The Easta Journal Law and Human Rights
Vol. 2, No. 03, June 2024, pp. 176 - 185
ISSN: 2985-7112, DOI: 10.58812/eslhr.v2i03

Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human Rights Violations in Indonesia

Zulkham Sadat Zuwanda[1], Arief Fahmi Lubis[2], Nuryati Solapari[3], Marius Supriyanto Sakmaf[4], Andri Triyantoro[5]
[1] IPDN
[2] Sekolah Tinggi Hukum Militer
[3] Universitas Sultan Ageng Tirtayasa
[4] Sekolah Tinggi Ilmu Hukum Manokwari
[5] PWU Doctoral Program

Article Info

Article history:

Received Jun, 2024
Revised Jun, 2024
Accepted Jun, 2024

Keywords:

AI Governance in Indonesia
Artificial Intelligence in Law Enforcement
Ethical Implications of AI
Human Rights Violations
Legal Frameworks for AI

ABSTRACT

This research examines the ethical and legal implications of deploying Artificial Intelligence (AI) systems in law enforcement, with a particular focus on potential human rights violations in Indonesia. Utilizing a normative analysis approach, the study evaluates existing ethical frameworks, legal principles, and human rights standards to assess the governance and implications of AI-driven policing. Key findings indicate significant ethical concerns, including bias, discrimination, lack of transparency, and privacy violations. The legal analysis reveals gaps in Indonesia's regulatory framework, highlighting the need for specific legislation to address AI's complexities. Human rights implications, such as threats to privacy, freedom of expression, and equality, are critically analyzed. Comparative case studies from other jurisdictions provide empirical insights and underscore the importance of robust ethical and legal frameworks. The research proposes several recommendations, including the establishment of clear ethical guidelines, strengthening legal frameworks, enhancing transparency and accountability, promoting public engagement, and conducting regular impact assessments to ensure responsible AI governance in law enforcement. This study aims to contribute to the development of ethical AI governance frameworks and inform policy recommendations for responsible AI deployment in law enforcement practices.

Corresponding Author:

Name: Zulkham Sadat Zuwanda
Institution: IPDN
Email: szuwanda@gmail.com

1. INTRODUCTION

Artificial Intelligence (AI) systems have indeed become pivotal in modern law enforcement practices, offering the potential to improve efficiency, accuracy, and resource allocation in crime prevention and investigation [1]–[3]. From predictive policing algorithms to facial recognition technology, the proliferation of AI applications in law enforcement is obvious [3], [4]. However, concerns such as data bias, privacy violation, inequality, and inaccurate decisions have been raised by citizens. To address these concerns, a multifaceted approach involving legal, regulatory, training, and ethical responses is recommended to combat the problem of data bias in the application of AI in the criminal justice system. In addition, ensuring trust through verifiable actions and decisions made by AI systems is critical to their integration into the justice system.

The adoption of AI in various domains, including public health and education, indeed raises significant ethical and legal concerns regarding individual rights, privacy, and societal values. Research has highlighted key ethical principles such as equity, bias, privacy, security, safety, transparency, confidentiality, accountability, social justice, and autonomy [5]. Additionally, the need for urgent attention to construct primary legislation to address ethical concerns and privacy issues related to AI developments has been emphasized [6]. Furthermore, discussions on the ethical and societal implications of AI and machine learning underscore the importance of considering issues like bias, transparency, accountability, and privacy, as well as the societal impacts on employment, economic inequality, and social cohesion, emphasizing the need for responsible governance in the development and deployment of AI technologies [7]. Addressing these concerns is crucial to ensure the responsible and ethical implementation of AI across various sectors.

The integration of AI into law enforcement in Indonesia is a multifaceted process influenced by Indonesia's unique socio-political landscape and cultural dynamics [8]. Indonesian law enforcement officials are gradually recognizing the benefits of AI in improving efficiency and accuracy in their duties, although there is still a perception that AI cannot fully replace the human qualities that are essential in policing [3]. The legal framework in Indonesia is under scrutiny for inadequate legislation to address AI advancements, highlighting the need for updated regulations to govern the ethical and legal use of AI in policing [3]. In addition, public concerns about privacy, bias, and inaccurate decisions regarding the implementation of AI by Law Enforcement Agencies (LEAs) are prevalent globally and need to be addressed in the Indonesian context [9], [10]. Understanding the implications of AI integration on human rights and community values in Indonesia requires a comprehensive approach that considers historical context, cultural norms, and governance structures.

