MSI Journal of
Multidisciplinary Research (MSIJMR)

ARTIFICIAL INTELLIGENCE, SURVEILLANCE AND THE NEED FOR THE GLOBAL HUMAN RIGHTS FRAMEWORK

Ariba Dar[1*]

[1*] 5th Year Law Student, PULC, University of Punjab, Lahore.

*** Correspondence:** Ariba Dar

The authors declare that no funding was received for this work.

OPEN ACCESS

Received: 10-April-2026
Accepted: 30-April-2026
Published: 06-May-2026

Copyright © 2026, Authors retain copyright. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/4.0/ (CC BY 4.0 deed)

This article is published in the **MSI Journal of Multidisciplinary Research (MSIJMR) ISSN 3049-0669 (Online)**

The journal is managed and published by MSI Publishers.

Volume: 3, Issue: 5 (May-2026)

ABSTRACT: Various forms of AI technology, most notably in surveillance applications, are crucial in the transformation of societies across the globe, creating significant and complex challenges for human rights. State and non-state actors utilise AI-enhanced surveillance technologies, in the form of facial recognition software and predictive analytics, to monitor individuals with little or no legal protections. This system violates different rights like right to privacy, freedom of expression and other rights. The paper critically addresses the crossroads of the AI-based surveillance and the international human rights law and discusses why a cohesive global system, based on the notion of cross-border solidarity should be established. Civil society and international mechanisms are advocating an integrated international system of governance of AI. As an example, the 2021 Recommendation on the Ethics of AI by (UNESCO) adopted by 193 countries expressly forbids mass surveillance via AI and points to data protection and individual rights. Equally, the new Framework Convention of the Council of Europe provides a binding set of regulations to guarantee that AI systems comply with human rights and democracy and the rule of law. By using the comparative case studies of the facial-recognition infrastructure in China or predictive policing in the United States and data privacy regimes in the European Union, the paper finds the most

significant areas in which AI surveillance violates privacy, freedom of expression, equality and autonomy. The research claims that it is only a consistent, universal human rights system constructed on international solidarities that can be sufficient to ensure human security in the era of AI surveillance. There is an urgent need of such a mechanism that serves humanity and protect its fundamental freedom. Different proposals and recommendations have been given for the development of Global Human Rights Framework.

Keywords: *Artificial Intelligence, surveillance, human rights, global governance, international solidarity*

Introduction

Artificial Intelligence (AI) is defined as computer science that focuses on the development of systems that can execute tasks that are normally performed by intelligent humans. These activities are learning, reasoning, problem-solving, perception, language understanding, decision-making and autonomous action. AI represents a convergence between mathematical models, algorithms, massive data processing, and computing power to allow machines to simulate and/or enhance the human mental process. The use of artificial intelligence technology infiltrates all aspects of our lives, whether it be making travel arrangements or giving instructions to an autonomous vehicle, or even simply giving us our morning news. Not only do governments utilise artificial intelligence when making decisions, but the same can be also found in many business sectors (UNESCO, 2021). There are also threats posed by AI such as possible disinformation, lack of data security and copyright violations. Besides, AI has no boundaries in this respect, the principles provide an international working base and interoperability with direction that would be able to withstand time in the rapidly changing environment of AI (OECD, 2019). In the paper, the increasing interrelation between AI-driven surveillance and human rights will be introduced. It will dwell upon the ways in which cutting- edge technologies are transforming surveillance on an international level and the reason as to why it poses dire human-rights issues. Artificial intelligence has significantly contributed to the civilisation in the face of algorithms and machine learning models, or robots and autonomous systems. One of the most important uses of artificial intelligence is

