

Legal and ethical implications of algorithmic decision-making systems: A critical analysis of challenges and regulatory solutions

I Nyoman Agus Prabawa, Eko Soponyono, Sri Kusriyah, Anis Mashdurohatun, Sri Endah Wahyuningsih

Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia

Abstract

This study critically examines the legal and ethical implications of algorithmic decision-making systems across various sectors, with particular focus on transparency, accountability, and discrimination concerns. The research employs a qualitative case study methodology to analyze how algorithms influence legal decision-making processes and the regulatory challenges that emerge in this rapidly evolving technological landscape. Findings reveal that algorithmic systems present significant challenges related to privacy protection, discrimination potential, accountability mechanisms, and transparency requirements. The study identifies that current regulatory frameworks, particularly in Indonesia, lack specificity regarding algorithmic governance, creating legal uncertainty and implementation gaps. We propose a three-pronged approach to address these challenges: (1) enhancing algorithmic transparency through mandatory disclosure requirements and independent auditing mechanisms; (2) implementing comprehensive social and ethical impact assessments throughout the algorithm development lifecycle; and (3) developing adaptive regulatory frameworks that respond to technological advancements while protecting fundamental rights. This research contributes to the emerging discourse on algorithmic governance by highlighting the need for collaborative approaches between government, industry, academia, and civil society to develop effective regulatory solutions that balance technological innovation with legal protections and ethical considerations.

Keywords: Algorithmic decision-making, legal implications, transparency, accountability, privacy, ethical governance

Introduction

In the contemporary digital landscape, algorithmic decision-making systems have become increasingly prevalent across diverse sectors, including finance, healthcare, education, and legal systems. Algorithms—defined as structured sequences of instructions designed to solve problems or perform specific tasks—now play a pivotal role in processes ranging from credit scoring and insurance underwriting to criminal sentencing and resource allocation. This algorithmic turn promises enhanced efficiency, consistency, and objectivity in decision-making processes that were previously dominated by human judgment^[1].

Algorithms represent a systematic approach to problem-solving through clearly defined steps or instructions. In computational contexts, they function as logical frameworks that enable computers to process data, solve complex problems, and generate decisions based on predefined parameters. While distinct from artificial intelligence (AI), algorithms frequently serve as foundational components of AI systems, particularly in machine learning applications where they organize learning processes and determine predictive outcomes based on identified patterns.

The integration of algorithmic systems into decision-making processes has expanded dramatically in recent years. In financial markets, algorithms analyze real-time data to execute trading decisions based on price movements and market indicators. Banking institutions employ algorithms to assess credit applications by analyzing financial histories, income levels, and asset portfolios to determine risk profiles. In human resources, algorithmic systems evaluate candidate qualifications against job criteria, often using AI to match suitable candidates to specific positions.

Perhaps most significantly, judicial systems increasingly incorporate algorithmic tools to support legal decision-making. These applications include sentencing

recommendations based on offender profiles and legal guidelines, probation supervision systems that monitor compliance with court-mandated conditions, and jury selection processes that identify suitable panelists based on demographic and behavioral characteristics. While these implementations enhance procedural efficiency and decision consistency, they simultaneously raise profound questions about fairness, transparency, and accountability in legal contexts^[2].

Despite their operational benefits, algorithmic decision-making systems present substantial challenges that demand critical examination. A primary concern involves fairness in algorithmic outcomes. Algorithms trained on historical data often replicate and potentially amplify existing societal biases and inequalities. In judicial contexts, this can manifest as discriminatory sentencing patterns that disproportionately impact marginalized communities, thereby perpetuating systemic injustices rather than mitigating them.

The opacity of algorithmic systems presents another significant challenge. Many contemporary algorithms, particularly those employing advanced machine learning techniques, function as "black boxes" whose decision-making processes remain inscrutable even to their developers. This lack of transparency undermines the ability of affected individuals to contest potentially unfair or discriminatory outcomes and diminishes the accountability of entities deploying such systems.