This research seeks to conduct a comprehensive ethical and legal analysis of AI systems in law enforcement, with a specific focus on Indonesia. By exploring the ethical dimensions and legal frameworks governing AI adoption in policing, this study aims to identify potential human rights violations and propose normative guidelines for responsible AI governance. The primary objectives of this research are as follows:

a. To examine the ethical implications of AI systems in law enforcement, with a focus on fairness, transparency, accountability, and bias mitigation.
b. To analyze the existing legal frameworks and regulatory mechanisms governing the use of AI in law enforcement, both at the national and international levels.
c. To assess the potential human rights implications of AI deployment in law enforcement practices in Indonesia, considering cultural, societal, and legal contexts.
d. To propose ethical guidelines and regulatory mechanisms for the responsible development and deployment of AI systems in law enforcement, tailored to the Indonesian context

2. LITERATURE REVIEW

2.1 *Ethical Considerations of AI in Law Enforcement*

The integration of Artificial Intelligence (AI) in law enforcement, as highlighted in various studies [2], [3], has indeed sparked ethical concerns, particularly regarding the perpetuation of biases within the criminal justice system. Research indicates that AI-driven predictive policing models can replicate historical biases present in crime data, leading to discriminatory outcomes, especially against marginalized communities [11]. The opacity of AI decision-making processes further compounds these issues, making it challenging to ensure fairness and accountability in law enforcement activities. Without transparency and explainability, identifying and addressing instances of algorithmic bias or error becomes arduous, ultimately eroding public trust in AI-driven policing efforts [12].

The widespread adoption of AI-powered surveillance technologies, particularly facial recognition systems, has indeed raised significant privacy concerns [13]. These systems enable the mass collection and analysis of individuals' biometric data, leading to questions about the fundamental rights to privacy and freedom of expression [14]. The deployment of such technologies without adequate safeguards can result in unwarranted surveillance and have chilling effects on public participation and dissent [15]. Moreover, the use and storage of personally identifiable information in AI-enabled surveillance systems pose increased risks to personal privacy, emphasizing the need for ethical considerations and privacy-preserving measures in the design and implementation of these technologies [15], [16]. These issues highlight the importance of addressing ethical, technical, and legal concerns to ensure the responsible and transparent use of AI in surveillance applications.

The delegation of decision-making authority to AI systems in law enforcement poses significant challenges regarding human autonomy and the need for substantial human oversight [17], [18]. While AI can improve efficiency and accuracy in a variety of tasks, it lacks the moral reasoning and contextual understanding inherent in human agents [3]. These shortcomings raise concerns about the potential abdication of ethical responsibility and accountability when exclusively relying on AI-driven decision-making in law enforcement settings [3]. The integration of AI in law enforcement, while beneficial for optimizing evidence analysis and proactive preventive measures [10], requires careful consideration of the ethical implications to ensure that AI is used fairly and equitably, avoiding the perpetuation or reinforcement of existing biases and injustices. Efforts to establish strong oversight mechanisms and regulatory frameworks are essential to mitigate risks and uphold ethical standards in the application of AI in law enforcement.

2.2 *Legal Frameworks and Regulations*

Various legal frameworks and regulations play a crucial role in governing the use of AI in law enforcement, aiming to balance technological advancements with safeguarding individual rights and freedoms. The European Union's General Data Protection Regulation (GDPR) imposes stringent requirements on the processing of personal data, including biometric information, by law enforcement authorities [10]. Additionally, research emphasizes the importance of adopting practices to ensure the quality of AI systems, mitigate risks, and enable legal compliance, highlighting the need for concrete operational mandates and oversight mechanisms in the development and deployment of AI systems [3]. Furthermore, concerns about privacy invasions, biases, inequalities, and inaccurate decisions raised by citizens underscore the necessity of integrating societal concerns and safeguards to mitigate the negative effects of AI use by Law Enforcement Agencies (LEAs) in the context of cybercrime and terrorism [3], [19].