enhancement of surveillance and monitoring. The Global Surveillance Index (GSI) notes that 75 out of the 176 countries in the world are making serious investments in surveillance using artificial intelligence (AI) and are actively implementing the concept in their respective countries, specifically in smart cities, facial recognition, and smart police (Saheb, 2022). The technologies establish both unprecedented individual community, and movement scale monitoring, and change the nature of power between institutions and citizens, essentially overturning the human rights pillars of privacy rights, rights to speech, rights to assemble, and individual rights. Moderation of platforms which are supported by AI may end up silencing genuine expression that are not even outlawed by the law in hate speech and other types of expressions that are unlawful. Indeed, AI systems cannot perceive context and nuance of speech, and the application of bots really opens new opportunities of misuse. In addition, systems, whose algorithms are designed in an addictive manner, or whose designs form an echo chamber like some social media platforms can impact the power to make choices and decisions without coercion or manipulation. After all, this also influences democratic participation and free flow of information. Besides, on top of the human rights issues, AI has a significant impact on human dignity overall. The effects of surveillance technologies on the structure harm the ideas of human autonomy, human agency, self-governance and self-determination. Meanwhile, emotional recognition technologies are also a threat to the dehumanisation of a person who has been reduced to a statistical figure without intrinsic value and dignity (European Network of National Human Rights Institutions, n.d.) The paper sheds light on the urgency of the intersection of artificial intelligence-driven surveillance technologies and international human rights law, showing that legal frameworks are not sufficient to combat the complexity and magnitude of today surveillance practices. Through analysing three groundbreaking case studies, including the Chinese system of facial recognition intertwined with social credit systems, the algorithms behind predictive policing in the US, and the rules of human rights protection in the European Union, the study can pick up several structural patterns of human rights abuses, as well as note the alternative regulatory acts of their own. The discussion shows that the idea of cross-border solidarity and transnational principles based on which a fully developed system of human rights

governance should be built can be the only sufficient solution to safeguard the persons during the days of AI surveillance (Gstrein & Beaulieu, 2022; Murray & Fussey , 2019; Prabhakaran, Mitchell, Gebru & Gabriel , 2022). The article explores the impacts of AI-equipped surveillance on human rights across the world and why a global human rights approach is required. We overlay (a) important technologies and applications of AI surveillance, (b) the harms they cause to human rights, (c) policy responses on the national and global levels. We also evaluate new global governance ideas of AI Ethics recommendation by *UNESCO, UN resolutions and AI treaty by the Council of Europe* and suggest that a universal and solidarity-oriented strategy is the only one that can prompt AI to address the issue of human dignity globally. The paper claims that the solution to this issue is the creation of the binding international governing mechanisms, which should not regard technology development as the primary objective but focus on human security, and make sure that AI surveillance systems do not contradict the principles of human rights and international law.

Literature Review

The swift development of the artificial intelligence (AI) has contributed to the emergence of more intensive surveillance tools, which allowed not only the state but also non-state actors to follow people on an unconventional scale. Face recognition technology, as well as biometric identification and predictive policing systems, are gradually being installed in the streets, in controls of borders, and law enforcement. These systems are effective and secure but, scholars highlight that at the same time, such systems also introduce deep threats to basic human rights, such as the right to privacy, freedom of expression, or equality (Negri et al., 2024).

Focusing on the marginalised groups, the literature has also noted that AI surveillance is highly disproportionate, which contributes to the disparities and adds more risks on misidentification, targeting and exclusions caused by the surveillance of marginalised communities (Almeida et al., 2021; Zuwanda et al., 2024). The pivotal impact of pervasive surveillance on people is also the so-called chilling effect, whereby people adjust their behaviours or self-censorship out of fear of getting spied on all the time, compromising its freedom of expression and identity formation (Matar and Murray, 2025). The lack of cohesive approach to regulation is

a very acute problem as AI technologies begin to permeate the fabric of our society. As an example, the General Data Protection Regulation (GDPR) by the European Union (EU) includes data privacy principles in their entirety, as well as specific provisions addressing AI, including the right to explanation however most other countries do not have a similar overall regulation (Kashefi et al., 2024). They have suggested HRIAs to evaluate the human rights impact of AI systems; nevertheless, in practice, so far, it is intermittent and underdeveloped (Mantelero & Esposito, 2024).

According to scholars, there should be a global human rights framework for AI surveillance given its transnational nature, which may have impact on fundamental rights. This framework would co-ordinate protections of privacy, accountability and non-discrimination across borders, and guarantee control over both private as well as state actors and provide remedies that are enforceable (Kashefi et al., 2024; Council of Europe, 2024). An international strategy seems to be viewed as a necessary measure to make sure that the positive aspects of the AI should not impose a cost on human dignity, freedom, and equality.

