has also intensified concerns regarding surveillance expansion, data protection, and human rights protection. Scholars of algorithmic governance argue that technological systems are not neutral instruments but rather socio-technical constructs that reflect institutional assumptions, political priorities, and underlying power relations (Yeung 2018).

Existing scholarship has generated substantial insights regarding algorithmic governance, AI regulation, and criminal justice innovation. Studies have examined the operational benefits of predictive policing, the ethical implications of automated decision-making, and the challenges associated with algorithmic accountability (Brayne 2021; Ferguson 2017). Similarly, due process scholarship has emphasized the importance of procedural safeguards, transparency, and judicial review in preventing arbitrary exercises of state power (Citron and Pasquale 2014). Human rights scholars have further highlighted the risks that algorithmic systems may pose to privacy, equality, and non-discrimination principles (McGregor, Murray, and Ng 2019).

Despite these contributions, significant gaps remain in the existing literature. Much of the current scholarship focuses on Western jurisdictions, particularly the United States and the European Union. Relatively limited attention has been devoted to understanding how algorithmic policing may affect due process rights within developing legal systems characterized by evolving digital governance frameworks. This gap is particularly evident in the Indonesian context, where discussions of AI governance have largely concentrated on data protection, cybersecurity, and ethical principles rather

than procedural justice concerns.

In this context, Indonesia has experienced substantial digital transformation over the past decade. Government initiatives promoting digital governance, smart cities, and electronic public services have accelerated the adoption of advanced technologies across multiple sectors. Law enforcement institutions have similarly embraced digital innovations aimed at enhancing operational effectiveness, improving public service delivery, and strengthening crime prevention capabilities.

The Indonesian National Police have implemented various digital policing initiatives, including integrated information systems, electronic traffic enforcement mechanisms, facial recognition technologies, and data-driven surveillance practices. These developments reflect broader governmental commitments to technological modernization and digital transformation. Moreover, emerging discussions regarding AI adoption indicate growing institutional interest in deploying advanced analytical tools to support policing functions and criminal investigations.

However, the rapid adoption of technological solutions has not been accompanied by equally comprehensive regulatory development. Indonesia currently lacks a dedicated legal framework governing algorithmic decision-making in law enforcement contexts. Existing regulations primarily address electronic information systems, personal data protection, and general administrative governance without specifically addressing the procedural implications of algorithmic policing. Consequently, important questions remain regarding transparency requirements, accountability mechanisms, and legal remedies available to individuals affected by algorithm-driven decisions.

Institutional challenges further complicate the regulatory landscape. Law enforcement agencies increasingly depend on digital technologies while simultaneously operating within legal frameworks that were largely developed before the emergence of sophisticated AI systems. This regulatory gap creates uncertainty regarding the legality, oversight, and evidentiary status of algorithmic outputs within criminal justice processes. As technological reliance expands, ensuring compatibility between innovation

and constitutional safeguards becomes an increasingly urgent policy objective.

Existing studies on AI governance in Indonesia predominantly focus on issues of privacy protection, cybersecurity regulation, personal data governance, and ethical principles surrounding emerging technologies. While these topics remain important, limited scholarly attention has been devoted to examining the implications of algorithmic policing for due process rights within Indonesia's criminal justice system.

Furthermore, comparative scholarship on predictive policing often concentrates on technical performance, crime reduction outcomes, or ethical considerations rather than comprehensive legal analyses of procedural fairness. Consequently, there remains insufficient understanding of how algorithmic decision-making may affect constitutional guarantees such as equality before the law, presumption of innocence, fair trial rights, and access to effective remedies. This article addresses this gap by situating algorithmic policing within the broader framework of due process protection and criminal justice governance in Indonesia.

This study seeks to answer the following primary research question: How does algorithmic policing affect due process rights within Indonesia's criminal justice system? To address this central inquiry, the article examines three supporting questions:

1. What legal risks arise from the implementation of algorithmic policing technologies?
2. Are existing Indonesian legal safeguards sufficient to address these risks?
3. What regulatory reforms are necessary to ensure accountability, transparency, and protection of due process rights?

These questions are explored through normative legal analysis supported by comparative examination of regulatory developments in the United States and the European Union.

This article argues that algorithmic policing possesses significant potential to enhance law enforcement efficiency through improved crime detection, predictive analytics, and resource allocation. Nevertheless, the

deployment of algorithmic systems simultaneously generates substantial risks for due process rights, particularly when decision-making processes lack transparency, explainability, and meaningful oversight.

The article further contends that Indonesia's current legal framework remains insufficient to address these challenges. Existing regulations do not adequately govern algorithmic decision-making in policing contexts, creating legal uncertainties regarding accountability, procedural fairness, and judicial review. As a result, individuals affected by algorithmic interventions may face difficulties in understanding, challenging, or contesting decisions that significantly impact their rights and liberties.

Accordingly, this study proposes a rights-based regulatory framework for algorithmic policing in Indonesia. Such a framework should incorporate mandatory algorithmic impact assessments, transparency obligations, explainability requirements, independent auditing mechanisms, and robust judicial oversight procedures. By integrating these safeguards, Indonesia can pursue technological innovation while preserving the fundamental principles of due process, equality, and the rule of law. The article contributes to emerging scholarship on AI governance by connecting debates on algorithmic policing with constitutional guarantees and criminal justice reform in developing legal systems.

## ALGORITHMIC POLICING & THE TRANSFORMATION OF CRIMINAL JUSTICE

### A. Understanding Algorithmic Policing

The emergence of algorithmic policing represents one of the most significant transformations in contemporary criminal justice governance. Advances in computational technologies have enabled law enforcement agencies to process unprecedented volumes of information, generate predictive insights, and support decision-making through automated systems. Although algorithmic policing is often associated with technological innovation and administrative efficiency, its conceptual foundations remain subject to considerable academic debate. Understanding the nature of

algorithmic policing requires clarification of several interconnected concepts, including algorithms, artificial intelligence, machine learning, and predictive analytics.

At its most basic level, an algorithm refers to a structured sequence of instructions designed to perform specific tasks or solve particular problems (Yeung 2018). Algorithms have long existed within administrative and legal systems; however, recent developments in computational power and data availability have significantly expanded their practical applications. Within criminal justice institutions, algorithms increasingly function as decision-support mechanisms that process large datasets and generate outputs intended to guide operational activities. The significance of algorithms lies not merely in their technical capabilities but also in their capacity to shape institutional judgments and influence governmental actions.

Artificial intelligence constitutes a broader technological category encompassing systems capable of performing tasks that traditionally require human cognitive abilities, such as pattern recognition, classification, prediction, and decision-making (Russell and Norvig 2021). Contemporary discussions of algorithmic policing frequently focus on AI-driven applications because such systems can identify relationships within complex datasets that may not be immediately observable to human analysts. While proponents emphasize the ability of AI to improve law enforcement efficiency, critics caution that automated systems often replicate existing institutional biases embedded within historical data (Crawford 2021).

Machine learning, a subset of artificial intelligence, has become particularly influential in policing contexts. Unlike traditional software programs that operate according to explicitly defined rules, machine learning systems develop predictive models by identifying patterns within training datasets (Mittelstadt et al. 2016). Through continuous data processing, these systems can adapt and refine their predictions over time. However, machine learning systems are not inherently objective. Their outputs depend heavily on the quality, representativeness, and neutrality of the data upon which they are trained. Consequently, concerns regarding discrimination and unfair treatment emerge when historical datasets reflect existing patterns of unequal

law enforcement practices.