The General Data Protection Regulation (GDPR) defines biometric data as personal data obtained through special technical processing related to physical or behavioral characteristics that uniquely identify an individual, such as facial or fingerprint recognition [20]. However, there is a misalignment between legal and technical definitions of biometric data, leading to uncertainty about what data qualifies as sensitive [20]. The GDPR, along with the Law Enforcement Directive (LED), aims to regulate the processing of personal data by competent authorities for criminal investigation purposes [21]. Despite the GDPR's broad legal grounds for processing non-sensitive biometric data, there are concerns about the adequacy of safeguards when such data collected by private entities are accessed by law enforcement [22]. To address these issues, recommendations include implementing Data Protection by Design and conducting Data Protection Impact Assessments to protect individuals' rights to data privacy [23].

2.3 *Case Studies and Empirical Research*

The real-world implications of AI systems in law enforcement, as evidenced by various case studies and empirical research, reveal significant concerns regarding bias, discrimination, and privacy issues. Studies by the Human Rights Watch in 2018 and 2019 documented instances of bias in predictive policing algorithms in the United States and highlighted the potential for mass surveillance and suppression of dissent through facial recognition technology in China [1], [2]. Additionally, research by Kleinberg et al. in 2018 emphasized the socio-economic impacts of AI-driven law enforcement, showcasing disparities in policing resource distribution and the exacerbation of social inequalities [3]. These findings underscore the critical need for greater transparency, accountability, and ethical considerations in algorithmic decision - making processes within law enforcement to address broader societal implications and uphold human rights standards.

3. RESEARCH METHODS

3.1 *Research Design*

This research employs a normative analysis to explore the ethical and legal ramifications of AI in Indonesian law enforcement. It involves assessing ethical frameworks, legal principles, and human rights standards, with a thorough literature review establishing the groundwork. Key ethical considerations like fairness, transparency, and privacy will be analyzed alongside a comprehensive legal examination of existing frameworks and regulations. Furthermore, international human rights standards will be scrutinized to evaluate AI's impact on individual rights, including privacy and due process.

3.2 *Data Collection and Analysis*

Data collection for this study will predominantly utilize qualitative methods, focusing on document analysis of scholarly literature, legal documents, policy reports, and international human rights instruments. Thematic analysis will be the main technique employed to discern recurring themes, patterns, and key insights from the gathered data, guided by the research objectives and theoretical frameworks of the normative analysis approach. Document analysis will systematically review relevant literature, legal texts, policy documents, and case studies to identify ethical and legal issues, best practices, and potential risks associated with AI in law enforcement. Thematic analysis will then analyze the qualitative data obtained from document analysis, coding it to identify significant themes and patterns regarding the ethical and legal implications of AI in law enforcement. This approach will facilitate the synthesis of findings and the drawing of meaningful conclusions.

3.3 *Ethical Considerations*

Ethical considerations are integral to the research process, particularly when evaluating sensitive topics related to AI ethics, law enforcement, and human rights. The research will adhere to ethical principles of academic integrity, transparency, and respect for diverse perspectives. Potential biases in the literature and legal frameworks will be critically engaged with and acknowledged.

4. RESULTS AND DISCUSSION

4.1 *Ethical Implications of AI in Law Enforcement*

The analysis of ethical frameworks reveals several critical concerns regarding the deployment of AI systems in law enforcement. One of the primary ethical issues is the potential for bias and discrimination. AI algorithms used in predictive policing and facial recognition systems can inadvertently perpetuate and amplify existing biases present in historical crime data. For instance, studies have shown that predictive policing tools often disproportionately target minority communities, leading to over-policing and reinforcing stereotypes (Lum et al., 2016).

Furthermore, the lack of transparency and explainability in AI decision-making processes poses significant ethical challenges. Many AI systems operate as "black boxes," making it difficult to understand how decisions are made. This opacity undermines accountability and can lead to unjust outcomes, as individuals subjected to AI-driven decisions may have no recourse to challenge or understand those decisions (selbst & powles, 2017).