Methodology

Here the paper's research design and methods are described. The methodology will likely be *a comparative case study and normative legal analysis*. One example of qualitative comparison of three examples of AI surveillance practices (China facial recognition infrastructure, U.S. predictive policing, EU data protection/AI regulation) is presented, as well as a description of sources of data (ex: laws, policy document, non-governmental organization reports, academic research, news coverage), and some analysis framework (such as a human rights impact assessment framework). As an illustration, it may be done systematically by reviewing each case to find indications of legal protections and violations of the rights. The methodology ought to as well articulate whatever theoretical lens (e.g. concept of international human rights law and solidarity) and why such cases are chosen as demonstrative examples. This section can list restrictions (e.g. use of secondary sources) and explain the reason why a qualitative approach would be suitable to conduct a conceptual study of norms and policies.

Rise of AI Driven Surveillance

• Scope and Scale

AI surveillance technology is increasingly being used worldwide to monitor public places, manage urban security systems, and collect data about people. As reported by *Carnegie Endowment for International Peace (2019), 75 out of 176* countries are deploying AI-enabled technology for surveillance, which includes smart-city platforms, facial recognition and policing analytics, as per *AI Global Surveillance Index* (Feldstein,2019). According to the data, AI surveillance is not limited to high-tech states. Instead, it occurs in democracies, hybrid regimes as well as autocracies. The technologies used for surveillance have global application which makes surveillance an important part of the modern government.

• Technology Trends in AI Surveillance

The surveillance systems powered by AI represent the continuum of technology that enhances the ability of officials to identify individuals, calculate trends, and predict behaviours. *Facial recognition technology (FRT)* was one of the most ubiquitous systems used, and is capable of real-time face detection, feature extraction, and matching faces in biometrical rich databases. Studies indicate that there has been considerable improvement in accuracy over the last ten years, and has been deployed in airports, public streets, and law-enforcement scenarios (Fadel, 2025).

Along with facial recognition, AI surveillance encompasses behaviour-analysis applications detecting events automatically like population rushes, loitering, suspicious local motion or objects left unattended. These systems can be used to categorize new behaviours using pattern- recognition algorithms that have been trained on a simulation of large datasets with their processing anomalies. With similar sophistication, predictive-policing algorithms analyse established crime and historical data to make predictions about the probability of crime in particular locations, or even who will be most at risk of wrongdoing. This is a type of system that is being developed and implemented by governments, especially in authoritarian environments, to track the actions of people, as well as detect potential security risks (Hillman, 2021).

• Democratic VS Authoritarian Use

Although AI surveillance is on the rise in all political systems, the use of such tools operates out of different frameworks between democratic and authoritarian regimes. AI surveillance in majoritarian states promotes primary devices of political regulation, social administration, and repression. China is the exemplary case to provide such a demonstration with vast technologies like a facial recognition camera network, citizen-scoring systems, and integrated datasets that track subjects across many spheres of life (Hillman, 2021). These systems are used relate to minority social management, dissenting voices, and political unrest predictions. China has also exported this technology to other countries, further entrenching its power to surveil and control its people and providing technology that serves to surveil and control the populace in other countries.

On the other hand, democratic states tend to use AI surveillance through an association with legal frameworks, public debates, and human rights. Democrats have communication with AI concerning border control, security, and effective governance, but its application is linked with a court ruling, civil-society regulation, and even data protection legislation. Indicatively, the Freedom Online Coalition, which consists of 39 nation-states, presented an international Guiding Principles on Surveillance Technology that contains provisions on transparency, necessity, proportionality and safeguarding of rights and liberties. Nonetheless, there are concerns that even the democratic states, if left unregulated, lead to mission creep, loss of privacy, and disproportionate targeting of marginalised groups, among other negative implications.

Human Rights Implication of AI Surveillance

The wide scope application of AI surveillance challenges fundamental human rights. *The Universal Declaration of Human Rights* and the *ICCPR* have ensured the right to privacy (*Article 12 UDHR/ICCPR 17*), freedom of expression, assembly, and equality before the law among others. Nonetheless, AI technologies tend to violate all these rights: all-time surveillance kills the privacy and anonymity right, algorithmic content censoring threatens free speech, artificial intelligence can choose the wrong suspect, and racial algorithms can alienate a person.