The potential for algorithmic systems to produce decisions that fail to account for individual circumstances and rights represents a further concern. Influential research revealed that facial recognition algorithms developed by leading technology companies demonstrated significantly lower accuracy rates for dark-skinned individuals and women compared to white males, illustrating how algorithmic bias

can manifest as indirect discrimination against specific demographic groups^[3].

These challenges necessitate robust legal frameworks governing algorithmic accountability. Organizations deploying algorithmic decision-making systems bear responsibility for ensuring compliance with relevant regulations, including data protection laws, anti-discrimination provisions, and human rights standards. They must further guarantee that their algorithmic systems do not adversely impact specific individuals or groups through privacy violations or discriminatory outcomes.

Regulatory responses to algorithmic governance have emerged in various jurisdictions. The European Union's General Data Protection Regulation (GDPR) establishes comprehensive provisions regarding personal data processing and individual rights, while the United States Federal Trade Commission enforces regulations concerning unfair business practices, including those involving algorithmic systems. However, significant regulatory gaps persist, particularly regarding algorithmic transparency, accountability mechanisms, and remediation processes for algorithmic harms^[4].

The complexity of algorithmic governance presents substantial enforcement challenges. Technical complexity renders many algorithms incomprehensible to individuals lacking specialized expertise, complicating determinations of legal compliance. Limited transparency in algorithmic decision-making processes further impedes regulatory oversight, while existing legal frameworks often inadequately address the specific challenges posed by algorithmic systems (Diakopoulos, 2016).

This research investigates the legal implications of algorithmic decision-making systems, with particular attention to the challenges they present and potential regulatory solutions. We examine critical issues including transparency requirements, accountability mechanisms, and discrimination potential, while considering how technological tools can strengthen rather than undermine fundamental principles of justice. By identifying existing challenges and proposing viable regulatory approaches, this study aims to contribute meaningfully to the development of legal frameworks governing algorithmic systems in the digital age^[5].

Research Methodology

This study employs a qualitative research design combining case study analysis with comprehensive literature review to examine the legal implications of algorithmic decision-making systems. The case study approach enables in-depth investigation of specific instances where algorithmic systems have been deployed in legal and quasi-legal decision-making contexts, providing concrete examples of the challenges and implications that emerge from such applications.

Case Study Selection and Analysis

The research identifies and analyzes representative cases involving algorithmic decision-making systems across multiple sectors, with particular focus on financial services, public administration, and judicial processes. Case selection criteria included: (1) implementation of algorithmic systems in consequential decision-making processes; (2) documented outcomes or impacts affecting individuals or groups; and (3) sufficient available information to permit

meaningful analysis. Selected cases from the Indonesian context include algorithmic credit scoring systems implemented by Bank Jombang, Bank Rakyat Indonesia's BRIBRAIN system, and Akulaku's machine learning risk assessment platform. Additionally, we examine data breach incidents involving algorithmic systems at Tokopedia, Bank Indonesia, BPJS Employment, and Bank Syariah Indonesia to analyze privacy and security implications.

Each case was systematically analyzed to identify: (a) the specific algorithmic application and its decision-making function; (b) legal and ethical issues arising from its implementation; (c) regulatory responses or gaps; and (d) outcomes for affected individuals or groups. This analytical framework enables identification of patterns across cases while maintaining attention to context-specific factors.

Literature Review

The study incorporates a structured literature review examining scholarly research on algorithmic decision-making systems and their legal implications. The literature review methodology involved systematic identification, selection, and analysis of relevant academic publications, with particular attention to works addressing algorithmic transparency, accountability, fairness, and regulatory approaches. Key works included in the analysis are:

1. Disparate impacts in big data analytics, which provides critical insights into how algorithmic systems can produce discriminatory outcomes despite apparent neutrality.
2. Algorithmic accountability, which offers conceptual tools for understanding transparency requirements and accountability mechanisms in algorithmic governance.
3. European Union regulations concerning algorithmic decision-making, with particular attention to transparency provisions and explanation rights.
4. Algorithmic opacity in financial and information systems, which highlights the challenges posed by "black box" algorithms for regulatory oversight and individual rights.
5. Examining efficiency and fairness in automated decision-making, which provides a structured approach to evaluating algorithmic systems.
6. Opacity in machine learning algorithms, which distinguishes between different forms of algorithmic inscrutability and their implications for governance.

