Vol. 34 (2026): Proceedings of the 2026 ICSSCS Symposium on Environmental, Social, and Governance (ICSSCS-ESG 2026)
E-ISSN: 3105-0522 P-ISSN: 3105-0514
DOI: https://doi.org/10.70267/ICSSCS-ESG-2026.2026.0107

AI Governance: Tripartite Joint Adjudication and the Triangular Supervision Model for AI-related Law Enforcement Disputes

Pinjia Chen*

Vanke Meisha Academy, Guangdong, China

**Corresponding author: Pinjia Chen.*

Abstract

Driven by pervasive social prejudice and bias, this study focuses on algorithmic discrimination emerging alongside widespread artificial intelligence adoption in public governance. Beyond inherent human biases, automated systems can embed encoded bias, which poses severe threats to civil rights when AI is deployed within law enforcement. Drawing on two typical U.S. cases involving wrongful detention triggered by misidentification from facial recognition and AI weapon detection tools, this paper identifies prominent institutional defects including the algorithmic black box and insufficient multi-party checks and balances under the existing regulatory framework. To mitigate such risks, the research proposes a tripartite joint adjudication mechanism, also defined as the triangular supervision model. This framework consists of professional public representatives, government technical supervisors, and AI technical developers, forming a balanced oversight system. It breaks algorithmic opacity, clarifies accountability for AI-induced harms, and transforms passive dispute resolution into proactive governance. By comparing the model with IBM's responsible AI governance principles, this article verifies its theoretical rationality. This research argues that relevant federal and state legislation should be introduced in the United States to formalize the mechanism, ensuring AI improves administrative efficiency without undermining due process, equal protection and fundamental human rights.

Keywords

AI governance, algorithmic bias, triangular supervision model, tripartite joint adjudication, law enforcement civil rights

1. Introduction

In modern society, artificial intelligence has become an indispensable tool in people's daily lives. Capable of simplifying workflows and delivering instant feedback, Artificial Intelligence significantly increases overall efficiency across global sectors. In the United States, governmental institutions have widely integrated artificial intelligence into public security systems; for instance, local police departments adopt facial recognition technology powered by AI to identify and track potential criminals. While such practical applications remarkably accelerate case handling and reduce the cost of dispatch, the biased algorithms and accidental technical errors simultaneously trigger severe and far-reaching controversies [1]. For instance, Buolamwini and Gebru empirically demonstrated that commercial facial recognition systems misidentified darker-skinned females at error rates of up to 34.7%, compared to just 0.8% for lighter-skinned males [2].

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

These hidden risks mainly involve wrongful arrests, racial discrimination, unauthorized privacy intrusion and fundamental violations aligned with innate human prerogatives. In reality, there are many real-life examples that demonstrate the risks and immaturity of AI supervision. AI still cannot make 100 percent accurate adjustments, as illustrated by crucial cases that happened in the United States. Therefore, tripartite joint adjudication is strongly demanded within government systems that involve artificial intelligence. This mechanism can be used to uphold justice and eliminate algorithmic bias in courts.

2. Typical AI Law Enforcement Misjudgment Cases and Governance Deficiencies

2.1 Wrongful Arrest Case Caused by AI Facial Recognition Error

In Tennessee, an attorney outlines potential lawsuit plans after AI led to the flawed arrest of a Tennessee grandmother [3]. AI is already used in United States police departments, which helps them conduct facial recognition of criminals or people who have already been charged, but their recognition results are not always accurate, which could produce adverse detention and cause harm either physically or mentally or both [4]. Related to FARGO, N.D. (Valley News Live): A woman who spent months behind bars after an AI system mistook her for a bank fraud suspect [3]. After release, the misidentified suspect and her family filed civil rights claims against Fargo authorities and demanded financial remediation. The suspect, named Angela Lipps, a Tennessee grandmother, was arrested in July of 2025 after Fargo Police used AI facial recognition technology allegedly linking her to a bank fraud scheme. Local attorneys proved in December that she was not the suspect. All these paradoxes were caused by AI-defective facial recognition and excessive baseline reliance upon automated screening outputs. Furthermore, it harms both the victims and the police department. The police department needs to compensate Angela Lipps' family and suffers contracted bureaucratic legitimacy, and Angela Lipps, the elderly grandmother, suffered cascaded physical and mental harm. While there is currently no formal legal action on record, Lipps has retained legal representation in order to explore possible claims related to civil rights violations [3]. From this case, we can see that the AI-opaque paradigm and incomplete legal provisions make these cases difficult to judge.