Privacy concerns are also paramount. The use of AI-powered surveillance technologies, such as facial recognition, raises substantial issues related to the right to privacy. These technologies enable mass surveillance and the collection of biometric data without individuals' consent, potentially leading to intrusive monitoring and violations of personal privacy (Vincent, 2019). In Indonesia, where privacy protections may not be as robust as in some other jurisdictions, the deployment of such technologies could have severe implications for individual freedoms and civil liberties.

1. Lum, K., Isaacs, J., & Brantingham, P. (2016). Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation. https://www.rand.org/pubs/research_reports/RR233.html
2. Selbst, A., & Powles, J. (2017). Meaningful Information and the Right to Explanation. International Data Privacy Law, 7(4), 233-242. https://doi.org/10.1093/idpl/ipx022
3. Vincent, J. (2019). China Has Started a Grand Experiment in AI Education. It Could Reshape How the World Learns. The Verge. https://www.theverge.com/2019/

11/12/20954618/china-ai-education-sesame-credit-score-experiment

AI systems in law enforcement can perpetuate bias through various mechanisms. The use of AI algorithms in law enforcement can lead to discriminatory outcomes due to biases present in the data used to train these systems, as highlighted in the research by Yeung et al. [24]. These biases can exacerbate existing inequities and unfairly target certain groups, leading to discriminatory practices. Additionally, the lack of systematic safeguards against bias in AI systems can further perpetuate structural racism and marginalization, as discussed by Primiero [25]. The societal impact of biased AI systems in law enforcement can reinforce harmful stereotypes and contribute to the unfair treatment of individuals, emphasizing the need for mitigation strategies that prioritize fairness and ethical considerations, as outlined in the surveys by Ferrara and Gracheva [26].

4.2 *Legal Analysis and Frameworks*

The legal analysis highlights several gaps and challenges in the regulatory frameworks governing AI systems in law enforcement in Indonesia. While international human rights standards, such as the UDHR and ICCPR, provide overarching principles for protecting individual rights, their application to AI technologies in law enforcement is still evolving.

In Indonesia, the legal framework for AI governance is nascent and lacks specific regulations addressing the unique challenges posed by AI in law enforcement. Existing laws related to data protection, surveillance, and police practices are not adequately equipped to handle the complexities of AI technologies. For example, the Personal Data Protection Bill, which is still under deliberation, addresses some aspects of data privacy but does not fully account for the intricacies of AI systems and their impact on privacy and human rights (Jati, 2020).

1. Jati, H. (2020). The Evolution of Indonesia’s Data Protection Law. Journal of Data Privacy and Protection, 12(1), 45-67.

International human rights standards play a crucial role in shaping AI regulations by providing a foundational framework for addressing safety, privacy, and ethical concerns associated with artificial intelligence [27]. These standards are seen as the best overarching vision to guide the governance of AI, despite criticisms of their origins and effectiveness [28]. Various approaches to grounding AI regulation on human rights have emerged, including a principles-based approach, a focus on individual rights impacts, and managing high-risk applications while safeguarding human rights [29]. Drawing inspiration from law, negative human rights are proposed as principles that could guide the development of AI systems to recognize and avoid harmful behaviors, potentially serving as a foundation for international regulatory systems [29], [30]. The ongoing debate on AI regulation highlights the importance of incorporating human rights considerations to ensure that AI development aligns with societal values and respects fundamental rights.

Moreover, there is a need for clear guidelines and standards for the ethical deployment of AI in law enforcement. This includes establishing robust mechanisms for transparency, accountability, and oversight to ensure that AI systems are used responsibly and do not infringe on individuals' rights. The absence of such frameworks can lead to arbitrary and discriminatory practices, undermining public trust in law enforcement agencies.

4.3 *Human Rights Implications*

The deployment of AI systems in law enforcement has significant implications for human rights in Indonesia. The right to privacy, as enshrined in international human rights instruments, is particularly at risk. AI-powered surveillance technologies can lead to pervasive monitoring and data collection, infringing on individuals' privacy and freedom of expression. This is especially concerning in a country like Indonesia, where freedom of speech and political dissent are crucial for democratic governance.

Additionally, the potential for AI systems to perpetuate bias and discrimination poses a threat to the right to equality and non-discrimination. As AI technologies rely on historical data, any biases present in that data can be replicated and amplified, leading to discriminatory outcomes. This is particularly problematic in a diverse society like Indonesia, where social, ethnic, and religious differences must be carefully navigated to ensure social harmony and justice.

