

LmunA 2026

Research report

Forum: Third General Assembly

Issue: Establishing International Standards for the Use
of Artificial Intelligence in Surveillance and
Human Rights Protection

Student Officer: Annika Maassen van den Brink

Position: Main chair GA3



LMUNA

Lorentz Lyceum
Model United Nations
Arnhem

Introduction

The rapid development of **artificial intelligence (AI)** has completely transformed the way governments, law enforcement agencies, and private organisations collect, analyse, and use information. One of the most useful and outstanding purposes of AI is its use in **surveillance**, allowing authorities to monitor individuals and populations on any scale. An example of such authority could be China, which monitors its population with cameras equipped with facial recognition. No country epitomizes the scale or intrusiveness of AI surveillance like China, where facial recognition is intertwined with the state's pervasive monitoring of daily life. Cameras are embedded in public and private spaces, from transport hubs to toilets, feeding data into systems used to track dissidents and ethnic minorities, notably Uyghurs, under the guise of maintaining public order. The system is tightly integrated with China's evolving social credit infrastructure, incentivizing "compliant" behavior and punishing dissent.

The relationship between AI-driven surveillance and **human rights** is particularly complex because surveillance technologies can directly affect several basic human rights. The right to privacy, for example, may be threatened when governments use facial recognition systems, biometric databases, location tracking, or other AI-based technologies to monitor individuals without their knowledge or meaningful consent. At the same time, extensive surveillance can have consequences for the freedom of expression, freedom of peaceful assembly, freedom of association, and freedom of movement. Individuals who know or believe that they are being constantly watched may be less willing to participate in political demonstrations, communicate controversial opinions, or engage in activities that are essential to a democratic society. Consequently, the impact of AI surveillance extends beyond **privacy** and can influence the broader exercise of civil and political rights.

It is a central issue in determining whether AI surveillance is compatible with human rights. Surveillance should not automatically be considered legitimate simply because it may improve security or assist authorities. Any interference with fundamental rights should have a legitimate logic behind it and should be necessary to that logic. This requires authorities to consider whether less intrusive alternatives are available and whether the expected benefits of surveillance justify its potential impact on individual rights. In this context, preventing AI surveillance from abusing basic human rights is an important principle for preventing excessive or unjustified surveillance.

This research report examines the question of how international standards for AI-based surveillance can be established while ensuring effective human rights protection. It explores the opportunities and risks associated with AI surveillance and analyses the legal and ethical principles that should not be looked over in its use. The report also considers the challenges of creating internationally consistent rules in a rapidly developing technological world. While these technologies can contribute to crime prevention, national security, border control, and public safety, their increasing use also raises serious concerns regarding human rights, privacy, discrimination, accountability, and the rule of law. The lack of (consistent) international rules

LmunA 2026

that regulate these technologies creates an urgent need to establish clear and uniform international rules for the use of AI in surveillance and the protection of human rights.

Definitions of key terms

Algorithm

A precise, step-by-step procedure or set of rules followed by a computer or calculator to solve a mathematical problem or complete a specific task in a finite number of steps.

Artificial Intelligence (AI)

The use or study of computer systems or machines that have some of the qualities that the human brain has, such as the ability to interpret and produce language in a way that seems human, recognize or create images, solve problems and learn from data supplied to them.

Human Rights

The basic rights to fair and moral treatment that every person is believed to have. Examples are right for healthcare, right for privacy and right for public speech.

Privacy

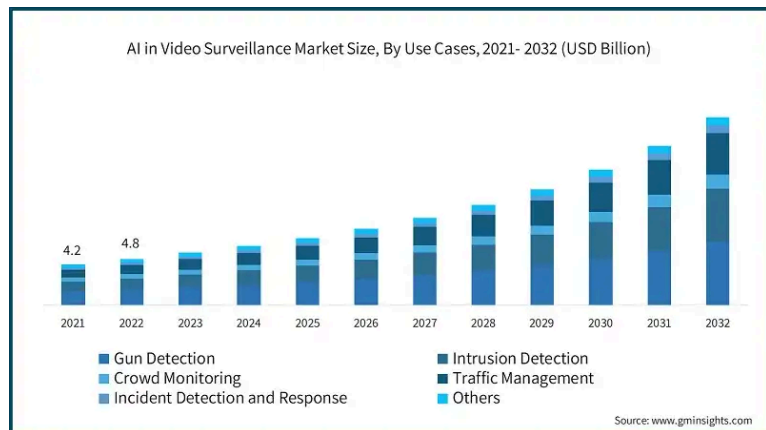
the right of people to choose what information about themselves they share with others, and to be free from uninvited monitoring or interference.

Surveillance

The careful watching of a person or place, especially by the police, army or government, because of a crime that has happened or is expected.