While there is currently no formal legal action on record, Lipps has retained legal representation in order to explore possible claims related to civil rights violations [3]. From this case, we can see that the AI black box and incomplete legal provisions make it hard to deal with these cases and judgments. The black box of AI makes judgments difficult. Nobody knows how the algorithm of AI works and how it conducts its facial recognition. Even if they did, judges, police departments, and victims would still find it hard to understand how AI's algorithm works without professional knowledge of computer science and artificial intelligence. From this case, we can see how the legislative institution and the new law targeting AI-related cases are important for the United States government. This is due to the fact that AI has become not only an easy tool that helps us solve problems, but it has also become a tool to help governance make decisions. The police department is totally misled by AI's false recognition and takes harmful actions. Therefore, AI must be limited and supervised, therefore the triangle supervising model should be established, which is a model that can solve the black box and algorithm bias and discrimination. From this case, we can clearly identify two prominent systemic flaws accompanying AI law enforcement. First is the AI black box problem, the internal logic of facial recognition algorithms remains opaque. Without specialized computer expertise, police, judges and ordinary citizens cannot trace how the algorithm reaches its matching conclusion. Furthermore, when errors and misrecognition in algorithms lead to wrongful arrest, it is hard to trace responsibility when victims appear. Second, there exists an absence of multi-party checks and balances within the existing governance framework. At present, police forces largely rely autonomously on AI outputs for law enforcement decisions. No independent third party can review algorithmic results or restrain over-reliance on automated screening. Once technical errors or biased data trigger misidentification, victims face lengthy obstacles seeking remedies for civil rights infringements.

Given these loopholes, effective restrictions and oversight mechanisms for AI law enforcement are urgently required. From this perspective, we can understand why legislative institutions and new regulations targeting AI-related cases are important for governments in the United States. This is due to the fact that AI has become not merely a convenient tool to help us solve problems; it has also grown into a tool supporting administrative governance and official decision-making. The police department was completely misled by false AI recognition and carried out harmful actions against citizens. Therefore, AI must be restricted and supervised.

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

Accordingly, the tripartite supervision model should be constructed. This model can address the challenges of algorithmic black boxes, algorithm bias and algorithmic discrimination. Given these loopholes, effective restrictions and oversight mechanisms for AI law enforcement are urgently required. From this perspective, we can understand why the legislative institutions and new regulations targeting AI-related cases are important for governments in the United States. This is due to the fact that AI has become not merely a convenient tool to help us solve problems; it has also grown into a tool supporting administrative governance and official decision-making. The police department was completely misled by false AI recognition and carried out harmful actions against citizens. Therefore, AI must be restricted and supervised. Accordingly, the tripartite supervision model should be constructed. This model can address the challenges of algorithmic black boxes, algorithm bias and algorithmic discrimination.

When AI-related legal disputes and rights violations occur, such as the wrongful arrest of Angela Lipps, adjudicating personnel entrusted by the government to hear these cases must be strictly professional and technically competent, rather than relying on untrained staff or one-sided law enforcement narratives. First and foremost, these government judicial specialists must undergo rigorous professional training in computer science, AI algorithm mechanics and ethical governance, equipping them to thoroughly scrutinize AI algorithmic logic, source code access protocols and decision-making chains. Their core duty is to verify whether AI systems harbor discriminatory tendencies, root out implicit biases embedded in training datasets or algorithmic design, and rigorously assess whether automated law enforcement decisions comply with federal civil rights laws and state-level governance standards. As the pivotal judicial backbone of the triangle supervision model, these professional government adjudicators hold the authority to review full AI system operation records, access permission logs and decision-making trails post-incident. They are tasked with independently verifying abnormal facial recognition outputs, unauthorized data usage and algorithmic drift that led to real-world harm, ensuring that rulings on AI-related cases are grounded in technical facts and legal fairness, instead of being swayed by opaque AI black box outputs or unsubstantiated law enforcement claims.

