Ethics of Cloud-Based AI in Predictive Policing and Surveillance in Authoritarian Regimes

Emmanuel Idowu *

Posted Date: 17 July 2025

doi: 10.20944/preprints202507.1358.v1

Keywords: cloud computing; artificial intelligence; predictive policing; surveillance; authoritarian regimes; ethics; human rights; privacy

 doi:10.20944/preprints202507.1358.v1

Article

Ethics of Cloud-Based AI in Predictive Policing and Surveillance in Authoritarian Regimes

Emmanuel Idowu

Independent Researcher, Nigeria; babm5730@gmail.com

Abstract

This study explores the ethical implications of deploying cloud-based artificial intelligence (AI) technologies in predictive policing and surveillance systems within authoritarian regimes. As governments increasingly leverage AI hosted on cloud infrastructures to enhance security operations, concerns over privacy violations, human rights abuses, and unchecked state power intensify, especially in contexts with limited democratic oversight. This research critically examines the ethical challenges posed by such technologies, analyzing the tension between state security objectives and individual freedoms. Through a comprehensive review of existing literature and case studies, the study identifies key risks associated with cloud-based AI in surveillance and proposes ethical guidelines and policy recommendations to mitigate harm. The findings aim to contribute to the development of responsible AI governance frameworks that balance technological innovation with respect for human rights in authoritarian settings.

Keywords: cloud computing; artificial intelligence; predictive policing; surveillance; authoritarian regimes; ethics; human rights; privacy

1. Introduction

The integration of artificial intelligence (AI) with cloud computing has revolutionized the capacity of modern surveillance systems, enabling real-time data processing, storage, and predictive analytics at an unprecedented scale. Among the most prominent applications of these technologies is **predictive policing**, which utilizes algorithmic models to forecast potential criminal activity based on historical and real-time data. While such innovations promise increased efficiency and crime prevention, their implementation raises significant ethical concerns—particularly when adopted by **authoritarian regimes**, where transparency, accountability, and civil liberties are often suppressed.

Authoritarian states have increasingly adopted cloud-based AI surveillance tools not only to manage security concerns but also to exert social control. The centralization of citizen data, combined with algorithmic decision-making, can lead to surveillance overreach, racial or political profiling, and suppression of dissent. Unlike democratic societies, where civil institutions and public oversight may impose checks on surveillance practices, authoritarian regimes often deploy these tools without meaningful oversight, making ethical scrutiny even more urgent.

Despite growing attention to AI ethics in general, there remains a significant gap in understanding the **specific ethical dilemmas posed by cloud-based AI used for surveillance and policing in nondemocratic contexts**. Most existing frameworks focus on technical bias, data privacy, or algorithmic transparency in liberal democracies, overlooking the broader socio-political dynamics in authoritarian environments.

This study aims to address this gap by examining the ethical dimensions of cloud-based AI in predictive policing and surveillance within authoritarian regimes. It asks critical questions: *What ethical risks emerge when cloud-based AI technologies are employed in surveillance by authoritarian governments? How do these technologies impact fundamental rights and civil liberties in such contexts? What ethical frameworks can guide the responsible development and deployment of these systems in politically repressive environments?*

 doi:10.20944/preprints202507.1358.v1

Through a multidisciplinary approach that incorporates political ethics, human rights law, and AI governance, this research seeks to advance ethical discourse and offer practical recommendations for mitigating harm. The ultimate objective is to foster responsible AI practices that are sensitive to context, especially where democratic accountability is limited or absent.

2. Literature Review

The literature on AI ethics, cloud computing, surveillance, and predictive policing has expanded significantly over the last decade, reflecting growing global concerns about the societal impacts of advanced technologies. However, much of this scholarship is rooted in democratic contexts and fails to fully capture the ethical stakes when these technologies are deployed in authoritarian regimes.

2.1. Cloud-Based AI in Predictive Policing and Surveillance

Cloud computing has enabled AI systems to scale rapidly by offering high-capacity data storage, distributed computing, and real-time analytics. In policing and surveillance, cloud-based AI facilitates the integration of diverse datasets (e.g., biometric records, geolocation data, social media activity) to identify patterns of behavior and predict criminal activity. Studies by Ferguson (2017) and Joh (2020) highlight the growing reliance on AI-driven surveillance infrastructure in law enforcement agencies, noting both the efficiency gains and the potential for abuse, especially where data governance is weak.