General overview

The use of AI is growing rapidly, and it does not plan to stop growing. According to *Global Market Insights*, the growth of AI in video surveillance is increasing every year, which means that it becomes a larger topic of discussion every year. Artificial Intelligence is a system that can be used for various things. Many members of generation Z and Y think of Chat GPT, which can create humanly written texts based on all available information on the internet.



However, one of the most important uses is surveillance. AI-powered surveillance technologies could include facial recognition, biometric identification, predictive policing, automated decision-making, and large-scale data analysis. These technologies are developing rapidly, causing them to offer more opportunities and dangers.

The biggest difficulty is AI-powered surveillance overstepping human rights. The most immediate threat is the mass, non-consensual invasion of privacy; AI systems continuously monitor entire populations, biometric facial recognition, precise location logs, and social media data to eliminate public anonymity and compile permanent digital dossiers on innocent citizens. Because AI models are trained on historical datasets that often reflect deep societal prejudices, facial recognition tools exhibit dangerously high error rates for racial minorities and women, directly causing disproportionate policing, wrongful accusations, and false arrests. This automated profiling completely ignores the core legal presumption of innocence, forcing ordinary citizens to actively defend themselves against automated machines. When individuals know they are being constantly watched, analyzed, and categorized by **algorithms**, they consciously change or watch their everyday behavior, which effectively suppresses open freedom of expression, can scare people from protesting which violates political activism, and dismantles the right to peaceful assembly due to the fear of being watched. AI surveillance radically alters the state-citizen dynamic, systematically eroding civil liberties in favor of automated, authoritarian social control.

Another major concern is the potential for algorithmic bias and discrimination. AI systems are trained using large datasets, and these datasets can contain existing social, racial, gender, or socioeconomic biases. As a result, surveillance systems may disproportionately identify, monitor,

LmunA 2026

or classify certain groups. Facial recognition technology, for instance, has raised concerns about differences in accuracy between demographic groups. When such systems are used by law enforcement or other state authorities, inaccurate or biased results can have severe consequences, including wrongful identification, unjustified police intervention, or discriminatory treatment. This demonstrates that the use of AI in surveillance is not merely a technological issue but also a question of equality and non-discrimination, both of which are fundamental principles of international human rights law.

The rapid development of AI also creates significant challenges concerning accountability and transparency. Many AI systems operate through complex algorithms that are difficult for individuals, and sometimes even authorities, to understand. This lack of transparency can make it difficult to determine why an individual was targeted, classified, or subjected to surveillance. The concept of explainability is therefore increasingly important: individuals affected by AI-assisted decisions should, where appropriate, have access to meaningful information about how those decisions were made. Furthermore, clear mechanisms for human oversight, responsibility, and remedy are necessary to ensure that governments and organisations cannot avoid responsibility by attributing harmful outcomes to an algorithm. Effective accountability requires identifiable decision-makers, independent oversight, auditing mechanisms, and accessible procedures through which individuals can challenge unlawful or harmful surveillance.

Right now, the international opinions differ extremely. Different countries and regions have adopted varying approaches to AI regulation, data protection, surveillance, and human rights. While instruments such as international human rights treaties and emerging AI governance frameworks provide important principles, significant differences remain in how these principles are interpreted and enforced. This fragmentation creates the possibility of regulatory gaps, particularly when AI surveillance technologies are used across national borders or by actors operating in jurisdictions with weaker safeguards. Establishing international standards could therefore provide a common framework based on universally recognised principles while allowing states to address legitimate concerns relating to national security and public safety.

However, establishing such standards involves a difficult balance between security and individual liberty. States have a legitimate responsibility to protect their populations from terrorism, organised crime, cybercrime, and other threats. AI technologies can assist governments in fulfilling these responsibilities more efficiently. Nevertheless, security measures must remain subject to human rights protections and the rule of law. International standards should therefore not seek to prohibit all forms of AI surveillance, but rather establish clear boundaries concerning when, how, and under what conditions such technologies may be used. Particular attention should be given to high-risk applications, including real-time biometric identification, predictive policing, mass surveillance, and automated profiling. This is why it is an urgent matter to create international regulations about the use of AI powered surveillance.

LmunA 2026

Major parties involved

China

Acts as the world's leading developer and exporter of state AI surveillance. Also houses several of the biggest companies that supply AI surveillance worldwide .

United States of America

Has invested over 471 Billion USD in AI, Which makes it the country that has committed the most in investing in ai. Also houses “*Clearview AI*”, which maintains a controversial facial recognition database.

Taiwan

sits at a critical chokepoint in the AI compute stack, producing roughly 90% of the world’s most advanced logic chips. The concentration is often described as Taiwan’s “silicon shield” for its strategic global importance.

United Kingdom

Pioneers heavy urban CCTV integration coupled with advanced live facial recognition trials by police forces and houses major AI safety and monitoring infrastructures.