2.2 AI Weapon Misjudgment Case Reflecting Algorithmic Racial Bias

There is another case in which a teen was detained after an AI system mistook chips for a weapon outside Kenwood High School [5]. The victim who was misidentified is an African American, which might indicate the algorithm bias of AI. A 16-year-old student from Kenwood High School claims he was held at gunpoint and handcuffed right outside his school, simply because the AI mistook a bag of chips for something suspicious. On Monday afternoon, after football practice, Taki Allen was sitting with his friends when armed police officers suddenly surrounded him. Taki Allen told FOX45 News: *I just in that moment, I didn't feel safe. I didn't feel like the school actually cared about me. Because nobody came up to me after, not even the principal.* [5]. Allen explained that the officers pointed their guns at him, told him to get on the ground, and took him into custody. He felt terrified and deeply shaken, worried that his life was in danger. This whole incident happened because an AI-powered gun detection system deployed in schools across Baltimore County gave out a false alarm [5]. This is not an isolated incident, Buolamwini and Gebru found that commercial facial analysis systems consistently underperform on individuals with darker skin tones due to severely unbalanced training datasets, indicating that the algorithmic bias targeting Allen is a structural, industry-wide problem [2]. Overall, in these cases, algorithmic bias distinctly demonstrates racial bias within AI decision-making, which has caused serious consequences.

3. Core Framework of Triangular Supervision Model Based on Tripartite Joint Adjudication

Cheong notes that effective AI governance requires interdisciplinary and multi-stakeholder approaches that integrate technical expertise, legal accountability, and ethical oversight, precisely the logic undergirding the *tripartite joint adjudication model* proposed here [6]. To break the AI black box and ensure impartial, transparent adjudication of AI-related legal disputes, the tripartite joint adjudication hinges on tripartite joint adjudication composed of three distinct professional cohorts, each bringing irreplaceable expertise to balance technical accuracy, legal fairness, and public trust. This collaborative framework replaces one-sided law enforcement reliance on AI outputs with a checks-and-balances system that addresses accountability gaps, demystifies algorithmic decisions, and protects vulnerable individuals from wrongful AI-driven actions.

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

3.1 Professional Public Representatives: Independent Ethical and Civil Rights Stewards

The first group includes trained, qualified public representatives, not everyday people, to keep oversight fair and well-informed. These members should have a solid background in civil rights, AI ethics, data privacy, or social fairness, and understand how AI affects communities, especially groups that are easily left behind. Their main job is to protect public interests and basic personal rights. Working independently, they can push back against unfair AI results, measure real harm caused by flawed algorithms, such as wrongful arrest, emotional distress, or damaged reputation, and make sure rules care more about people than fast, simple work. In the end, they help reduce hidden official bias and make sure AI rules follow normal democratic ideas, instead of only helping police or government improve operational efficiency.

3.2 Government Professional Oversight Personnel: Technical and Regulatory Supervisors

The second pillar comprises government-employed technical and regulatory professionals with formal training in computer science, AI engineering, cybersecurity, and public sector compliance. These experts work directly inside government agencies that use AI, such as police and homeland security teams. They have clear authority to check how AI algorithms run, review basic computer code, look through training data, and make sure the AI follows state and federal rules.

They monitor every decision made by public safety AI tools, including facial recognition, suspect searches, and risk assessments. They record mistakes, biased data, and hidden adjustments made to the algorithm. Outside reviewers cannot access real-time updates immediately, but these internal specialists can view live AI records. When the AI gives false or unsafe results, they can step in quickly and stop police from acting unfairly or hurting people based on flawed information.