The literature review enabled identification of theoretical frameworks, empirical findings, and regulatory approaches relevant to understanding the legal implications of algorithmic decision-making systems. By synthesizing insights from diverse scholarly perspectives, the review establishes a conceptual foundation for analyzing the case studies and developing regulatory recommendations.

Data Collection and Analysis

Data collection involved gathering documentation related to the selected case studies, including company reports, regulatory filings, media coverage, and, where available, technical documentation of algorithmic systems.

Additionally, we collected and analyzed relevant legal and regulatory texts, including Indonesia's Law No. 27 of 2022 on Personal Data Protection, to assess the current regulatory landscape governing algorithmic systems.

Data analysis employed qualitative content analysis techniques to identify key themes, patterns, and relationships across the collected materials. This analytical approach enabled systematic examination of how algorithmic decision-making systems function in practice, the legal challenges they present, and the adequacy of existing regulatory frameworks to address these challenges.

Limitations

This research acknowledges several methodological limitations. First, the opacity of many algorithmic systems limits access to detailed information about their functioning, potentially constraining the depth of analysis. Second, the rapidly evolving nature of algorithmic technologies means that specific applications may change during the research period. Third, the focus on Indonesian cases may limit generalizability to other jurisdictions with different legal frameworks and technological contexts. Despite these limitations, the research design provides a robust foundation for examining the legal implications of algorithmic decision-making systems and developing informed regulatory recommendations.

Results and Discussion

Regulatory Challenges in Algorithmic Decision-Making Systems in Indonesia

The current regulatory framework in Indonesia regarding algorithmic decision-making systems presents significant limitations that require careful consideration. Existing regulations lack specificity regarding the implementation of AI algorithms across various sectors such as finance, healthcare, and industry. This regulatory gap leaves organizations without clear guidelines for effective and safe algorithmic deployment, creating legal uncertainty in an increasingly algorithm-dependent landscape^[6].

A primary concern involves privacy protection and data security. While Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) addresses personal data protection through Article 26, this legislation is insufficiently comprehensive to manage the complex privacy implications of algorithmic systems. Recognizing this deficiency, the Indonesian government has developed Law No. 27 of 2022 on Personal Data Protection, which aims to align with international standards such as the European Union's General Data Protection Regulation (GDPR). However, this law still requires further refinement to specifically address algorithmic decision-making contexts^[7].

The determination of legal responsibility for algorithm-generated decisions represents another significant regulatory challenge. Current provisions fail to clearly establish accountability when algorithms cause harm or loss, creating legal uncertainty that complicates enforcement efforts. This ambiguity is particularly problematic given the "black box" nature of many algorithmic systems, where decision-making processes remain opaque even to system developers.

The potential for algorithmic bias and discrimination presents a significant regulatory challenge. As noted by Barocas and Selbst (2016), algorithms trained on historical data often replicate and potentially amplify existing societal

biases and inequalities. In the Indonesian context, where diversity spans ethnicity, religion, socioeconomic status, and geographic location, ensuring algorithmic fairness becomes particularly complex.

Current Indonesian regulations do not adequately address the potential for algorithmic discrimination, leaving vulnerable populations at risk. The absence of specific provisions requiring algorithmic impact assessments or fairness audits means that discriminatory outcomes may go undetected and unremedied. This regulatory gap is especially concerning in high-stakes domains such as financial services, where algorithmic credit scoring can determine economic opportunities and financial inclusion^[8].

Case Studies of Algorithmic Implementation and Data Breaches in Indonesia

The banking sector in Indonesia demonstrates widespread adoption of algorithmic decision-making systems. Bank Jombang pioneered the integration of AI for credit analysis among rural banks (BPR) in 2023, becoming the first to implement this technology for operational efficiency and credit decision-making. Similarly, Bank Rakyat Indonesia (BRI) developed BRIBRAIN ("BRI Digital Brain Center"), combining AI and analytical capabilities to enhance customer interactions, anti-fraud measures, risk analysis, credit scoring, and service automation. BRI's AI recommendation system has successfully increased conversion rates by 60% and improved debtor recruitment quality by 49% by 2023.