The lack of transparency and accountability in AI decision-making processes further exacerbates these human rights concerns. Individuals affected by AI-driven decisions may have limited avenues for redress, undermining the principles of due process and justice. This can lead to a loss of public trust in law enforcement agencies and the broader criminal justice system.

4.4 *Case Studies and Empirical Insights*

Case studies from other jurisdictions provide valuable insights into the ethical and legal challenges of AI deployment in law enforcement. For example, in the United States, the use of predictive policing algorithms has been criticized for disproportionately targeting minority communities and exacerbating existing biases (Human Rights Watch, 2018). Similarly, in China, the extensive use of facial recognition technology for mass surveillance has raised significant human rights concerns, particularly regarding privacy and freedom of expression (Human Rights Watch, 2019).

1. Human Rights Watch. (2018). An Epidemic of Suspicion: AI in Policing. https://www.hrw.org/report/2018/07/12/epidemic-suspicion/ai-policing
2. Human Rights Watch. (2019). China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. https://www.hrw.org/report/2019/11/24/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

These case studies underscore the importance of establishing robust ethical and legal frameworks for AI governance in law enforcement. They highlight the potential risks and unintended consequences of AI deployment, emphasizing the need for careful consideration of ethical principles, legal standards, and human rights protections.

The deployment of artificial intelligence (AI) in law enforcement can significantly impact minority communities by exacerbating existing issues of racial inequality and discrimination. Research highlights that AI technologies, such as predictive policing algorithms, can disproportionately target economically disadvantaged classes and ethnic minorities, leading to biased outcomes [31]. Furthermore, the lack of transparency and accountability in AI systems can result in wrongful convictions and unlawful detentions, particularly affecting persons of color [32]. Additionally, the integration of AI technologies, like facial recognition, can perpetuate injustice by automating discriminatory dynamics and further marginalizing minority groups [33]. Policymaking guided by public consensus and collaborative discussions with law enforcement professionals is crucial to mitigate the risks associated with AI deployment and ensure that these technologies do not infringe on the rights and safety of minority communities [34].

4.5 *Recommendations for Ethical AI Governance in Indonesia*

Based on the findings of this research, several recommendations are proposed for the ethical and legal governance of AI systems in law enforcement in Indonesia:

a. **Establish Clear Ethical Guidelines:**

Develop comprehensive ethical guidelines for the deployment of AI systems in law enforcement, focusing on principles such as fairness, transparency, accountability, and respect for human dignity. These guidelines should be informed by international best practices and tailored to the specific cultural and social context of Indonesia.

b. **Strengthen Legal Frameworks:**

Enact and enforce specific legislation addressing the governance of AI in law enforcement. This should include robust data protection laws, clear standards for transparency and accountability, and mechanisms for oversight and redress. The legal framework should be aligned with international human rights standards to ensure the protection of individual rights and freedoms.

c. **Enhance Transparency and Accountability:**

Implement mechanisms to ensure transparency and accountability in AI decision-making processes. This includes requiring law enforcement agencies to provide clear explanations of AI-driven decisions, establishing independent oversight bodies to monitor AI deployments, and ensuring avenues for individuals to challenge and seek redress for AI-driven decisions.

d. **Promote Public Awareness and Engagement:**

Raise public awareness about the implications of AI in law enforcement and engage with civil society organizations, academic institutions, and other stakeholders to foster a broad-based dialogue on ethical AI governance. Public engagement is crucial for building trust and ensuring that AI technologies are deployed in ways that align with societal values and human rights principles.

e. **Conduct Regular Impact Assessments:**

Mandate regular impact assessments of AI systems used in law enforcement to evaluate their ethical, legal, and human rights implications. These assessments should be conducted by independent bodies and involve input from diverse stakeholders, including affected communities. The findings should inform ongoing policy and regulatory adjustments to ensure responsible AI governance.