3.3 AI Developers and Training Professionals: Technical Accountability and Transparency Providers

The third pillar is made up of AI developers, data scientists, and model training specialists from the tech companies or research institutions that design, build, and maintain the AI systems deployed by government agencies. These professionals possess firsthand knowledge of the AI model’s architecture, training methodologies, accuracy thresholds, and known limitations, insights that are impossible for non-technical stakeholders to replicate. Under the triangle supervision model, they are legally obligated to participate in AI-related legal case adjudication, provide full transparency into algorithmic decision-making processes, explain technical errors (such as facial recognition misidentification due to poor dataset diversity or flawed feature matching), and assume accountability for defects in model design or training. They cannot withhold technical details under the guise of commercial confidentiality when such information is critical to resolving civil rights violations or wrongful harm claims; instead, they must collaborate with the other two cohorts to demystify the AI black box.

4. Operational Logic of the Tripartite Joint Adjudication System

4.1 Complete Operating Process of the Tripartite Panel

In practice, this three-party professional panel takes collective responsibility for reviewing AI-related cases, investigating algorithmic harm cases, and making final decisions about who is responsible and what should be done to remedy the harm. When a case like Angela Lipps' wrongful arrest happens, the panel gets to work right away. First, the AI developers need to identify what went wrong with the facial recognition system, such as why it made the mistake and whether bias exists within training data. Second, the government oversight personnel need to check if the police department used the AI correctly and if they ignored internal regulations or violated arrest procedures. Third, the public representatives evaluate harm inflicted on the victim, not just physical injury, but outcomes like emotional distress and violated civil rights. The three-party panel jointly audits the whole AI decision-making process, identifies algorithmic bias, and unpacks the black box without requiring full universal disclosure of proprietary code. The synchronized, expertise-driven collaboration envisioned here aligns with Cheong’s call for transparent decision-making processes and clear accountability mechanisms that do not rely on a single stakeholder's interpretation of algorithmic outputs [6]. Only through

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

this synchronized, expertise-driven collaboration can courts and regulatory bodies issue fair, well-founded judgments, assign clear accountability (whether to the AI developer, the overseeing agency, or both), and establish enforceable precedents for future AI governance. This triangle supervision model not only resolves the current deadlock of AI-related legal cases but also establishes a prevention mechanism. Before permanently deploying AI in governance, professional tripartite panels conduct advance oversight of AI systems. Thus, governments can curb algorithmic bias, eliminate black box opacity, and ensure that AI serves as a responsible governance tool, one that enhances efficiency without sacrificing justice, privacy, or fundamental human rights. For the United States, enacting legislation to formalize this professional tripartite framework is not merely a regulatory choice, but a necessary step to moderate AI innovation with the nation's commitment to equal protection under the law, making them more compatible.

4.2 Consistency between the Model and IBM's Standard AI Governance Principles

IBM states that good AI governance needs "oversight mechanisms" to deal with risks like bias and privacy violations [7], which is exactly the function of the three cohorts outlined above: forming a dedicated oversight mechanism. Instead of letting police or other agencies use AI without independent verification, this model creates a specialized panel tasked with investigating incidents. They do not simply accept AI outputs at face value, they examine underlying code, training data and decision trails. IBM also lists four principles for responsible AI: empathy, bias control, transparency, and accountability [7], which fully correspond to the core design of the tripartite supervision model. In terms of transparency and accountability, IBM argues AI companies should be able to explain how their algorithms make decisions [7], and in the proposed model, this responsibility falls to AI developers, who cannot hide behind commercial confidentiality when innocent citizens suffer wrongful arrest and must fully cooperate with the panel to clarify technical failures, making such transparent explanation a necessary legal requirement rather than an optional industry standard. In terms of bias control, IBM emphasizes auditing training data to prevent AI from inheriting human prejudices [7], a core duty undertaken by government oversight personnel in the tripartite system, who inspect algorithmic code and training datasets thoroughly to identify biased materials and root out structural discrimination, which is well illustrated by the Kenwood High School incident, where specialists can trace problematic dataset designs if the AI system repeatedly produces false alarms targeting Black teenagers carrying daily items like snacks.