In the financial technology sector, companies like Akulaku have implemented machine learning for 98% of their risk assessments, facilitating safer financial services while minimizing manual errors and internal fraud that typically affect conventional financing companies. These implementations demonstrate the potential benefits of algorithmic decision-making in improving efficiency and accuracy in financial services^[9].

However, these technological advancements have been accompanied by significant data security challenges. Several major data breach incidents highlight the vulnerabilities in Indonesia's data protection infrastructure:

1. **Tokopedia Data Breach (2020):** An estimated 91 million user accounts and 7 million merchant accounts were compromised, with data sold on the dark web for approximately US\$5,000 (Rp. 74 million). The leaked information included user IDs, email addresses, full names, birth dates, gender, phone numbers, and encrypted passwords. This massive breach affected a significant portion of Indonesia's online consumers, undermining trust in digital platforms.
2. **Bank Indonesia Ransomware Attack (2021):** The Conti ransomware gang breached 237 devices at Bank Indonesia, resulting in a 74GB data leak. This attack on Indonesia's central bank raised serious concerns about the security of critical financial infrastructure and the potential implications for national economic stability.
3. **BPJS Employment Data Breach (2023):** Approximately 18.5 million BPJS Employment user records were compromised and offered for sale on dark web forums for Rp. 153 million. The exposed data included National Identification Numbers (NIK), full names, birth dates, addresses, phone numbers, email

addresses, job types, and company names. This breach was particularly concerning as it involved sensitive employment information of millions of Indonesian workers.

4. **Bank Syariah Indonesia (BSI) Data Theft (2023):** LockBit hackers allegedly stole 1.5TB of data, including 15 million user records, internal access passwords, customer personal information, and loan details. After unsuccessful ransom negotiations, the hackers publicly disseminated the data. This incident highlighted the vulnerability of Islamic banking institutions and raised questions about the adequacy of cybersecurity measures in the financial sector.
5. **Bjorka Hacking Incidents (2022-2023):** A hacker known as Bjorka gained notoriety for accessing and leaking various government and public data, including NIK, addresses, telephone numbers, KTP numbers, cellular operator information, Kominfo data, IndiHome customer data, SIM card registration information, and KPU data. These incidents revealed significant vulnerabilities in government data systems and contributed to public anxiety about data security.

These incidents underscore the critical need for robust regulatory frameworks specifically addressing algorithmic systems and data protection. While Law No. 27 of 2022 represents progress in personal data protection, additional regulations are necessary to address the unique challenges posed by algorithmic decision-making systems, particularly regarding transparency, accountability, and bias mitigation ^[10].

Regulatory Response and Implementation Challenges

Law No. 27 of 2022 on Personal Data Protection

In response to growing concerns about data security and privacy, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection. This legislation aims to ensure that individual rights are guaranteed in terms of protecting personal data and to increase public awareness about the importance of maintaining privacy. The law is grounded in Article 28G paragraph 1 of the 1945 Constitution, which establishes the right to protection of privacy, honor, and property ^[11].

The Personal Data Protection Law aims to safeguard individual interests, uphold legal certainty, balance public and private interests, ensure benefits for society, prioritize precautionary principles, achieve a balance between rights and obligations, uphold accountability, and maintain the confidentiality of personal information. While this represents a significant step forward in data protection, the law has several limitations when applied to algorithmic decision-making systems ^[12]:

1. **Limited Algorithmic Transparency Provisions:** The law does not specifically address the need for transparency in algorithmic decision-making processes, making it difficult for individuals to understand how their data is being used to generate decisions that affect them.
2. **Insufficient Accountability Mechanisms:** While establishing general accountability principles, the law lacks specific provisions for algorithmic accountability,

including clear responsibility allocation when algorithmic systems cause harm.