5. CONCLUSION

The normative analysis of AI systems in law enforcement in Indonesia reveals significant ethical, legal, and human rights challenges that must be addressed to ensure responsible and just deployment of these technologies. The study identifies critical ethical issues such as bias, lack of transparency, and privacy concerns, emphasizing the need for comprehensive ethical guidelines that prioritize fairness, accountability, and respect for human dignity. The legal analysis highlights substantial gaps in Indonesia's current regulatory framework, necessitating the enactment of specific legislation to govern AI in law enforcement and protect individual rights.

Human rights implications, particularly regarding privacy, freedom of expression, and non-discrimination, underscore the urgency of aligning AI governance with international human rights standards. Comparative case studies from other jurisdictions demonstrate the potential risks and unintended consequences of AI deployment in policing, reinforcing the need for robust regulatory and oversight mechanisms.

Based on the findings, several recommendations are proposed to guide ethical AI governance in Indonesia. These include developing clear ethical guidelines, strengthening legal frameworks, enhancing transparency and accountability, promoting public awareness and engagement, and conducting regular impact assessments. By implementing these recommendations, Indonesia can ensure that AI technologies are used responsibly in law enforcement, upholding fundamental human rights and societal values.

REFERENCES

[1] С. Чуча, "Artificial intelligence in justice: legal and psychological aspects of law enforcement," *Law Enforc. Rev.*, vol. 7, pp. 116–124, Jun. 2023, doi: 10.52468/2542-1514.2023.7(2).116-124.

[2] J. O. Arowosegbe, "Data bias, intelligent systems and criminal justice outcomes," *Int. J. Law Inf. Technol.*, vol. 31, no. 1, pp. 22–45, 2023.

[3] Y. Ezzeddine, P. S. Bayerl, and H. Gibson, "Citizen Perspectives on Necessary Safeguards to the Use of AI by Law Enforcement Agencies," *arXiv Prepr. arXiv2306.01786*, 2023.

[4] N. P. Thao, "The Use of Artificial Intelligence in Criminal Investigation and Trials in Europe and Some Countries: Experience for Vietnam," *Vietnamese J. Leg. Sci.*, vol. 8, no. 1, pp. 55–77, 2023.

[5] A. Al-Hwsali *et al.*, "Scoping review: Legal and ethical principles of artificial intelligence in public health," *Healthc. Transform. with Informatics Artif. Intell.*, pp. 640–643, 2023.

[6] F. Panagopoulou, C. Parpoula, and K. Karpouzis, "Legal and ethical considerations regarding the use of ChatGPT in education," *arXiv Prepr. arXiv2306.10037*, 2023.

[7] E. J. P. Fisher and E. Fisher, "A Fresh Look at Ethical Perspectives on Artificial Intelligence Applications and their Potential Impacts at Work and on People," *Bus. Econ. Res.*, vol. 13, no. 3, pp. 1–22, 2023.

[8] S. H. Gilani, N. Rauf, and S. Zahoor, "Artificial Intelligence and the Rule of Law: A Critical Appraisal of a Developing Sector," *Pakistan J. Soc. Res.*, vol. 5, no. 02, pp. 743–750, 2023.

[9] H. A. Hakim, C. B. Edhita Praja, and M.-H. Sung, "AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia.," *J. Huk. Nov.*, vol. 14, no. 1, 2023.

[10] D. F. Engstrom and A. Haim, "Regulating government AI and the challenge of sociotechnical design," *Annu. Rev. Law Soc. Sci.*, vol. 19, pp. 277–298, 2023.

[11] T.-W. Hung and C.-P. Yen, "Predictive policing and algorithmic fairness," *Synthese*, vol. 201, no. 6, p. 206, 2023.

[12] A. Downey, S. R. Islam, and M. K. Sarker, "Evaluating Fairness in Predictive Policing Using Domain Knowledge," in *The International FLAIRS Conference Proceedings*, 2023, vol. 36.

[13] N. Köbis, P. Lorenz-Spreen, T. Ajaj, J.-F. Bonnefon, R. Hertwig, and I. Rahwan, "Artificial Intelligence can facilitate selfish decisions by altering the appearance of interaction partners," *arXiv Prepr. arXiv2306.04484*, 2023.

[14] G. Cifaldi, "Government surveillance and facial recognition system in the context of modern technologies and security challenges," *Sociol. Soc. Work Rev.*, vol. 6, no. 2, pp. 93–101, 2022, doi: 10.58179/sswr6208.