Predictive analytics constitutes the practical application of algorithmic and machine learning techniques to forecast future events or behaviors. In policing environments, predictive analytics is utilized to estimate crime risks, identify potential offenders, and determine areas requiring heightened police attention (Perry et al. 2013). Such technologies exemplify the growing shift from reactive law enforcement toward anticipatory governance, where intervention is increasingly based on probabilistic assessments rather than established criminal conduct.

These technological developments have generated several forms of algorithmic policing. One of the most widely discussed examples is predictive policing, which employs statistical models to identify locations, individuals, or circumstances associated with elevated risks of criminal activity. Predictive policing systems seek to optimize resource allocation by directing law enforcement efforts toward areas considered vulnerable to future crimes (Ferguson 2017). Supporters argue that predictive models enhance efficiency and crime prevention capabilities, while critics contend that they frequently reinforce existing patterns of over-policing in marginalized communities.

Another important form of algorithmic policing involves risk assessment systems. These systems evaluate the likelihood that individuals will engage in criminal conduct, fail to appear in court, or reoffend after release. Risk assessment tools have become increasingly influential within criminal justice processes, including bail decisions, sentencing recommendations, and parole evaluations (Berk 2017). Despite their apparent objectivity, scholars have questioned whether algorithmic risk classifications reproduce structural inequalities by relying on variables that correlate with socioeconomic disadvantage or historical discrimination.

Facial recognition technologies have also emerged as a significant component of algorithmic policing. These systems utilize biometric algorithms to identify or verify individuals based on facial characteristics. While facial recognition technologies may assist criminal investigations and public security operations, empirical research demonstrates that their accuracy varies across demographic groups, potentially leading to

disproportionate misidentification of racial and ethnic minorities (Garvie, Bedoya, and Frankle 2016). The deployment of facial recognition technologies therefore raises important questions regarding accuracy, accountability, and procedural justice.

In addition, automated surveillance systems increasingly combine artificial intelligence with extensive data collection infrastructures. These systems monitor public spaces, analyze behavioral patterns, and generate alerts regarding potentially suspicious activities. Although such technologies may enhance situational awareness and crime prevention capacities, they simultaneously expand state surveillance capabilities and create significant risks for civil liberties and individual autonomy (Zuboff 2019).

## B. Algorithmic Decision-Making in Criminal Justice

The growing adoption of algorithmic systems reflects broader transformations in criminal justice decision-making. Traditionally, policing decisions were primarily based on professional discretion, investigative expertise, and contextual judgment. Contemporary law enforcement increasingly supplements these human-centered approaches with data-driven analytical tools that influence operational priorities and strategic planning. As a result, algorithmic decision-making has become an integral component of modern criminal justice governance.

One of the primary applications of algorithmic decision-making involves crime prediction. Through the analysis of historical crime data, demographic information, and environmental variables, predictive systems generate forecasts regarding future criminal activities. These forecasts are subsequently used to inform patrol deployment, surveillance strategies, and preventive interventions (Perry et al. 2013). The underlying rationale is that more accurate predictions will enable law enforcement agencies to allocate resources more efficiently and reduce criminal incidents before they occur.

Resource allocation represents another important dimension of algorithmic governance. Police organizations operate under significant financial and personnel constraints, making efficient deployment a critical operational concern. Algorithmic systems assist decision-makers by

identifying areas considered high-risk and recommending resource distribution strategies based on statistical analyses. Such approaches align with broader public administration trends emphasizing performance optimization and evidence-based policymaking (Brayne 2021). Nevertheless, efficiency gains may come at the expense of fairness if predictive models systematically target particular communities.

Algorithmic decision-making also plays a central role in automated risk classification. Criminal justice institutions increasingly utilize risk scores to categorize individuals according to perceived levels of threat, dangerousness, or recidivism. These classifications influence decisions regarding detention, supervision, and intervention priorities. While risk-based approaches aim to improve consistency and objectivity, scholars have noted that algorithmic classifications often obscure normative judgments behind technical calculations (Citron and Pasquale 2014). Consequently, individuals may be subjected to adverse consequences based on statistical probabilities rather than demonstrable conduct.

These developments are closely connected to the rise of intelligence-led policing. Intelligence-led policing emphasizes proactive crime prevention through systematic data analysis, information sharing, and strategic risk management. Algorithmic systems enhance this model by enabling the rapid processing of large datasets and generating actionable intelligence for operational purposes (Ratcliffe 2016). However, the increasing integration of algorithmic tools into intelligence-led policing also raises concerns regarding transparency and democratic accountability, particularly when predictive assessments influence coercive state actions.

### C. Due Process as a Fundamental Legal Principle

The expansion of algorithmic policing must be evaluated against the foundational legal principle of due process. Due process constitutes one of the central safeguards within constitutional democracies, ensuring that governmental authority is exercised in accordance with law and that individuals are protected against arbitrary state action. Although the precise formulation of due process varies across legal systems, its underlying

objectives remain closely associated with the rule of law, constitutionalism, and fair trial guarantees.

Historically, the concept of due process emerged from broader struggles to limit governmental power and protect individual liberties. The rule of law tradition emphasizes that public authorities must act within legally established boundaries and remain accountable to legal norms rather than arbitrary discretion (Dicey 1982). Constitutionalism further reinforces this principle by establishing institutional mechanisms that constrain governmental authority and safeguard fundamental rights. Together, these traditions form the normative foundation for procedural protections within modern criminal justice systems.

Fair trial principles constitute another essential component of due process. International human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, recognize procedural fairness as a fundamental legal entitlement. These protections ensure that individuals are treated fairly throughout criminal proceedings and possess meaningful opportunities to defend their interests against state accusations (Ashworth and Redmayne 2010).

Several core components define contemporary understandings of due process. The presumption of innocence requires that individuals be regarded as innocent until proven guilty through lawful procedures. This principle serves as a safeguard against premature judgments and arbitrary punishment. In criminal justice contexts, the presumption of innocence limits the state's ability to impose burdens on individuals based solely on suspicion or perceived risk.

Equality before the law represents another fundamental element of procedural justice. Legal systems committed to due process must ensure that individuals receive equal treatment regardless of social status, ethnicity, economic position, or other personal characteristics. This principle becomes particularly relevant in algorithmic environments because discriminatory data patterns may produce unequal outcomes despite the appearance of technological neutrality (Selbst 2017).

Procedural fairness further requires transparency, consistency, and opportunities for participation. Individuals affected by governmental decisions should understand the basis of those decisions and possess meaningful opportunities to challenge adverse outcomes. Procedural legitimacy depends not only on substantive accuracy but also on the fairness of decision-making processes themselves (Tyler 2006).

Closely related to these principles is the right to challenge state action. Due process requires that governmental decisions remain subject to review, appeal, and independent scrutiny. Accountability mechanisms ensure that public authorities cannot exercise coercive powers without justification and oversight. In democratic legal systems, the ability to contest governmental decisions functions as a critical safeguard against abuse of power.

### D. Why Algorithmic Policing Challenges Due Process

The increasing adoption of algorithmic policing introduces significant tensions between technological efficiency and procedural justice. A central concern arises from the shift from reactive to predictive models of criminal justice. Traditional criminal law generally responds to completed or attempted conduct. Algorithmic policing, by contrast, seeks to anticipate future risks and intervene before criminal behavior occurs. This transformation fundamentally alters the temporal orientation of law enforcement by emphasizing probabilities rather than established facts (Završnik 2021).