3. **Inadequate Bias and Discrimination Safeguards:** The law does not explicitly address the potential for algorithmic bias and discrimination, leaving a significant regulatory gap in ensuring fairness in automated decision-making.
4. **Implementation Challenges:** The effective implementation of the law faces challenges including limited technical expertise among regulators, resource constraints, and difficulties in monitoring compliance across diverse sectors and technologies.

The enforcement of regulations governing algorithmic decision-making systems faces several significant challenges ^[13]:

1. **Technical Complexity:** Algorithms, particularly those involving advanced machine learning techniques, are often highly complex and difficult to understand without specialized technical expertise. This complexity makes it challenging for regulators to assess compliance and identify potential violations.
2. **Opacity of Algorithmic Systems:** Many algorithmic systems operate as "black boxes," with decision-making processes that are not transparent or easily explainable. This opacity complicates regulatory oversight and makes it difficult to determine whether systems comply with legal requirements.
3. **Rapid Technological Evolution:** The fast pace of technological development in algorithmic systems means that regulations may quickly become outdated or inadequate to address new challenges and risks.
4. **Cross-Border Data Flows:** The global nature of data flows and algorithmic systems creates jurisdictional challenges for enforcement, particularly when data processing occurs across multiple countries with different regulatory frameworks.
5. **Limited Regulatory Resources:** Indonesian regulatory authorities often face constraints in terms of technical expertise, financial resources, and institutional capacity to effectively monitor and enforce compliance with data protection and algorithmic governance regulations.

Potential Solutions to Algorithmic Governance Challenges

1. Enhancing Transparency in Algorithmic Systems

Transparency is fundamental to ensuring that algorithm-generated decisions can be understood, verified, and held accountable by relevant stakeholders. Several strategies can enhance algorithmic transparency ^[5]:

- **Information Disclosure Requirements:** Organizations implementing algorithmic decision-making systems should be required to disclose information about algorithmic operations, including data types utilized, factors considered in decision-making, and the underlying logic of the system. This disclosure enables stakeholders to better understand how algorithms influence decision processes.

- **Independent Auditing Mechanisms:** Regular independent audits of algorithmic systems and their training data can verify accuracy, fairness, and reliability. These audits should be conducted by qualified third parties with expertise in algorithmic analysis and should be mandatory for systems making high-impact decisions.
- **Transparency Tools Development:** Creating accessible tools and platforms that allow affected individuals to examine and understand algorithm-generated decisions can significantly enhance transparency. Data visualization tools that illustrate decision-influencing factors represent one approach to making algorithmic processes more comprehensible.
- **Stakeholder Education Programs:** Comprehensive education about algorithmic functioning and its decision-making impact can improve transparency through enhanced understanding. This education should target various stakeholders through training programs, seminars, and accessible educational materials.
- **Transparency-Enhancing Regulations:** Implementing regulations that mandate organizational disclosure of algorithmic information and decision processes would effectively increase transparency. These regulations should include requirements for algorithmic explanations and provisions for external examination.

2. Implementing Social and Ethical Impact Assessments

Social and ethical impact assessments throughout the algorithmic development lifecycle represent a crucial approach to ensuring responsible technology use aligned with moral and social values ^[14]:

- **Comprehensive Social Impact Studies:** Conducting thorough social impact analyses before and during algorithm development helps identify potential positive and negative consequences across various social, economic, and cultural contexts. These studies should consider differential impacts on various population segments.
- **Ethical Assessment Frameworks:** Developing and implementing ethical assessment frameworks identifies relevant values and principles for consideration during algorithm development and deployment. These frameworks should address fairness, transparency, privacy, and non-discrimination principles.
- **Multi-stakeholder Consultation Processes:** Involving diverse stakeholders—including civil society representatives, academic experts, and legal practitioners—in algorithm development ensures consideration of multiple perspectives and interests. This inclusive approach helps identify potential issues that developers might otherwise overlook.
- **Rigorous Testing and Continuous Monitoring:** Thorough algorithm testing before widespread implementation, followed by ongoing impact monitoring after deployment, enables problem detection and necessary adjustments. This continuous evaluation

process is essential for responsible algorithmic governance.

