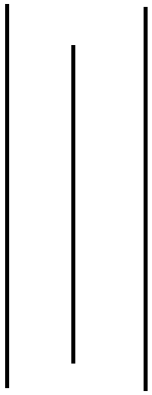
REPORT

AI Surveillance and Facial Recognition: Balancing Public Safety with Civil Liberties

Course: 5CS037 – Concepts and Technologies of AI



Name: Bhawanath Sapkota

Student ID:2513314

Group: L5CG4

Module Leader: Siman Giri

Tutor: Ayush Regmi

Abstract

Artificial intelligence (AI) surveillance and facial recognition systems are being adopted by the government and institutions in order to improve public safety and administrative efficiency. Although the adoption of AI surveillance has many advantages, there are many serious ethical and legal challenges associated with this technology. Issues such as privacy invasion, threats to civil liberties, lack of transparency, and misuse of personal data have become central to debates on responsible AI use. This report explores the ethical implications of AI-enabled mass surveillance and facial recognition in public spaces. It examines challenges related to consent, accountability, and discrimination, while also considering how public safety objectives can be balanced with individual rights. The report reviews key national and international initiatives that promote ethical AI practices and proposes a general ethical framework aimed at ensuring that AI surveillance technologies protect human rights while supporting societal well-being.

Keywords: AI surveillance, facial recognition, privacy, civil liberties, ethical AI

Introduction

Artificial intelligence has significantly transformed modern surveillance practices. AI-powered systems, including facial recognition and automated video analytics, are now commonly deployed in public spaces such as airports, streets, shopping centers, and transport hubs. Governments and institutions often justify these technologies by highlighting their potential to improve public safety, prevent crime, and enhance operational efficiency. As a result, AI surveillance has become an increasingly visible part of everyday life.

Nevertheless, the increasing use of AI in the surveillance of people has sparked numerous debates concerning ethics and society. Among the most pressing concerns related to the applications of artificial intelligence is the effect it may have on the right to privacy. The permanent surveillance in public areas might lead individuals to feel as if they are being closely watched all the time, thus affecting freedom of expression and assembly. Different human rights agencies have acknowledged the effect that excessive surveillance may have on human rights such as the right to privacy and freedom of expression (United Nations Human Rights Council Report, 2021).

Ethical norms have a crucial role to play in such a context. International frameworks lay down fairness, transparency, accountability, and human review as some of the most important aspects of ethical AI, according to UNESCO in the year 2021. In high-risk domains, such as surveillance, ethical norms play a crucial role in ensuring that AI developed functions in a human and democratic way.

It is therefore important for AI surveillance to be governed well. If this is not done, it will be possible to misuse AI technology in a manner that challenges human rights. Ethical and legal aspects relating to AI surveillance should therefore be incorporated into technology in order to ensure that human rights are not violated despite technological advancements.

Thematic Review: Key Ethical Challenges and Emerging Debates in AI Surveillance

Mass Surveillance and Human Rights Concerns

AI-abled mass surveillance lets authorities track large populations via cameras connected through data analytics systems. While such systems may support crime prevention and emergency response, they raise serious concerns regarding human rights. Large-scale data collection often occurs without meaningful consent, increasing the risk of privacy violations. International human rights frameworks highlight that indiscriminate surveillance can weaken individual autonomy and democratic participation (United Nations Human Rights Council, 2021). It may also promote self-censorship, in which people adjust their actions based on the threat of observation.

Real-time Facial Recognition in Public Spaces

Facial recognition technology has increasingly been deployed in public space to enable real-time identification and monitoring. Although it can assist law enforcement, its use raises ethical concerns related to fairness and proportionality. Reports have highlighted that facial recognition systems may disproportionately affect

certain communities, increasing the risk of discriminatory practices when safeguards are insufficient (UNESCO, 2021). Errors in identification can result in unjust surveillance or wrongful suspicion, particularly when these systems are used without adequate oversight.

Consent, transparency, and misuse by Corporations or governments

One ethical issue that is pertinent regarding AI-powered surveillance is a lack of transparency and consent. In fact, people are often oblivious about when a surveillance system is running or how their private data is being collected and stored. The absence of clear public communication and accountability mechanisms increases the risk of misuse by governments or corporations. International guidelines emphasize that transparency and accountability are essential to prevent the abuse of surveillance technologies and to maintain public trust (OECD, 2019).