European Union

Currently debating about the topic of AI powered surveillance, and one of the first to pass rules for AI: “the AI pact”.

LmunA 2026

Timeline of Key Events

1956	Artificial intelligence was founded as an academic field at the Dartmouth Workshop, where the term "artificial intelligence" was coined.
2014	AI-powered voice assistants and facial recognition technology, Amazon introduced " <i>Alexa</i> ".
2014	Japan installed the first outdoor street surveillance.
2022	<i>Open AI</i> made " <i>Chat GPT</i> " publicly available, which resulted in the increase of public recognition and popularity of AI.
2024	The European Union passes the AI Act, restricting high-risk surveillance tactics like real-time biometric tracking and predictive policing.

Previous attempts to solve the issue

The most aggressive attempt to solve the issue was the "European Union's AI Act". The Act completely prohibits untargeted scraping of CCTV footage to build facial recognition databases, bars emotion recognition in workplaces, and bans real-time biometric tracking in public spaces (barring narrow law enforcement exceptions). Despite its strength internally, human rights organizations have criticized the EU AI Act because it does not prohibit EU-based tech firms from exporting highly invasive, banned AI surveillance systems to non-EU countries, creating structural human rights gaps abroad. The reason that this attempt at solving failed was because surveillance tech companies frequently operate transnationally, dodging local regulations by registering or testing their algorithmic models in countries with weak privacy protections.

The U.S. Department of State is releasing a "Risk Management Profile for Artificial Intelligence and Human Rights" (the "Profile") as a practical guide for organizations, including governments, the private sector, and civil society, to design, develop, deploy, use, and govern AI in a manner consistent with respect for international human rights. When used in a rights-respecting manner, AI can propel technological advances that benefit societies and individuals, including by facilitating enjoyment of human rights. However, AI can be applied in ways that infringe on human rights unintentionally, such as through biased or inaccurate outputs from AI models. AI can also be intentionally misused to infringe on human rights, such as for mass surveillance and censorship. International human rights are uniquely valuable to AI risk management because they provide an internationally recognized, universally applicable normative basis for assessing the impacts of technology. However, human rights are not always familiar to those involved in AI design, development, deployment, and use, and there is a gap in translating human rights concepts for technologists. This is a good start point to resolve the issue, but it fails to resolve the issue completely.

LmunA 2026

Possible solutions

Ban the most harmful uses. Governments can prohibit mass biometric surveillance, untargeted facial recognition, and AI systems that predict whether someone is likely to commit a crime based only on personal profiling. The EU AI Act already prohibits several such practices and places strict limits on real-time biometric identification.

Require necessity and proportionality. Surveillance should only be used when there is a clearly defined and legitimate purpose, when less intrusive alternatives are inadequate, and when the expected benefit justifies the intrusion into people's rights.

Keep humans responsible for important decisions. An AI-generated match or risk score should not by itself lead to arrest, punishment, denial of rights, or other serious consequences. Human decision-makers should independently verify the evidence. EU rules, for example, restrict adverse law-enforcement decisions based solely on certain biometric-identification outputs.

Improve transparency. Governments should disclose when surveillance AI is being used, what its purpose is, what data it processes, how long data is retained, and what safeguards exist. Independent researchers should be able to scrutinize systems where possible.

Minimize and protect data. Collect only information necessary for the specific purpose, retain it for the shortest reasonable period, restrict access, and securely delete it afterward. This reduces the risk of surveillance data being repurposed for unrelated monitoring.

Give people meaningful remedies. People should have ways to find out whether they have been subjected to unlawful surveillance, challenge automated decisions, correct inaccurate information, and obtain compensation or other remedies when their rights have been violated.

LmunA 2026

Further reading

1. <https://www.gminsights.com/industry-analysis/ai-in-video-surveillance-market>
2. <https://youtu.be/dQw4w9WgXcQ?si=FawocEVy4mNk0o7q>
3. <https://www.franklintempletonglobal.com/articles/2026/etf/where-global-economies-sit-in-the-ai-stack>
4. <https://ennhri.org/ai-resource/key-human-rights-challenges/>

Bibliography

1. <https://www.omnilert.com/blog/ai-surveillance-benefits-applications-and-future-potential>
2. <https://dictionary.cambridge.org/dictionary/english/ai>
3. <https://www.gminsights.com/industry-analysis/ai-in-video-surveillance-market>
4. <https://www.franklintempletonglobal.com/articles/2026/etf/where-global-economies-sit-in-the-ai-stack>
5. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12438284/>
6. <https://www.tech.gov.sg/technews/the-history-of-ai-part-1/>
7. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
8. <https://www.undp.org/eurasia/blog/when-ai-governs-who-guards-our-rights>
9. <https://impactpolicies.org/news/553/ai-and-surveillance-are-reshaping-global-human-rights-protections-rapidly>
10. <https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/>