The rise of predictive governance is closely linked to broader trends in risk-based regulation. Contemporary governments increasingly rely on risk assessments to manage uncertainty and allocate resources. Within criminal justice systems, algorithmic tools classify individuals and communities according to predicted levels of danger, thereby shaping policing priorities and intervention strategies. Although risk-based approaches may improve efficiency, they also risk undermining principles of individual responsibility by focusing on statistical group characteristics rather than personal conduct.

Perhaps the most profound challenge concerns the emergence of automated suspicion. Algorithmic systems generate predictions and risk

scores that may influence police attention, surveillance intensity, and investigative decisions. Individuals can therefore become subjects of suspicion not because of proven wrongdoing but because algorithmic models identify correlations associated with future risk. This development raises fundamental due process concerns because it blurs the distinction between evidence-based suspicion and probabilistic prediction.

Furthermore, many algorithmic systems operate through opaque computational processes that are difficult for affected individuals, legal practitioners, and even government officials to understand. The absence of transparency complicates efforts to evaluate the legality, accuracy, and fairness of algorithmic decisions. As a result, procedural safeguards traditionally associated with due process—including explanation, reviewability, and contestability—may become significantly weakened. These concerns provide the analytical foundation for examining the implications of algorithmic policing within Indonesia's criminal justice system in the subsequent sections of this article.

## EFFICIENCY GAINS *&* OPERATIONAL JUSTIFICATIONS FOR ALGORITHMIC POLICING

### A. Crime Prevention Benefits

One of the most frequently cited justifications for the adoption of algorithmic policing lies in its potential to enhance crime prevention capabilities. Contemporary criminal justice systems are increasingly expected to operate under conditions of resource scarcity, rising crime complexity, and heightened public demand for safety. In this context, algorithmic tools are promoted as instruments capable of improving foresight and enabling more proactive forms of policing. The core promise of algorithmic policing is that data-driven prediction can transform crime prevention from a reactive to a preventive model (Perry et al. 2013).

A central mechanism through which algorithmic systems contribute to crime prevention is crime forecasting. By analyzing historical crime data, temporal trends, and spatial distributions, predictive models attempt to

estimate where and when future criminal incidents are most likely to occur. These forecasts are then used to guide policing strategies, enabling law enforcement agencies to allocate patrols and surveillance resources more strategically (Ferguson 2017). Crime forecasting is often framed as a scientific advancement that reduces reliance on intuition or discretionary judgment.

Hotspot identification represents another key function of algorithmic policing. Hotspot policing techniques rely on geospatial analytics to identify areas with statistically higher concentrations of criminal activity. These identified zones are then prioritized for increased police presence and intervention measures. Empirical studies suggest that hotspot policing may contribute to short-term reductions in certain types of crime, particularly property-related offenses (Braga et al. 2019). However, the effectiveness of hotspot identification is contingent on the quality and neutrality of underlying data, which may reflect historical enforcement patterns rather than actual crime prevalence.

Resource deployment constitutes a further operational benefit associated with algorithmic policing. Law enforcement agencies often face constraints in personnel, funding, and logistical capacity. Algorithmic systems assist in optimizing resource allocation by providing recommendations regarding where officers should be deployed and how operational priorities should be structured. In theory, this enables more efficient use of limited resources and enhances institutional responsiveness (Brayne 2021). Nevertheless, such optimization processes may inadvertently concentrate policing in already over-surveilled communities, thereby reinforcing structural inequalities.

### B. Investigative Efficiency

Beyond preventive functions, algorithmic policing is widely justified on the basis of its ability to improve investigative efficiency. Modern law enforcement agencies operate within increasingly complex informational environments characterized by vast volumes of digital evidence, communication data, and surveillance inputs. Traditional investigative methods are often insufficient to process such large datasets in a timely manner. Algorithmic tools therefore play a critical role in enhancing the speed

and accuracy of investigative processes.

Data processing is one of the most significant efficiency gains associated with algorithmic policing. Machine learning systems and automated analytics tools can process large-scale datasets far more rapidly than human analysts. This includes structured data such as criminal records as well as unstructured data such as social media activity, audio recordings, and video surveillance footage. The ability to process heterogeneous datasets allows law enforcement agencies to identify relevant information more efficiently and reduce investigative delays (Mittelstadt et al. 2016).

Pattern recognition represents another key advantage of algorithmic systems. Machine learning algorithms are particularly effective at identifying correlations and patterns within complex datasets that may not be immediately apparent to human investigators. These patterns can assist in linking criminal incidents, identifying networks of suspects, and uncovering behavioral trends relevant to ongoing investigations. In certain contexts, pattern recognition tools have been used to support financial crime investigations, trafficking cases, and fraud detection operations (Berk 2017).

Real-time monitoring further enhances investigative capacity by enabling continuous surveillance and immediate response mechanisms. Through the integration of sensor technologies, surveillance cameras, and automated alert systems, law enforcement agencies can monitor public spaces and digital environments in real time. When combined with predictive analytics, real-time monitoring systems can generate alerts regarding potential threats or suspicious activities, thereby facilitating rapid intervention. However, such capabilities also raise concerns regarding proportionality and the expansion of surveillance powers (Zuboff 2019).

### C. Public Security and National Security Rationales

In addition to operational efficiency, algorithmic policing is frequently justified on the basis of broader public security and national security objectives. Governments increasingly frame algorithmic technologies as essential tools for addressing complex security threats that transcend traditional crime categories. These include terrorism, organized crime, and

cybercrime, all of which are characterized by transnational networks, digital infrastructures, and adaptive operational strategies.

Terrorism prevention constitutes one of the most prominent justifications for algorithmic policing. Security agencies utilize data analytics and machine learning systems to identify potential radicalization patterns, monitor suspicious communications, and detect behavioral indicators associated with extremist activity. The underlying rationale is that early detection of risk signals can prevent terrorist incidents before they occur. However, research indicates that predictive systems in counterterrorism contexts may produce high rates of false positives, thereby raising serious concerns regarding civil liberties and discriminatory profiling (Lyon 2018).

Organized crime detection represents another key area where algorithmic tools are deployed. Criminal organizations often operate through complex transnational networks involving financial transactions, logistics chains, and digital communication platforms. Algorithmic systems can assist in mapping these networks by analyzing transactional data, communication patterns, and movement records. Such analytical capabilities are particularly valuable in financial crime investigations, money laundering detection, and drug trafficking cases. Nevertheless, the opacity of algorithmic models may limit accountability in high-stakes enforcement decisions.

Cybercrime detection further underscores the relevance of algorithmic policing in contemporary security environments. As criminal activities increasingly migrate to digital spaces, law enforcement agencies must rely on automated systems to detect cyber threats, identify malicious behavior, and respond to digital attacks. Machine learning algorithms can detect anomalies in network traffic, identify phishing attempts, and flag suspicious digital behavior in real time. Given the scale and complexity of cyber environments, algorithmic tools are often viewed as indispensable for maintaining digital security (Brenner 2010).

### D. The Efficiency Narrative

The widespread adoption of algorithmic policing is underpinned by a powerful efficiency narrative that emphasizes technological solutions to

complex social problems. Governments, policymakers, and law enforcement institutions often justify the deployment of algorithmic systems by highlighting their potential to enhance effectiveness, reduce costs, and improve public safety outcomes. This narrative reflects broader trends in digital governance, where data-driven decision-making is positioned as inherently superior to traditional bureaucratic processes (Yeung 2018).