2.2. Ethical Frameworks for AI and Surveillance

Scholars such as Mittelstadt et al. (2016) and Floridi et al. (2018) have developed ethical principles to guide AI development, including fairness, accountability, transparency, and respect for autonomy. In the context of surveillance, Lyon (2007) and Zuboff (2019) emphasize the need to protect privacy and civil liberties against the backdrop of the "surveillance society." However, these ethical guidelines often assume the presence of democratic oversight, legal recourse, and civic engagement—all of which are lacking in authoritarian regimes.

2.3. Surveillance in Authoritarian Regimes

Authoritarian governments use surveillance not just for public safety but as a mechanism for political control and social repression. Reports from Human Rights Watch and Freedom House document extensive use of facial recognition, social credit systems, and internet monitoring in countries like China, Iran, and Saudi Arabia. These regimes leverage cloud-based platforms to centralize and automate surveillance, making dissent riskier and more easily detectable. Scholars such as Morozov (2011) argue that authoritarianism has evolved through "digital authoritarianism," where technology becomes a tool of oppression rather than empowerment.

2.4. Predictive Policing and Bias

There is robust literature on the dangers of algorithmic bias in predictive policing. Studies by Lum and Isaac (2016) and Angwin et al. (2016) demonstrate that predictive algorithms often replicate and amplify existing social inequalities, disproportionately targeting marginalized communities. These biases are particularly dangerous in authoritarian settings, where legal protections are minimal and there is often no mechanism for appeal or correction.

2.5. Gaps in the Literature

Despite extensive research on AI ethics and surveillance, there is a lack of focused investigation into the **combined role of cloud infrastructure, AI-driven policing, and authoritarian governance**. Most ethical discussions do not account for the political environment in which these technologies

 doi:10.20944/preprints202507.1358.v1

operate. Moreover, policy proposals and frameworks often fail to address how technologies should be evaluated or restricted when deployed by regimes that systematically violate human rights.

3. Methodology

This study adopts a **qualitative, exploratory research design** aimed at critically examining the ethical implications of cloud-based AI technologies used in predictive policing and surveillance within authoritarian regimes. The complex interplay between technology, governance, and human rights necessitates a multi-layered approach grounded in ethical analysis, political theory, and technology studies.

3.1. Research Design

A **case study methodology** is employed to provide contextual depth and specificity. The research investigates selected authoritarian regimes where cloud-based AI surveillance systems are known to be in operation (e.g., China, Iran, and Russia). These cases are chosen for their documented use of advanced AI surveillance tools and their relevance to ongoing human rights discussions.

3.2. Data Collection

Data is drawn from multiple sources to ensure triangulation and richness of analysis:

1. **Academic Literature** – Peer-reviewed journals on AI ethics, surveillance studies, political science, and law.
2. **NGO and Human Rights Reports** – Publications from Amnesty International, Human Rights Watch, Freedom House, and the United Nations.
3. **Government and Corporate Disclosures** – Policy documents, procurement records, and technical whitepapers from AI companies operating in these regions.
4. **Media and Investigative Journalism** – Reports from reputable news organizations covering surveillance practices and ethical breaches.
5. **Expert Interviews** *(if applicable)* – Conversations with scholars, ethicists, or human rights lawyers familiar with digital authoritarianism.

3.3. Analytical Framework

The analysis applies **normative ethical frameworks** such as:

- **Deontological ethics** – to evaluate duties and rights regardless of outcomes.
- **Utilitarian ethics** – to assess overall harms and benefits of surveillance programs.
- **Rights-based approaches** – to examine violations of fundamental rights like privacy, autonomy, and freedom of expression.

A **thematic content analysis** is conducted across the data to identify recurring ethical concerns, mechanisms of control, and potential safeguards.

3.4. Scope and Limitations

- The study focuses exclusively on state-driven applications of predictive AI policing in authoritarian regimes.
- It does not evaluate technical efficiency but rather the ethical and political consequences of these systems.
- Due to the sensitive nature of surveillance practices, direct access to certain data may be limited; reliance on secondary sources is acknowledged.

4. Results / Findings

This section presents key findings from the case study analysis and ethical evaluation of cloud-based AI applications in predictive policing and surveillance across selected authoritarian regimes.

 doi:10.20944/preprints202507.1358.v1

The results are organized around four core ethical themes: **privacy violations**, **political repression**, **algorithmic bias**, and **lack of accountability and oversight**.