- **Right to Privacy**

  Right to Privacy is guaranteed under the *International Human Rights Law* but AI Surveillance poses a serious threat to this right. The obligation to respect to the right of privacy and security of digital communication is included in *Article 17* of the *International Covenant on Civil and Political Rights*. The State is not allowed to interfere in the right of the individuals to share information and ideas with each other (Bennett, 2014). Another issue is surveillance at workplaces. AI-powered systems have the capability of monitors employee conduct 24/7 through cameras, key-stroke tracking, or behavioural points, grossly infringing upon personal freedom and privacy. Malik (2025) goes on to claim that this type of policing kills off the freedom of individuals and infringes the dignity of individuals. When implemented in a responsible manner, such as inclusive development AIs can positively contribute to more effective social and political participation and enhanced delivery of services to the population; however, when applied without proper governance and openness, they present a tremendous threat to human rights and other basic freedoms, such as the freedom of expression, freedom of assembly, freedom of association, and freedom of belief or religion, and their privacy rights (Freedom Online Coalition , 2025). *The UN High Commissioner of Human Rights* has requested heavy protective measures citing the fact that unscrutinised digital surveillance will destroy privacy in the open and closed contexts.

- **Freedom of Expression and Assembly**

  Surveillance by AI also poses a threat to the freedom of speech and assembly. Since people are aware that they may be detected, trailed, and filmed on the spot, they might start self- censoring, they might feel like not expressing themselves or they might not attend political meetings. It has been cautioned by the *Council of Europe* that AI-enhanced biometric surveillance and behaviour tracking may contravene *Article 10 (expression)* and *Article 11 (assembly)* of the *European Convention on human rights (ECHR)* as it would erode group anonymity as well as deter participation in the process (Steering Committee for Human Rights, 2025). In theory, this menace is not a hypothesis. *Human Rights Watch* records that facial- recognition cameras are used in dictatorial regimes, including Russia and Iran, to find out

protestors, suppress dissent, and silence political speech. The threat to fundamental freedoms is evident: facial recognition surveillance system is equivalent to mass surveillance. It compromises privacy rights and interposes rights to freedom of expression and freedom of assembly (Stroehlein, 2023).

• Non-Discrimination and Equality

One fundamental human rights issue of AI surveillance is algorithmic bias. Most facial recognition systems, predictive-police code and profiling applications are taught to operate on historical biases and therefore they have an imbalanced number of minorities or marginalised groups (i.e. racial minorities, the poor) to falsely identify or target. These discriminatory systems may be prejudiced against the principle of non-discrimination *(ICCPR Article 26 or ECHR Article 14)*. An example can be found on the Council of Europe, which has directly warned the state about the risk of discrimination during the use of AI-based surveillance and requested them to reduce any form of algorithmic bias. *The Toronto Declaration*, when applied to the machine-learning setting, also highlights the overall threat posed by unfairness and discrimination to mind AI systems, warning against the need to implement practices that protect the right to equality and non-discrimination in AI systems.

Opponents, however, allege that there is little transparency from agencies that operate predictive policing programs, and they highlight several civil rights and civil liberties concerns about the algorithms, including the potential for the algorithms to exacerbate racial biases in the criminal justice realm. Opponents further claim that independent audits of the programs have contributed to leading police agencies, including those in Los Angeles and Chicago, to discontinue or reduce the use of their predictive policing programs after independent audits (Lau, 2020).

• Other Rights

Other fundamental rights in addition to privacy, expression and equality could also be impacted by AI surveillance. With automated profiling systems, *the freedom of movement* is limited when people are indicated as being risky or suspicious depending on their biometrics or behavioural information. Reports also suggest that such systems can also disrupt the people to congregate to worship or participate in

political actions in a repressive environment where the profiling is being done on some *ethnicity or religion* (Steering Committee for Human Rights, 2025).