However, a critical examination reveals that the efficiency narrative may obscure significant normative and structural concerns. One key issue is that algorithmic policing is frequently adopted without sufficient evaluation of its long-term social consequences. While short-term gains in crime detection or resource optimization may be observable, these benefits may come at the cost of increased surveillance, reduced transparency, and weakened procedural safeguards.

The adoption of algorithmic policing also reflects a broader tendency toward technological solutionism—the belief that complex social problems can be effectively resolved through technological innovation alone. Scholars of digital governance caution that this perspective often underestimates the political, legal, and ethical dimensions of technology deployment (Morozov 2013). In the context of criminal justice, technological solutionism may lead to overreliance on algorithmic outputs while neglecting the importance of human judgment, contextual understanding, and institutional accountability.

Moreover, the efficiency narrative tends to prioritize measurable outcomes, such as crime reduction rates or response times, while marginalizing less quantifiable but equally important values such as fairness, due process, and public trust. This creates a risk that criminal justice systems may gradually shift toward performance-driven models that emphasize statistical efficiency over constitutional protections. As a result, the legitimacy of law enforcement institutions may be undermined if efficiency gains are perceived to come at the expense of fundamental rights.

Ultimately, while algorithmic policing offers undeniable operational advantages, its justification on efficiency grounds alone is insufficient. A comprehensive evaluation must consider not only whether algorithmic systems improve performance metrics but also whether they align with

principles of justice, accountability, and human rights. These tensions form the basis for the subsequent analysis of legal safeguards and regulatory frameworks in the Indonesian context.

## DUE PROCESS RISKS IN ALGORITHMIC POLICING

### A. Algorithmic Bias and Discrimination

One of the most widely documented risks associated with algorithmic policing is the emergence and amplification of bias within automated decision-making systems. Although algorithmic tools are often presented as objective and neutral, their outputs are fundamentally shaped by the data on which they are trained, the design choices embedded within their architectures, and the institutional contexts in which they operate. As a result, algorithmic systems may reproduce or even intensify existing forms of discrimination within criminal justice practices (Barocas and Selbst 2016).

Historical bias constitutes the most foundational source of distortion in algorithmic policing systems. Law enforcement datasets typically reflect historical patterns of policing activity rather than actual distributions of criminal behavior. If certain communities have historically been subjected to more intensive policing, arrest rates in those areas will appear disproportionately high in official records. When such data are used to train predictive systems, algorithms may incorrectly interpret these patterns as indicators of higher criminal propensity, thereby perpetuating cycles of over-policing (Lum and Isaac 2016). This phenomenon demonstrates how algorithmic systems can encode institutional history into future decision-making processes.

Sampling bias further exacerbates these concerns. In many jurisdictions, crime data are incomplete, unevenly collected, or disproportionately focused on specific geographic or demographic groups. Consequently, algorithmic models may be trained on datasets that fail to represent the full complexity of criminal behavior across society. This leads to skewed predictions that disproportionately affect marginalized communities while underrepresenting crime in less-policed areas (O'Neil 2016).

Data quality problems also contribute significantly to algorithmic bias. Inaccurate, outdated, or inconsistently recorded data can distort model outputs and reduce the reliability of predictive systems. Law enforcement databases often contain errors, duplicates, or misclassified records, which may be systematically incorporated into algorithmic decision-making processes. When such flawed data are used at scale, even small inaccuracies can generate significant distortions in predictive outputs.

Feedback loops represent another critical mechanism through which algorithmic bias is reinforced. When predictive policing systems direct law enforcement attention toward specific neighborhoods, increased police presence often leads to higher recorded crime rates in those areas, regardless of actual changes in criminal activity. These inflated crime statistics are then reintroduced into algorithmic models, reinforcing the perception that such areas require further surveillance. This cyclical process creates self-reinforcing patterns of inequality that are difficult to disrupt (Ensign et al. 2018).

The consequences of algorithmic bias are both structural and deeply consequential for affected communities. One of the most significant outcomes is over-policing, where certain geographic areas or demographic groups are subjected to disproportionate levels of surveillance, stops, searches, and interventions. Over-policing not only increases the likelihood of criminal justice involvement but also contributes to broader social harms, including community distrust, psychological stress, and economic marginalization.

Socioeconomic bias is another important consequence. Algorithmic systems may indirectly encode socioeconomic indicators such as income level, employment status, or housing conditions as proxies for criminal risk. As a result, individuals from lower-income backgrounds may be disproportionately classified as high-risk, even in the absence of individualized evidence of wrongdoing (Eubanks 2018).

Geographic discrimination also emerges as a key concern. Predictive policing systems frequently concentrate surveillance in specific neighborhoods identified as “high-risk” zones. However, these designations may reflect historical policing intensity rather than actual crime prevalence.

Consequently, entire communities may become subject to persistent surveillance and intervention.

Minority targeting is perhaps the most widely criticized outcome of algorithmic bias in criminal justice systems. Empirical studies have demonstrated that algorithmic tools may disproportionately affect racial and ethnic minorities, particularly when training data reflect historical disparities in arrest and conviction rates. This raises serious concerns regarding equality before the law and non-discrimination principles (Benjamin 2019).

## B. The Black Box Problem

A central challenge in algorithmic policing is the so-called "black box" problem, which refers to the opacity and lack of interpretability associated with many machine learning systems. While algorithmic models may produce highly accurate predictions in certain contexts, the internal processes through which these outputs are generated are often difficult to understand, even for technical experts (Pasquale 2015).

Lack of transparency is a defining feature of many algorithmic systems used in policing. Law enforcement agencies frequently deploy proprietary software developed by private companies, which may not disclose the underlying algorithms, training data, or decision-making logic. This opacity makes it difficult for external stakeholders, including courts, defense attorneys, and affected individuals, to evaluate the validity or fairness of algorithmic outputs.

Proprietary systems further intensify transparency concerns. Commercial vendors often claim intellectual property protection over their algorithms, limiting public access to information about how these systems operate. As a result, critical decisions affecting liberty, surveillance, or criminal suspicion may be based on systems that cannot be independently scrutinized.

Explainability deficits also pose significant challenges. Many modern machine learning models, particularly deep learning systems, operate through complex mathematical structures that are not easily interpretable. Even when technical documentation is available, translating algorithmic

outputs into understandable explanations for legal purposes remains difficult. This creates a gap between technical functionality and legal accountability.

The due process implications of the black box problem are profound. One major concern is the inability of individuals to meaningfully challenge algorithmic decisions. If a person is classified as high-risk or subjected to increased surveillance based on an opaque algorithm, they may not be able to understand the basis of that classification, making it difficult to contest or refute the decision.

Weak judicial review is another consequence. Courts traditionally rely on evidence that can be examined, tested, and cross-examined. However, algorithmic outputs may not meet these standards of evidentiary transparency. Judges may lack the technical expertise or access to underlying data necessary to assess algorithmic reliability, thereby limiting effective judicial oversight.

Reduced accountability emerges as a broader systemic issue. When decision-making processes are opaque, it becomes difficult to assign responsibility for errors or harms. This undermines the foundational principle that state power must be subject to legal and institutional control (Citron and Pasquale 2014).

### C. Presumption of Innocence under Predictive Policing

Predictive policing systems challenge the traditional legal principle of the presumption of innocence by shifting the focus of criminal justice from completed acts to predicted behaviors. This transition introduces a form of anticipatory governance in which individuals may be treated as potential offenders based on statistical probabilities rather than actual conduct (Završnik 2021).