In terms of the empathy principle highlighted by IBM, effective AI governance must prioritize and understand the real social impact of AI deployment on ordinary people [7], a human-centered mission undertaken by professional public representatives in the model. These representatives balance technical and regulatory judgments by focusing on tangible personal harm, including the emotional trauma experienced by Angela Lipps during wrongful arrest and the fear endured by the misidentified high school student, ensuring that the supervision mechanism never prioritizes administrative efficiency over basic human rights and public interests. Beyond these core principles, IBM advocates for proactive and continuous monitoring mechanisms to supervise AI systems in real time and eliminate potential risks before they cause substantial harm [7], a practical function that can be fully embedded into the tripartite adjudication framework. After investigating and resolving AI-related misjudgment cases, the panel can issue standardized regulatory requirements, such as mandating real-time bias detection modules for law enforcement AI systems and establishing complete operation and audit logs, enabling timely fault tracing and risk prevention for future AI applications. Beyond industry standards, Cheong further argues that participatory governance models incorporating public representatives alongside technical and legal experts are essential for ensuring AI systems reflect the values and priorities of diverse communities, reinforcing the necessity of professional public representatives in the tripartite model [6]. While the *triangular supervision model* was initially conceived for this research, its high consistency with IBM's authoritative AI governance system proves that the framework possesses a solid theoretical basis and practical feasibility. Rather than merely providing passive litigation remedies after AI-induced harm occurs, the model constructs a complete, professional, and multi-dimensional accountability system that can actively supervise AI operation, locate technical defects, constrain algorithmic bias, and prevent repeated violations of civil rights, which is increasingly essential as AI gains growing dominance in public governance.

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

5. Conclusion

In conclusion, the cases of Angela Lipps and Taki Allen are not isolated technological glitches; they are harbingers of a future where unaccountable AI systems can inflict profound harm on individuals and erode the foundational trust between citizens and their government. The current paradigm, where law enforcement relies on opaque algorithmic outputs without meaningful oversight, is incompatible with the constitutional guarantees of due process and equal protection. The *Tripartite Joint Adjudication Model* offers a pragmatic, constitutionally sound pathway forward. By establishing a permanent, professional framework that unites technical expertise, regulatory oversight, and civil rights advocacy, this model transforms AI governance from a reactive process of litigation and settlement into a proactive system of accountability. It does not seek to halt the use of AI, but to ensure that when AI is deployed in high-stakes government decisions, it serves as a tool for justice, not a source of its denial. Cheong contends that legislative frameworks must mandate transparency requirements, accountability mechanisms, and multi-stakeholder oversight, the three pillars embedded in the tripartite joint adjudication system. For the United States, the path forward is clear. Legislative action at both the state and federal level is required to mandate this framework. Such legislation must define the qualifications of each professional cohort, establish clear procedural rules for tripartite panels, grant them binding authority, and create a public registry of AI systems used by government to ensure transparency. This is not merely a regulatory burden; it is a necessary investment in democratic resilience. Only by embedding accountability into the architecture of AI governance can we harness the immense benefits of this technology while safeguarding the fundamental rights that define American society.

References

[1] Kumar, A., et al. (2025). Algorithmic accountability and the future of public security.

[2] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

[3] Ballweber, A. (2026, March 19). Attorney outlines potential lawsuit plans after AI led to wrongful arrest of Tennessee grandmother. Valley News Live. https://www.valleynewslive.com/2026/03/19/attorney-outlines-potential-lawsuit-plans-after-ai-led-wrongful-arrest-tennessee-grandmother/

[4] Butler, M. (2025). AI in law enforcement: Accuracy, bias, and civil rights implications.

[5] Dikos, A. (2025, October 22). Teen detained after AI system mistakes chips for weapon outside Kenwood High School. WBFF Fox Baltimore. https://foxbaltimore.com/news/local/teen-detained-after-ai-system-mistakes-chips-for-weapon-outside-kenwood-high-school

[6] Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6, 1421273.

[7] Mucci, T., & Stryker, C. (2024, October 10). AI governance. IBM Think. https://www.ibm.com/think/topics/ai-governance

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group

Open Access

This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



Copyright © 2026 The Authors. All individual papers remain the copyright of their respective author(s) · Published by Zeus Academic Research Publishing Group