- **Developer and User Training Programs:** Providing comprehensive training on the social and ethical implications of algorithmic systems raises awareness and promotes responsible practices among developers, users, and other stakeholders.

3. Developing Adaptive Regulatory Frameworks

Creating regulatory frameworks that respond effectively to rapid technological advancement is essential for addressing algorithmic decision-making challenges ^[6]:

- **Multi-stakeholder Collaboration:** Involving government agencies, academic institutions, industry representatives, and civil society organizations in regulatory development ensures consideration of diverse perspectives and interests. This collaborative approach produces more balanced and effective regulations.
- **Continuous Monitoring and Evaluation Mechanisms:** Implementing ongoing monitoring and evaluation of existing regulations identifies weaknesses and enables necessary adjustments aligned with technological developments. This adaptive approach maintains regulatory relevance and effectiveness over time.
- **Flexible Regulatory Approaches:** Developing adaptable regulatory frameworks accommodates rapid technological change without unduly restricting innovation. A principles-based approach focusing on specific objectives rather than prescriptive requirements offers necessary flexibility.
- **International Regulatory Coordination:** Collaborating with other nations to develop harmonized regulations aligned with international best practices reduces trade barriers and promotes global consistency in technology regulation. This coordination is particularly important given the transnational nature of many algorithmic systems.
- **Responsible Innovation Incentives:** Creating incentives and stimuli that encourage responsible innovation with consideration of social, ethical, and environmental impacts promotes positive technological development. These incentives may include fiscal benefits, subsidies, or research and development support programs.

Comparative Analysis of International Regulatory Approaches

To enhance Indonesia's regulatory framework, it is valuable to examine approaches adopted by other jurisdictions ^[15]:

1. The European Union has established the most comprehensive regulatory framework for algorithmic systems globally. The General Data Protection Regulation (GDPR) includes specific provisions related to automated decision-making, including:
 - Article 22, which provides individuals with the right not to be subject to purely automated decisions with significant effects

- Requirements for explicit consent for automated processing
 - Rights to explanation of the logic involved in automated decisions
 - Data protection impact assessments for high-risk processing activities
2. Building on this foundation, the proposed EU AI Act introduces a risk-based approach to regulating AI systems:
 - Prohibiting AI applications considered unacceptably risky
 - Imposing strict requirements on high-risk AI systems, including transparency, human oversight, and robustness
 - Creating lighter obligations for limited-risk systems

Conclusions

The legal implications of algorithmic decision-making systems present multifaceted challenges requiring comprehensive solutions. The Indonesian regulatory landscape currently exhibits significant limitations: existing regulations lack specificity regarding algorithmic implementation across sectors; privacy protection and data security provisions remain inadequate for algorithmic contexts; and legal responsibility for algorithm-generated decisions remains ambiguously defined.

The case studies examined—including Bank Jombang's AI credit analysis system, BRI's BRIBRAIN platform, and Akulaku's machine learning risk assessment—demonstrate the potential benefits of algorithmic decision-making in financial services. However, major data breach incidents at Tokopedia, Bank Indonesia, BPJS Employment, and Bank Syariah Indonesia highlight the substantial risks associated with inadequate data protection frameworks.

Three key solution areas emerge from this analysis:

- First, enhancing algorithmic transparency through information disclosure requirements, independent auditing mechanisms, transparency tools, stakeholder education, and supportive regulations would significantly improve accountability and trust in algorithmic systems.
- Second, implementing comprehensive social and ethical impact assessments—including social impact studies, ethical frameworks, stakeholder consultation, rigorous testing, and awareness training—would help ensure that algorithmic systems align with societal values and minimize harmful consequences.
- Third, developing adaptive regulatory frameworks through multi-stakeholder collaboration, continuous evaluation, flexible approaches, international coordination, and responsible innovation incentives would create a governance environment that balances technological advancement with necessary protections.