4.1. Erosion of Privacy and Autonomy

In all studied cases, the use of cloud-based AI enables unprecedented levels of mass surveillance. Governments deploy tools such as facial recognition, gait analysis, and social media monitoring powered by real-time cloud analytics. In China, for example, the **Integrated Joint Operations Platform (IJOP)** aggregates personal data—including biometric, financial, and behavioral inputs—to flag "suspicious" individuals. These systems operate without consent, transparency, or meaningful limits, thereby **eroding personal autonomy and violating international norms on the right to privacy**.

4.2. Reinforcement of Authoritarian Control

AI-enhanced surveillance is not merely a tool for crime prevention—it is a mechanism of **political control and intimidation**. In Iran and Russia, data from surveillance feeds is often linked to law enforcement databases and used to monitor political opponents, journalists, and protest organizers. Predictive models flag individuals not necessarily based on criminal activity, but on association patterns and past behaviors, which authorities interpret as preemptive threats. This leads to **pre-crime interventions**, arbitrary detentions, and a climate of fear that stifles civic engagement.

4.3. Embedded Bias and Discrimination

Algorithms used in predictive policing are trained on historical data that often reflect **systemic discrimination**. In authoritarian contexts, such biases are compounded by political targeting. For instance, predictive systems in China's Xinjiang region reportedly flagged Uyghur individuals for "pre-criminal" behavior based on cultural and religious practices. Such applications not only reproduce societal biases but **institutionalize ethnic and political profiling** under the guise of neutrality and efficiency.

4.4. Absence of Accountability Mechanisms

One of the most concerning findings is the complete **lack of transparency and accountability**. Authoritarian regimes rarely disclose how AI models are built or used, nor do they offer appeals processes for those affected. Because these systems are hosted on cloud platforms, often with international tech company support, the locus of responsibility becomes blurred. Victims have little to no legal recourse, and even foreign governments or companies involved face minimal consequences due to opaque contracts and cross-jurisdictional barriers.

4.5. International Complicity and Cloud Infrastructure

Findings also indicate that **international cloud providers and AI vendors**, knowingly or unknowingly, facilitate these surveillance regimes. While some companies have pulled out of controversial markets, others continue to provide the infrastructure necessary for real-time tracking and mass data storage. This raises urgent questions about **corporate ethical responsibility and complicity in human rights violations**.

5. Discussion

The findings reveal profound ethical challenges associated with the deployment of cloud-based AI in predictive policing and surveillance systems within authoritarian regimes. This section contextualizes those findings within relevant ethical theories and explores their broader implications for governance, corporate responsibility, and international norms.

5.1. Ethical Evaluation Through Normative Frameworks

 doi:10.20944/preprints202507.1358.v1

From a **deontological perspective**, the use of AI surveillance without consent, transparency, or due process is inherently unethical. Authoritarian regimes routinely violate individuals' rights to privacy, free expression, and movement. Regardless of outcomes or claimed benefits, the absence of individual autonomy and informed consent makes such practices morally indefensible.

A **utilitarian analysis** might argue for maximizing public safety through predictive policing. However, in the cases examined, the **harms significantly outweigh potential benefits**. The systems produce widespread fear, social control, and discrimination while offering limited verifiable gains in crime prevention. Moreover, the chilling effects on society—especially among political dissidents, minority communities, and activists—undermine the collective well-being.

Using a **rights-based approach**, it becomes clear that these systems threaten core human rights enshrined in international law, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Cloud-based AI in these contexts becomes a tool not for justice but for oppression, surveillance, and silencing of dissent.

5.2. Surveillance, Technology, and Power Consolidation

The implementation of predictive policing in authoritarian contexts is not a neutral or technocratic exercise—it is **deeply political**. These systems enable regimes to expand and automate their surveillance apparatus, embedding technological control into the everyday lives of citizens. This technological infrastructure consolidates power and **reduces the ability of civil society to challenge the state**.

Moreover, the shift to cloud platforms further empowers these regimes by allowing centralized, scalable, and remotely controllable surveillance. The **global nature of cloud infrastructure** complicates jurisdiction, regulation, and transparency, making it harder to hold governments and private corporations accountable.