Predictive suspicion refers to the process by which individuals or groups are identified as risks before any criminal act has occurred. This represents a fundamental departure from conventional criminal law, which is based on evidence of past or present wrongdoing. In predictive systems, suspicion is generated algorithmically through correlations derived from data patterns,

rather than individualized evidence.

The emergence of pre-crime logic further intensifies this transformation. Pre-crime approaches prioritize prevention by intervening before crimes are committed. While this may appear beneficial from a security perspective, it raises significant legal concerns because it allows state action to be justified on the basis of potential future behavior rather than proven conduct.

Risk profiling is another mechanism through which presumption of innocence is undermined. Individuals may be assigned risk scores based on demographic, geographic, or behavioral data. These scores can influence police attention, surveillance intensity, and investigative decisions. However, such classifications may not reflect actual wrongdoing but rather statistical correlations.

The constitutional implications of these developments are significant. First, algorithmic policing introduces the possibility of suspicion without conduct, where individuals are subjected to state scrutiny without having engaged in any unlawful behavior. This undermines core principles of criminal law that require individualized suspicion grounded in evidence.

Second, it shifts the evidentiary foundation of criminal justice from probability versus evidence. Traditional legal systems prioritize evidence that demonstrates past conduct beyond reasonable doubt. Algorithmic systems, by contrast, rely on probabilistic predictions that estimate future risk. This raises concerns about whether statistical inference can legitimately substitute for legal proof in coercive state actions.

### D. Fair Trial Concerns

Algorithmic policing also raises serious concerns regarding fair trial rights. A fundamental issue relates to the reliability of algorithmic outputs. Although algorithmic systems may appear precise, their predictive accuracy is often context-dependent and subject to significant error rates. If algorithmic outputs are used in criminal proceedings without adequate validation, there is a risk that individuals may be subject to unjustified legal consequences.

Evidentiary problems arise when algorithmic outputs are introduced into judicial processes. Courts must determine whether algorithmic evidence

meets admissibility standards, including relevance, reliability, and probative value. However, the complexity of machine learning systems makes it difficult to assess these criteria adequately. Without transparency regarding model design and data sources, algorithmic evidence may lack sufficient evidentiary integrity.

The burden of proof may also be indirectly affected by algorithmic systems. When risk scores or predictive outputs are used in bail or sentencing decisions, individuals may effectively be required to disprove algorithmic assessments of dangerousness or recidivism risk. This inversion of evidentiary logic challenges fundamental principles of criminal justice.

Automated risk scores further complicate fair trial guarantees. These scores may influence judicial decision-making even when their methodological foundations are unclear. Judges may rely on algorithmic outputs as authoritative indicators of risk, potentially reducing independent judicial reasoning and increasing the influence of opaque technological systems.

### E. Privacy and Surveillance

Algorithmic policing is closely linked to expanding surveillance infrastructures that raise significant privacy concerns. Facial recognition technologies enable continuous identification and tracking of individuals in public spaces. While these systems may assist in criminal investigations, they also create conditions for pervasive biometric surveillance that can erode anonymity in public life (Garvie, Bedoya, and Frankle 2016).

Continuous monitoring systems further extend surveillance capacities by enabling real-time observation of individuals and environments. These systems may integrate data from CCTV networks, mobile devices, and online platforms, creating comprehensive surveillance ecosystems. Such practices raise questions regarding proportionality and necessity within democratic societies.

Mass data collection is another key concern. Law enforcement agencies increasingly gather vast amounts of personal data from multiple sources, often without clear limitations on scope or purpose. This raises the risk of

function creep, where data collected for one purpose is used for unrelated investigative or predictive activities.

Data retention practices also present legal challenges. Prolonged storage of personal data increases the risk of misuse, unauthorized access, and secondary use beyond original intentions. Without strict regulatory frameworks, data retention can become a mechanism for indefinite surveillance.

### F. Accountability Gaps

A final structural concern in algorithmic policing relates to accountability gaps involving multiple actors within the criminal justice ecosystem. Responsibility for algorithmic outcomes is often distributed across police agencies, technology vendors, and government institutions, making it difficult to assign clear legal accountability.

Police agencies may rely on algorithmic systems without fully understanding their technical limitations or embedded biases. Technology vendors, on the other hand, may claim that responsibility lies with end-users who deploy the systems. Government institutions may further diffuse responsibility through regulatory ambiguity. This fragmented structure creates a "responsibility gap" in which no single actor is fully accountable for harmful outcomes (Matthias 2004).

The absence of clear accountability mechanisms undermines fundamental principles of administrative and constitutional law. Without identifiable responsibility, affected individuals may face significant barriers in seeking remedies, challenging decisions, or obtaining compensation for harms caused by algorithmic systems. Strengthening accountability therefore becomes essential for ensuring that algorithmic policing operates within the boundaries of due process and the rule of law.

## ASSESSING INDONESIAN LEGAL FRAMEWORKS

The rapid emergence of algorithmic policing practices in Indonesia raises fundamental questions regarding the adequacy of existing legal frameworks

in safeguarding constitutional rights, particularly due process guarantees. While Indonesia possesses a relatively comprehensive constitutional and statutory structure governing criminal justice, data protection, and electronic systems, these instruments were not designed to regulate automated decision-making in law enforcement contexts. As a result, significant normative and regulatory gaps persist. This section evaluates the extent to which Indonesian law can accommodate algorithmic policing by examining constitutional safeguards, criminal procedure law, police regulations, data protection rules, and electronic transaction legislation.

## A. Constitutional Safeguards

The Indonesian Constitution (UUD 1945) provides the foundational legal framework for the protection of human rights and the limitation of state power. Several constitutional provisions are particularly relevant to algorithmic policing and due process protections.

Article 28D(1) guarantees the right to recognition, guarantees of protection, and certainty of law that is just, as well as equal treatment before the law. This provision is central to the principle of legal certainty (*rechtszekerheid*), which requires that state actions be based on clear, predictable, and accessible legal norms. In the context of algorithmic policing, legal certainty becomes problematic when decisions are derived from opaque computational systems that lack clear regulatory grounding or interpretability (Asshiddiqie 2006). If individuals cannot understand the basis of algorithmic classifications or predictions, the constitutional requirement of legal certainty may be undermined.

Article 28G(1) provides protection of personal security, family, honor, dignity, and property, as well as the right to feel secure and protected from threats of fear. This provision is increasingly relevant in the digital age, where surveillance technologies and predictive systems may generate indirect forms of harm, including psychological pressure and anticipatory policing effects. Algorithmic surveillance systems that continuously monitor individuals or classify them as potential risks may interfere with the constitutional right to personal security by creating an environment of persistent state observation.

Article 28I(2) guarantees freedom from discriminatory treatment and protection against such discrimination. This provision is particularly significant in relation to algorithmic bias, as discussed in previous sections. If algorithmic policing systems disproportionately target specific demographic groups based on biased training data or proxy variables, such outcomes may constitute indirect discrimination under constitutional law. The challenge lies in establishing evidentiary standards capable of demonstrating algorithmic discrimination in complex technical systems.

Overall, while the Indonesian Constitution provides strong normative protections for legal certainty, privacy, and equality, it does not explicitly address algorithmic governance or automated decision-making. This creates interpretive challenges when applying constitutional principles to emerging technologies.

## B. Criminal Procedure Law

Indonesia's Criminal Procedure Code (*Kitab Undang-Undang Hukum Acara Pidana* / KUHAP) forms the backbone of procedural safeguards in criminal justice. It regulates investigation processes, prosecutorial authority, and judicial proceedings. However, KUHAP was enacted in a pre-digital era and therefore does not explicitly regulate algorithmic tools in criminal investigations or decision-making processes.