Effective algorithmic governance requires collaboration between government agencies, industry stakeholders, academic institutions, and civil society organizations to develop regulatory frameworks that are both adequate and responsive to technological developments. By implementing these solutions, Indonesia can harness the benefits of algorithmic decision-making systems while mitigating their risks and protecting fundamental rights.

References

1. D Prayogo, I Ruwaida, "Rethinking Nationalism: Looking Back and Looking Forward."
2. DJ Brand, "Algorithmic decision-making and the law," *eJournal of eDemocracy and Open Government*, 2020;12(1):115–132. doi: 10.29379/jedem.v12i1.576.
3. DU Socol De La Osa, N Remolina, "Artificial intelligence at the bench: Legal and ethical challenges of informing - Or misinforming - Judicial decision-making through generative AI," *Data Policy*, Dec, 2024, 6. doi: 10.1017/dap.2024.53.
4. E Yunara, T Kemas, "The Role of Victimology in the Protection of Crime Victims in Indonesian Criminal Justice System," *Mahadi: Indonesia Journal of Law Journal homepage*, 2024;03:63–78. doi: 10.26594/register.v6i1.idarticle.
5. Tsamadou *et al.*, "The ethics of algorithms: key problems and solutions," *AI Soc*, 2022;37(1):215–230, Mar., doi: 10.1007/s00146-021-01154-8.
6. W Ekatjahjana, K Hauerstein, D. Heilmann, *Regulatory Reform in Indonesia A Legal Perspective*, 2019.
7. R Riyanto, B Waluyo, B. Harefa, "Application of Customary Law in the Indonesian Criminal Law Framework after the Enactment of Law Number 1 of 2023 concerning the Criminal Code," *Journal of Progressive Law and Legal Studies*, May, 2025;3(02):161–175. doi: 10.59653/jplls.v3i02.1540.
8. S Subiyanto, S Endah Wahyuningsih, J Hafidz, A Mashdurohatun, "Reconstruction of Employment Regulations that are Integral in Realizing Industrial Relations Based on Pancasila Justice," *Enrichment: Journal of Multidisciplinary Research and Development*, 2025;2(11):1–12. doi: 10.55324/enrichment.v2i11.307.
9. Faisal, A Yanto, DP Rahayu, D Haryadi, A Darmawan, JDN Manik, "Genuine paradigm of criminal justice: rethinking penal reform within Indonesia New Criminal Code," *Cogent Soc Sci*, 2024;10(1). doi: 10.1080/23311886.2023.2301634.
10. Gunarto, EP Marwantono, SE Wahyuningsih, "Reconstruction of regulation of evidence of state financial loss in corruption crime based on justice value," *International Journal of Law*, 2022;8(4):6–7.
11. D Prayogo, I Ruwaida, "Rethinking Nationalism: Looking Back and Looking Forward."
12. L Tibaka, R Rosdian, "The Protection of Human Rights in Indonesian Constitutional Law after the Amendment of the 1945 Constitution of the Republic of Indonesia," *FIAT JUSTISIA: Jurnal Ilmu Hukum*, 2018;11(3):266. doi: 10.25041/fiatjustisia.v11no3.1141.
13. FB Alfian, "Reconstruction of Law Enforcement in Indonesia Through Strengthening the Embodiment of Pancasila Values of Justice to Realize Humane Law Enforcement," *Pancasila and Law Review*, Dec, 2022;3(2):131–142. doi: 10.25041/plr.v3i2.2739.
14. SE Wahyuningsih, S Setiyowati, HR Mahmuhtarom, M Iksan, "Implementation of Restorative Justice on Elderly Actors in Criminal Law Enforcement Based on Justice Value in Indonesia," *International Journal of Social Science and Human Research*, Feb, 2023;06(02). doi: 10.47191/ijsshr/v6-i2-41.
15. SO Manullang, "Understanding the Duties and Responsibilities of the Police in Criminal Cases in the Jurisdiction of a Country: A Study of Legal Literacy," *Legal Brief*, 2022;11(4):2722–4643. doi: 10.35335/legal.