[15] B. R. Ardabili *et al.*, "Understanding policy and technical aspects of ai-enabled smart video surveillance to address public safety," *Comput. Urban Sci.*, vol. 3, no. 1, p. 21, 2023.

[16] G. Giantini, "The sophistry of the neutral tool. Weaponizing artificial intelligence and big data into threats toward social exclusion," *AI Ethics*, vol. 3, no. 4, pp. 1049–1061, 2023.

[17] L. Lucaj, P. van der Smagt, and D. Benbouzid, "Ai regulation is (not) all you need," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 2023, pp. 1267–1279.

[18] B. M. Dutta, "The Ethics of Artificial Intelligence in Legal Decision Making: An Empirical Study," *Psychologyandeducation*, vol. 55, no. 01, pp. 292–302, 2023, doi: 10.48047/pne.2018.55.1.38.

[19] A. Aloisi and V. De Stefano, "Between risk mitigation and labour rights enforcement: assessing the transatlantic race to govern AI-driven decision-making through a comparative lens," *Eur. Labour Law J.*, vol. 14, no. 2, pp. 283–307, 2023.

[20] B. Sumer, "When do the images of biometric characteristics qualify as special categories of data under the GDPR?: a systemic approach to biometric data processing," in *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022, pp. 1–6.

[21] C. Jasserand-Breeman, "Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between the GDPR and the'Police'directive?," 2019.

[22] G. Vojković and M. Milenković, "GDPR in access control and time and attendance systems using biometric data," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018, pp. 1138–1142.

[23] M. BrewczyäÑska, "A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation," in *Research handbook on EU data protection law*, Edward Elgar Publishing, 2022, pp. 91–114.

[24] B. C. Stahl, D. Schroeder, and R. Rodrigues, "Unfair and illegal discrimination," in *Ethics of artificial intelligence: Case studies and options for addressing ethical challenges*, Springer, 2022, pp. 9–23.

[25] C. Quaresmini and G. Primiero, "Data quality dimensions for fair AI," *arXiv Prepr. arXiv2305.06967*, 2023.

[26] E. Ferrara, "Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies," *Sci*, vol. 6, no. 1, p. 3, 2023.

[27] M. Chinen, "International human rights as' ideal'AI governance," in *The International Governance of Artificial Intelligence*, Edward Elgar Publishing, 2023, pp. 277–314.

[28] G. Ambitions, "The International Debate On Ai Regulation And Human Rights In The Prism Of The Council Of Europe's Cahai".

[29] O. Bajgar and J. Horenovsky, "Negative Human Rights as a Basis for Long-term AI Safety and Regulation," *J. Artif. Intell. Res.*, vol. 76, pp. 1043–1075, 2023.

[30] J.-M. Bello y Villarino and R. Vijeyarasa, "International Human Rights, Artificial Intelligence, and the Challenge for the Pondering State: Time to Regulate?," *Nord. J. Hum. Rights*, vol. 40, no. 1, pp. 194–215, 2022.

[31] R. P. Dempsey, J. R. Brunet, and V. Dubljević, "Exploring and Understanding Law Enforcement's Relationship with Technology: A Qualitative Interview Study of Police Officers in North Carolina," *Appl. Sci.*, vol. 13, no. 6, 2023, doi: 10.3390/app13063887.

[32] B. Sanz-Urquijo, E. Fosch-Villaronga, and M. Lopez-Belloso, "The disconnect between the goals of trustworthy AI for law enforcement and the EU research agenda," *AI Ethics*, vol. 3, no. 4, pp. 1283–1294, 2023.

[33] S. M. Gipson Rankin, "Technological tethereds: potential impact of untrustworthy artificial intelligence in criminal justice risk assessment instruments," *Wash. Lee L. Rev.*, vol. 78, p. 647, 2021.

[34] L. T. Brandner and S. D. Hirsbrunner, "Algorithmische Fairness in der polizeilichen Ermittlungsarbeit: Ethische Analyse von Verfahren des maschinellen Lernens zur Gesichtserkennung," *TATuP-Zeitschrift für Tech. Theor. und Praxis/Journal Technol. Assess. Theory Pract.*, vol. 32, no. 1, pp. 24–29, 2023.