Regarding investigation powers, KUHAP grants police broad authority to conduct investigations, collect evidence, and undertake coercive measures under legal supervision. In practice, algorithmic systems may increasingly assist or influence investigative decision-making, including suspect identification and prioritization. However, KUHAP does not provide guidance on whether algorithmic outputs can be considered valid investigative grounds or how such outputs should be evaluated in terms of reliability and legality.

The rights of suspects are a core component of KUHAP, including the right to legal counsel, the right to be informed of charges, and the right to challenge evidence. In algorithmic policing contexts, these rights face new challenges. If suspect identification is based on predictive analytics or risk

scoring, individuals may not be informed of the algorithmic basis of suspicion, thereby limiting their ability to challenge the grounds of investigation.

Evidentiary requirements under KUHAP emphasize the importance of lawful, relevant, and credible evidence in criminal proceedings. However, algorithmic outputs do not easily fit within traditional evidentiary categories. It remains unclear whether predictive risk scores or machine-generated classifications can be admitted as evidence, and if so, under what standards of reliability and admissibility. The absence of clear evidentiary rules for algorithmic outputs creates legal uncertainty and risks undermining procedural fairness.

### C. Police Law

The Indonesian Police Law (Law No. 2 of 2002) regulates the structure, functions, and authority of the Indonesian National Police (*Kepolisian Negara Republik Indonesia*). The law grants police broad discretion in maintaining public order, enforcing the law, and protecting society. However, it does not explicitly regulate the use of algorithmic systems in policing activities.

In terms of scope of authority, police institutions are empowered to conduct preventive and repressive measures in the context of law enforcement. Algorithmic policing technologies may be integrated into these functions to enhance efficiency and operational effectiveness. Nevertheless, the absence of specific legal provisions governing algorithmic decision-making creates ambiguity regarding the limits of technological use in police operations.

Institutional accountability is another critical issue. The Police Law establishes internal and external oversight mechanisms, including professional ethics divisions and supervisory institutions. However, these mechanisms are not designed to evaluate algorithmic systems or assess technical decision-making processes. As a result, accountability structures may be insufficient to address harms arising from automated or semi-automated policing decisions.

The lack of algorithm-specific accountability mechanisms raises concerns

regarding the delegation of discretionary power to technological systems without adequate legal safeguards. This situation risks shifting decision-making authority from human officers to opaque computational systems that are not directly accountable under existing institutional frameworks.

## D. Personal Data Protection Law

Indonesia's Personal Data Protection Law (Law No. 27 of 2022) represents a significant advancement in regulating digital data governance. The law establishes standards for data processing, defines the rights of data subjects, and imposes obligations on data controllers and processors.

Data processing standards under the PDP Law require that personal data be processed lawfully, transparently, and for specified purposes. These principles are highly relevant to algorithmic policing, where large volumes of personal data are collected and analyzed for predictive purposes. However, the law does not explicitly regulate the use of personal data for predictive law enforcement analytics, leaving interpretive gaps regarding secondary use and automated profiling.

The rights of data subjects include access, correction, deletion, and objection to data processing. These rights are essential for ensuring individual control over personal data. However, in algorithmic policing contexts, exercising these rights may be difficult due to the complexity of data ecosystems and the opacity of algorithmic systems. Individuals may not be aware that their data has been used in predictive models, thereby limiting the practical effectiveness of these rights.

While the PDP Law provides a strong foundation for data protection, it does not specifically address algorithmic decision-making, automated profiling, or predictive policing systems. As such, additional regulatory instruments may be required to bridge the gap between data protection and due process rights.

## E. Electronic Information and Transactions Law

The Electronic Information and Transactions Law (Law No. 11 of 2008, as amended) regulates electronic systems, digital transactions, and the

admissibility of electronic evidence in Indonesia. This law plays a crucial role in shaping the legal environment for digital governance and technology-driven law enforcement.

Regarding digital evidence, the law recognizes electronic information and documents as valid legal evidence under certain conditions. This provision is highly relevant to algorithmic policing, as digital records and algorithmic outputs may be used in investigative and judicial processes. However, the law does not specify standards for evaluating the reliability or transparency of algorithmic evidence.

The regulation of electronic systems primarily focuses on administrative compliance, security requirements, and system governance. While this provides a general framework for digital infrastructure, it does not address the specific characteristics of artificial intelligence systems, such as machine learning models or predictive analytics tools. Consequently, the legal status of algorithmic outputs remains ambiguous within Indonesia's evidentiary system. Courts may accept digital evidence in general, but there is no explicit guidance on how to assess algorithmic validity, error rates, or bias risks.

## F. Regulatory Deficiencies

Despite the existence of multiple legal instruments governing constitutional rights, criminal procedure, policing, data protection, and electronic systems, Indonesia currently lacks a comprehensive regulatory framework addressing algorithmic policing. Several critical deficiencies can be identified. *First*, there is no legal definition of algorithmic policing within Indonesian law. This absence creates conceptual ambiguity regarding the scope, boundaries, and legal status of algorithm-driven law enforcement practices. Without a clear definition, regulatory oversight becomes fragmented and inconsistent.

Second, there are no explicit transparency requirements for algorithmic systems used in policing. Law enforcement agencies are not legally obligated to disclose the use of predictive tools, their underlying methodologies, or their decision-making criteria. This lack of transparency undermines accountability and due process protections.

Third, Indonesian law does not establish explainability standards for algorithmic systems. Individuals affected by algorithmic decisions have no guaranteed right to receive meaningful explanations regarding how decisions were made. This gap is particularly problematic in contexts involving deprivation of liberty or increased surveillance.

Fourth, there are no mandatory algorithmic audit mechanisms. Independent auditing of algorithmic systems is essential to detect bias, ensure accuracy, and evaluate compliance with legal standards. The absence of such mechanisms increases the risk of unchecked algorithmic errors and systemic discrimination.

Finally, there is no requirement for human rights impact assessments in the deployment of algorithmic policing technologies. Without such assessments, the potential consequences of algorithmic systems on fundamental rights may not be systematically evaluated prior to implementation.

Taken together, these regulatory deficiencies demonstrate that Indonesia's current legal framework is not yet adequately equipped to govern algorithmic policing. This gap highlights the urgent need for a rights-based regulatory approach that integrates constitutional protections, procedural safeguards, and technological accountability mechanisms.

## COMPARATIVE PERSPECTIVES AND LESSONS FOR INDONESIA

The development of algorithmic policing is a global phenomenon shaped by diverse legal, institutional, and political responses. Comparative analysis is essential to understanding how different jurisdictions regulate algorithmic decision-making in criminal justice and how such experiences can inform regulatory development in Indonesia. This section examines approaches in the United States, the European Union, the United Kingdom, Canada, and emerging international frameworks, before distilling key lessons for Indonesia.

### A. United States

The United States represents one of the earliest adopters of algorithmic tools in policing and criminal justice. Systems such as COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) have been widely used in risk assessment for sentencing, bail decisions, and parole evaluations. COMPAS generates risk scores intended to predict recidivism, thereby assisting judicial and correctional decision-making (Angwin et al. 2016).

However, COMPAS has also become emblematic of the risks associated with algorithmic governance. Empirical investigations have raised concerns regarding racial bias, with evidence suggesting that the system may disproportionately classify minority defendants as higher risk compared to white defendants with similar profiles (Angwin et al. 2016). These findings have fueled extensive debate about fairness, accountability, and transparency in algorithmic decision-making.