5.3. Corporate Ethics and Global Technology Markets

Multinational technology firms that provide cloud and AI services face ethical dilemmas when operating in authoritarian environments. While profit motives and legal compliance drive their actions, **ethical responsibility transcends legality**. Firms that enable surveillance abuses risk becoming complicit in human rights violations. Voluntary principles such as the **UN Guiding Principles on Business and Human Rights (UNGPs)** urge companies to conduct human rights impact assessments and avoid contributing to abuses, yet enforcement is weak and inconsistent.

5.4. The Need for Context-Sensitive Governance

Conventional AI ethics frameworks—developed largely in liberal democracies—often assume the presence of rule of law and civil oversight. These assumptions break down in authoritarian regimes. **Ethical AI governance must be adapted** to account for environments where checks and balances are absent. New approaches should focus on:

- Red lines for deployment (e.g., bans on real-time facial recognition).
- Transparency mandates for cloud service providers.
- International regulation and sanctions for technology misuse.

5.5. Toward Responsible AI Practices

To mitigate these ethical risks, a multipronged strategy is needed:

1. **Policy reform** at the international level to define and prohibit certain AI surveillance practices.
2. **Corporate accountability** measures such as supply chain audits, human rights due diligence, and stakeholder engagement.
3. **Civil society engagement** to build public awareness and demand transparency.
4. **Research and advocacy** to develop global norms for AI and surveillance in high-risk political contexts.

 doi:10.20944/preprints202507.1358.v1

6. Conclusion

The deployment of cloud-based AI in predictive policing and surveillance by authoritarian regimes presents a profound ethical dilemma at the intersection of technology, governance, and human rights. This study has demonstrated that while such technologies offer enhanced state capabilities in crime detection and public monitoring, they are often weaponized in ways that infringe on fundamental freedoms, entrench political power, and erode civil liberties.

Key findings highlight that these systems frequently operate with minimal transparency or accountability, rely on biased data, and disproportionately target vulnerable or dissenting populations. Far from being neutral tools, AI and cloud computing in these contexts serve as enablers of digital authoritarianism. Traditional ethical frameworks—such as deontological, utilitarian, and rights-based approaches—unanimously expose the incompatibility of these surveillance systems with core moral and legal principles when deployed without consent, oversight, or redress.

The role of international technology firms further complicates the ethical landscape, as cloud infrastructure providers and AI developers may inadvertently support repressive state practices. These actors must be held to higher standards of responsibility through enforceable ethical guidelines and regulatory mechanisms.

Moving forward, it is essential to recognize that **ethical AI governance cannot be one-size-fits-all**. It must be sensitive to political context and include proactive safeguards against abuse. A combination of international legal reforms, corporate accountability, and civil society activism is required to curb the misuse of cloud-based AI in policing and surveillance.

Ultimately, this research underscores the urgent need for **contextual ethics and global cooperation** in regulating AI technologies. Left unchecked, these systems risk accelerating the decline of democratic values and entrenching authoritarianism under the guise of technological progress.

References

1. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine bias: There's software used across the country to predict future criminals. And it's biased against Blacks.* ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
2. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement.* NYU Press.
3. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
4. Freedom House. (2021). *Freedom on the net: The global drive to control big tech.* https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech
5. Human Rights Watch. (2019). *China's algorithms of repression: Reverse engineering a Xinjiang police mass surveillance app.* https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass
6. Joh, E. E. (2020). Policing by numbers: Big data and the Fourth Amendment. *Washington Law Review, 94*(2), 559–582.
7. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
8. Lyon, D. (2007). *Surveillance studies: An overview.* Polity Press.
9. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2). https://doi.org/10.1177/2053951716679679
10. Morozov, E. (2011). *The net delusion: The dark side of internet freedom.* PublicAffairs.
11. United Nations. (1966). *International Covenant on Civil and Political Rights.* https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

 doi:10.20944/preprints202507.1358.v1

12. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.
13. Islam, R., Rivin, M. A. H., Sultana, S., Asif, M. A. B., Mohammad, M., & Rahaman, M. (2025). Machine learning for power system stability and control. Results in Engineering, 105355.
14. Ahmed, K. R., Islam, R., Alam, M. A., Rivin, M. A. H., Alam, M., & Rahman, M. S. (2024, September). A Management Information Systems Framework for Sustainable Cloud-Based Smart E-Healthcare Research Information Systems in Bangladesh. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-5). IEEE.