Balancing Public Safety with Civil Liberties

AI-based surveillance technology can increase public security through the detection of crimes and rapid response to emergencies. However, the use of the technology must be considered in relation to the protection of the rights of the people. In order to be used effectively, it is important that any form of surveillance exercised is carried out under the principles of legality, necessity, and proportionality as far as the threats are concerned, for which the states target to reduce (United Nations Human Rights Council, 2021).

National & International Initiatives

The ethical development and control of AI is ensured by a number of international initiatives. Respect for human rights, accountability, and openness are all included in the UNESCO Recommendation Regarding the Ethics of Artificial Intelligence (UNESCO, 2021). In order to achieve equitable growth and societal well-being, the OECD AI Principles promote responsible innovation in AI (OECD, 2019). Facial recognition is regarded as a high-risk field by the European Union's Artificial Intelligence Act, which offers strict regulations to prevent abuse in this domain (European Union, 2023). Finally, the NIST AI Risk Management Framework offers recommendations for mitigating artificial intelligence-related risks during the course of the system's life cycle (NIST, 2023).

Proposed Generic Ethical AI Framework

A general ethical AI framework for surveillance systems should include the following principles:

- **Fairness:** Measures to prevent bias and discriminatory outcomes
- **Transparency:** Clear communication about how and why surveillance systems are used
- **Human Oversight:** Meaningful human control over high-risk decisions
- **Accountability:** Defined responsibility for AI-driven outcomes and misuse
- **Sustainability:** Consideration of long-term social trust and societal impact

Discussion / Personal Reflection

While researching AI surveillance and facial recognition, I realized how closely technology is connected to human rights. Although these systems can improve public safety, they can also cause serious harm when used without clear rules and safeguards. One insight that stood out to me was how easily surveillance technologies can affect ordinary people in their daily lives. For example, when I see CCTV cameras and facial recognition systems in shopping centers or public transport areas, I often wonder how my data is being collected, who has access to it, and whether I have any real control over its use.

This research helped me understand that ethical concerns around AI surveillance are not just theoretical but closely linked to real-world experiences. A major concern is that when transparency and accountability are weak, surveillance technologies can be misused without the public even being aware of it. Ethical AI practices are therefore essential to ensure that these systems serve the public interest rather than undermine trust and personal freedom. Overall, this study reinforced the idea that responsible AI development is not only a technical challenge but also a social responsibility. In the long term, ethical AI can support safer and more inclusive societies, while unethical deployment risks increasing fear, inequality, and the loss of civil liberties.

References

European Union (2023) *The Artificial Intelligence Act*. Brussels: European Commission. Available at: https://artificialintelligenceact.eu (Accessed: 10 January 2026).

National Institute of Standards and Technology (NIST) (2023) *AI Risk Management Framework*. Gaithersburg, MD: NIST. Available at: https://www.nist.gov/itl/ai-riskmanagement-framework (Accessed: 10 January 2026).

OECD (2019) *OECD Principles on Artificial Intelligence*. Paris: Organization for Economic Co-operation and Development. Available at: https://www.oecd.org/going-digital/ai/principles/ (Accessed: 10 January 2026).

UNESCO (2021) *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization. Available at: https://www.unesco.org/en/artificial-intelligence/ethics (Accessed: 10 January 2026).

United Nations Development Programme (UNDP) (2022) *Human Development Report 2022*. New York: UNDP. Available at: https://hdr.undp.org (Accessed: 10 January 2026).

United Nations General Assembly (2021) *Artificial Intelligence and Human Rights*. New York: United Nations. Available at:https://www.un.org/en/ai-advisorybody (Accessed: 10 January 2026).

United Nations Human Rights Council (2021) *The Right to Privacy in the Digital Age*. Geneva: United Nations Office of the High Commissioner for Human Rights. Available at: https://www.ohchr.org/en/special-procedures/sr-privacy/right-privacy-digital-age (Accessed: 10 January 2026).