Predictive policing programs in the United States, including systems deployed in cities such as Los Angeles and Chicago, have similarly faced scrutiny. These systems rely on historical crime data to generate predictions about future criminal activity. Critics argue that such systems reproduce existing patterns of over-policing, particularly in marginalized communities (Ferguson 2017). Moreover, the use of opaque proprietary software has complicated efforts to evaluate their legality and fairness.

Constitutional challenges have emerged primarily under due process and equal protection doctrines. Courts have struggled to determine whether algorithmic risk assessments meet procedural fairness requirements, particularly when defendants are unable to interrogate the underlying methodology of predictive tools. The lack of transparency has raised concerns about "black box justice," where individuals are subject to algorithmic determinations without meaningful explanation or review.

### B. European Union

The European Union has adopted a more precautionary and rights-based approach to algorithmic governance. The EU Artificial Intelligence Act represents the world's first comprehensive attempt to regulate AI systems

through a risk-based legal framework. Under this regime, AI applications used in law enforcement are classified as high-risk systems, subject to strict requirements regarding transparency, accuracy, documentation, and human oversight (Veale and Borgesius 2021).

The General Data Protection Regulation (GDPR) further strengthens individual rights in relation to automated decision-making. Article 22 of the GDPR provides individuals with the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. It also establishes rights to obtain meaningful information about the logic involved in automated processing. This provision directly addresses concerns related to algorithmic opacity and due process violations (Wachter, Mittelstadt, and Floridi 2017). Fundamental rights protection is central to the EU regulatory model. Algorithmic systems must comply with the Charter of Fundamental Rights of the European Union, which guarantees rights to privacy, data protection, equality, and effective judicial remedy. This constitutionalized approach ensures that technological innovation is systematically aligned with human rights standards.

### C. United Kingdom

The United Kingdom has been a significant testing ground for facial recognition technologies in public policing. The deployment of live facial recognition systems by police forces has generated substantial legal controversy. Courts have examined whether such deployments comply with privacy rights under the European Convention on Human Rights, particularly Article 8, which protects the right to private life.

Judicial responses have been mixed but increasingly cautious. In *R (Bridges) v South Wales Police*, the Court of Appeal held that the use of facial recognition technology lacked sufficient legal clarity and safeguards, rendering its deployment unlawful in that instance. The judgment emphasized the need for clear legal frameworks, proportionality assessments, and safeguards against arbitrary surveillance.

These developments illustrate the judiciary's role in scrutinizing algorithmic policing practices. While UK courts have not rejected facial

recognition technology outright, they have insisted on stricter governance standards and clearer statutory regulation to ensure compatibility with fundamental rights.

### D. Canada

Canada has developed one of the most structured governmental approaches to algorithmic governance through its Algorithmic Impact Assessment (AIA) framework. The AIA is a mandatory tool used by federal agencies to evaluate the potential risks and impacts of automated decision-making systems prior to deployment.

The assessment categorizes AI systems based on risk levels and requires mitigation strategies proportionate to the severity of potential impacts. High-risk systems must comply with enhanced transparency, auditing, and human oversight requirements. This preventive governance model reflects a shift toward ex ante regulation of algorithmic systems (Government of Canada 2020). Canada's broader AI governance strategy emphasizes ethical principles, public accountability, and human rights protection. The framework also encourages documentation, public reporting, and continuous monitoring of algorithmic systems in government use.

### E. Emerging International Standards

At the international level, several normative frameworks have emerged to guide the ethical and legal development of artificial intelligence. The OECD AI Principles establish five core values: inclusive growth, human-centered values, transparency, robustness, and accountability. These principles provide a soft law framework for AI governance adopted by multiple states.

UNESCO's Recommendation on the Ethics of Artificial Intelligence similarly emphasizes human rights, proportionality, fairness, and sustainability. It calls for impact assessments, governance mechanisms, and international cooperation to ensure that AI systems respect human dignity and fundamental freedoms. Human rights-based AI governance has become an increasingly dominant paradigm in international policy discourse. This approach asserts that AI systems must be designed, deployed, and regulated

in accordance with international human rights law, ensuring that technological innovation does not undermine fundamental legal protections (Yeung 2018).

### F. Lessons for Indonesia

The comparative analysis reveals several key lessons for Indonesia in developing regulatory frameworks for algorithmic policing. First, transparency is essential. Jurisdictions such as the EU and Canada demonstrate the importance of requiring disclosure of algorithmic systems, including their purposes, limitations, and operational logic. Without transparency, accountability mechanisms remain ineffective. Second, explainability must be institutionalized. Individuals affected by algorithmic decisions should have access to meaningful explanations that allow them to understand and challenge outcomes. The GDPR model provides a useful reference point for embedding explainability into legal frameworks.

Third, human oversight is indispensable. Across jurisdictions, there is growing consensus that high-impact algorithmic decisions must not be fully automated. Human-in-the-loop mechanisms ensure that final decisions remain subject to human judgment and legal responsibility. Fourth, independent accountability mechanisms are critical. The Canadian AIA model illustrates the importance of ex ante risk assessments and ongoing auditing processes. Independent oversight bodies can help ensure compliance with legal and ethical standards.

Collectively, these lessons suggest that Indonesia must move toward a comprehensive, rights-based regulatory framework that integrates transparency, explainability, human oversight, and independent accountability to govern algorithmic policing effectively.

## TOWARDS A RIGHTS-BASED REGULATORY FRAMEWORK FOR ALGORITHMIC POLICING IN INDONESIA

Building on the comparative insights and normative analysis, this section proposes a rights-based regulatory framework for algorithmic policing in

Indonesia. The framework is designed to balance technological efficiency with constitutional protections, particularly due process rights, equality, and human dignity. It emphasizes a multi-layered governance structure encompassing preventive, operational, and judicial accountability.

The proposed framework is grounded in four foundational principles: the rule of law, due process, human rights protection, and democratic accountability. The rule of law requires that all algorithmic systems used in policing operate within clear, accessible, and predictable legal frameworks. This includes statutory authorization for the use of AI systems and explicit limitations on their scope of application. Without a clear legal basis, algorithmic policing risks undermining legality and legal certainty.

Due process constitutes the central safeguard against arbitrary state action. Algorithmic systems must not replace procedural guarantees but rather operate within them. Individuals affected by algorithmic decisions must retain rights to information, explanation, and challenge. Human rights protection ensures that algorithmic policing is consistent with constitutional guarantees and international human rights obligations, particularly regarding privacy, equality, and fair trial rights. Democratic accountability requires that algorithmic systems remain subject to public oversight, legislative scrutiny, and institutional checks. Technological governance must not become insulated from democratic control.

Preventive accountability mechanisms aim to regulate algorithmic systems before they are deployed. Mandatory Algorithmic Impact Assessments (AIA) should be required for all high-risk policing technologies. These assessments evaluate potential impacts on rights, fairness, and legality prior to implementation. Human Rights Impact Assessments should complement technical evaluations by focusing specifically on constitutional and international human rights implications.

Bias testing must be conducted to identify discriminatory outcomes in training data and model outputs. Such testing should be continuous rather than one-time, given the dynamic nature of algorithmic systems. Certification mechanisms should be introduced to ensure that only audited and approved algorithmic systems can be used in law enforcement contexts. Certification

bodies should be independent from both government and vendors.

Operational accountability governs the use of algorithmic systems during their active deployment. Transparency obligations require law enforcement agencies to disclose the existence and general functioning of algorithmic systems used in policing activities. This includes public reporting on system purpose and scope. Explainability requirements ensure that individuals affected by algorithmic decisions can obtain meaningful explanations regarding how outcomes were generated.

Human-in-the-loop controls mandate that final decision-making authority remains with human officers rather than fully automated systems, particularly in high-impact contexts such as arrest or surveillance escalation. Documentation standards require comprehensive record-keeping of algorithmic inputs, outputs, and decision-making processes to enable later review and audit.

Judicial accountability ensures that algorithmic systems remain subject to independent legal scrutiny. Judicial review of algorithmic outputs should be explicitly recognized, allowing courts to assess the legality, reliability, and proportionality of algorithmic evidence. Admissibility standards must be developed to regulate when and how algorithmic outputs can be used in criminal proceedings. These standards should include requirements for validation, transparency, and error rate disclosure. Contestability rights guarantee that individuals can challenge algorithmic decisions through administrative or judicial mechanisms. Independent audits should be accessible to courts to support evaluation of algorithmic systems during litigation.

The proposed governance model consists of three interconnected layers. Layer 1: Preventive Governance focuses on pre-deployment assessment, certification, and risk evaluation of algorithmic systems. Layer 2: Operational Governance regulates the ongoing use of algorithmic tools through transparency, explainability, and human oversight requirements. Layer 3: Judicial Governance ensures post-deployment accountability through judicial review, admissibility rules, and legal remedies. Together, these layers form a comprehensive regulatory architecture designed to ensure that algorithmic

policing remains consistent with constitutional and human rights standards.

To operationalize the proposed framework, several legislative reforms are necessary. First, amendments to police regulations should explicitly define and regulate the use of algorithmic systems in law enforcement activities, including limits on predictive policing and automated surveillance. Second, Indonesia requires an AI-specific criminal justice regulation that addresses algorithmic decision-making, transparency obligations, bias mitigation, and accountability mechanisms. Third, a national AI governance framework should be established to harmonize sectoral regulations and ensure consistency across governmental institutions. This framework should align with constitutional principles and international human rights standards. Through these reforms, Indonesia can develop a balanced regulatory approach that harnesses the benefits of algorithmic policing while safeguarding due process rights and democratic accountability.

## CONCLUSION

In conclusion, this article demonstrates that while algorithmic policing offers significant operational advantages in terms of efficiency, predictive capacity, and resource optimization, it simultaneously generates profound challenges for due process rights within criminal justice systems. The analysis shows that issues such as algorithmic bias, opacity of decision-making systems, erosion of the presumption of innocence, weakened fair trial guarantees, expanded surveillance practices, and fragmented accountability structures collectively threaten core constitutional principles. Although comparative jurisdictions such as the European Union, Canada, and the United States have begun to develop regulatory responses, Indonesia's current legal framework remains insufficiently equipped to govern algorithmic decision-making in policing. Existing constitutional provisions, criminal procedure rules, and data protection laws provide important but indirect safeguards that do not specifically address the unique risks posed by AI-driven law enforcement. Therefore, this study concludes that Indonesia requires a comprehensive rights-based regulatory framework that integrates preventive impact

assessments, operational transparency, human oversight, and robust judicial review mechanisms. Such an approach is essential to ensure that technological innovation in policing does not come at the expense of legality, accountability, and fundamental human rights, but instead operates within a constitutionally grounded system that balances efficiency with fairness in the administration of criminal justice.

## ACKNOWLEDGMENTS

None.

## FUNDING INFORMATION

None.

## CONFLICTING INTEREST AND ORGINALITY STATEMENT

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

## GENERATIVE AI STATEMENT

None.

## REFERENCES

Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. "Machine Bias." *ProPublica*.

Ashworth, Andrew, and Mike Redmayne. 2010. *The Criminal Process*. 4th ed. Oxford: Oxford University Press.

Asshiddiqie, Jimly. 2006. *Pengantar Ilmu Hukum Tata Negara*. Jakarta: Sekretariat Jenderal MK RI.

Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparate Impact." *California Law Review* 104 (3): 671–732.

Benjamin, Ruha. 2019. *Race After Technology*. Cambridge: Polity Press.

Berk, Richard. 2017. *Artificial Intelligence, Predictive Policing, and Risk*

*Assessment for Law Enforcement*. New York: Springer.

Braga, Anthony A., Andrew V. Papachristos, and David M. Hureau. 2019. "The Effects of Hot Spots Policing on Crime." *Annals of the American Academy of Political and Social Science* 578 (1): 104–125.

Brayne, Sarah. 2021. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger.

Citron, Danielle Keats, and Frank Pasquale. 2014. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89 (1): 1–33.

Crawford, Kate. 2021. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press.

Dicey, A. V. 1982. *Introduction to the Study of the Law of the Constitution*. Indianapolis: Liberty Fund.

Ensign, Danielle, et al. 2018. "Runaway Feedback Loops in Predictive Policing." *Conference on Fairness, Accountability, and Transparency (FAT*) Proceedings*.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. 2016. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Washington, DC: Georgetown Law Center on Privacy & Technology.

Government of Canada. 2020. *Directive on Automated Decision-Making*.

Lum, Kristian, and William Isaac. 2016. "To Predict and Serve?" *Significance* 13 (5): 14–19.

Lyon, David. 2018. *The Culture of Surveillance*. Cambridge: Polity Press.

Matthias, Andreas. 2004. "The Responsibility Gap." *Ethics and Information Technology* 6 (3): 175–183.

McGregor, Lorna, Daragh Murray, and Vivian Ng. 2019. "International Human Rights Law as a Framework for Algorithmic Accountability."

*International and Comparative Law Quarterly* 68 (2): 309–343.
Mittelstadt, Brent D., Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. 2016. "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society* 3 (2): 1–21.
Morozov, Evgeny. 2013. *To Save Everything, Click Here*. New York: PublicAffairs.
O'Neil, Cathy. 2016. *Weapons of Math Destruction*. New York: Crown.
Pasquale, Frank. 2015. *The Black Box Society*. Cambridge: Harvard University Press.
Perry, Walter L., Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood. 2013. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation.
Ratcliffe, Jerry H. 2016. *Intelligence-Led Policing*. 2nd ed. London: Routledge.
Republic of Indonesia. Law No. 11 of 2008 concerning Electronic Information and Transactions (as amended).
Republic of Indonesia. Law No. 2 of 2002 concerning the Indonesian National Police.
Republic of Indonesia. Law No. 27 of 2022 concerning Personal Data Protection.
Richards, Neil M., and Jonathan H. King. 2014. "Big Data Ethics." *Wake Forest Law Review* 49 (2): 393–432.
Russell, Stuart, and Peter Norvig. 2021. *Artificial Intelligence: A Modern Approach*. 4th ed. Harlow: Pearson.
Selbst, Andrew D. 2017. "Disparate Impact in Big Data Policing." *Georgia Law Review* 52 (1): 109–195.
Tyler, Tom R. 2006. *Why People Obey the Law*. Princeton: Princeton University Press.
Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. "Demystifying the Draft EU Artificial Intelligence Act." *Computer Law Review International* 22 (4): 97–112.
Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. 2017. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR." *International Data Privacy Law* 7 (2): 76–99.

Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505–523.

Završnik, Aleš. 2021. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." *ERA Forum* 20 (4): 567–583.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

This page is intetionally left blank