Transnational Nature of AI Surveillance

AI surveillance is not border respecting. Internet portals, cloud services and cross-country data flows imply that the data gathered in one nation can be done in another country. An algorithm of facial recognition invented in a certain country can be spread into the rest of the world using cameras; even social media analysis software can track people around the world. AI knows no borders (OECD, 2019). Indicatively, the database of face images offered by Clear view AI is open to clients located on all corners of the world. The data of the company, which was scraped on web sources, incriminates millions of people who represent a wide range of countries. Similarly, the governments of other countries have been monitoring activists and disseminating disinformation using social media content analysis tools produced by U.S. or European firms. International surveillance networks (e.g. data exchange in allied intelligence civilizations) equally overcome national restrictions.

Such an international aspect requires solidarity: the abuse of AI in a single area can affect persons in other parts of the world. There is a risk that data privacy violations may target the diaspora communities; discriminative AI models in a particular culture are going to be a disadvantage to the minority population in a different area. The shared values and principles will stand to implement the required legal infrastructure to support the healthy development of AI (UNESCO, 2021).

Current Policy Responses at National and Regional Level

While many governments and institutions have begun to address the issue of AI surveillance, they have not responded in any coordinated fashion.

• United Nations and Global

The UN has brought up professional teams. UN Secretary General António Guterres said *"We need to build an open, dynamic, and efficient international AI structure obligatory AI governance on the basis of international standards and values, such as human rights"*. The issues raised by Turk are a tidal crush into the AI sector that can

create more undesired issues of misinformation, election propaganda and discrimination faster than the sector can control. Robots have overwhelmed challenges of human rights to be observed by companies and countries in the creation of AI, which are mostly failing (Ashar, 2024). In addition, in collaboration with other agencies, UNESCO spearheaded the development of the first international AI Ethics standard, *Recommendation on the Ethics of AI*. This Recommendation (*consented to by 193 states*) specifically outlaws AI systems on social scoring and mass surveillance and makes protection of human rights and dignity central to it.

Successfully addressing AI governance is one of the most critical social challenges of our time, requiring multilateral learning based on the lessons and good practices arising from the varied contexts of practice in several jurisdictions worldwide (UNESCO,2021).

• Council of Europe

The first sort of legal binding treaty would be The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which would be opened on 5 September 2024, and that would seek to ensure that all activities throughout the lifecycle of artificial intelligence systems are entirely accommodating to human rights, democracy, and the rule of law and help lead to progress and innovation (Council of Europe Framework, 2024). By 2025, more than *eleven countries* (to include G7 countries and EU states) have ratified the Convention. In essence, the Convention indicates that all AI activities during their lifecycle will respect rights, fill legal gaps arising from rapid technological developments, and remain technology neutral.

• European Union

The European Union has established a comprehensive and leading regulatory framework. Currently, the General Data Protection Regulation protects the personal data and bans the biometric surveillance unless permitted. The proposed European Union Artificial Intelligence Act, which was proposed in 2021 and is now at the finalisation stage, categorises biometric surveillance as either being high risk or

prohibited in many domains. The European Union law will be supplemented with the Council of Europe Framework Convention that will underline international norms.

• Other Countries

Numerous nations are developing artificial intelligence strategies (China seeks to become the leader in AI, while still implementing state-based surveillance; India has a personal data protection bill under consideration; African and Latin American countries have policies that are developing, albeit in nascent stages). Nonetheless, there are few national-level AI strategies that include a restriction on human rights. One analysis recently revealed, "few" AI strategies mentioned or even acknowledged human rights as important terms, which left vast gaps globally.

Case Studies Illustrating Global Risks

• China's Surveillance State

China shows that monitoring on AI can be scaled to an ordinary tool of social control. The Chinese state has installed cameras with facial-recognition and other sensors in transport centres and on the sidewalks and courtyards of the population, which directly feed into databases and other social-security initiatives, according to which a person can be identified, tracked and profiled in real time (Human Rights Watch, 2019). Human-rights groups state that they have been employed to escalate surveillance and extreme limitations of ethnic minorities (e.g., Uyghurs), and they threateningly state that the integration of widespread sensors, low procedural protections, and a lack of transparency in purchasing and limited accountability assures a significant likelihood of systemic human-rights violations, such as abuses of privacy, freedom of movement, freedom of assembly and non-discrimination (Human Rights Watch, 2019).

• Digital Authoritarianism in Democracies

The use of AI surveillance is not restricted in any way to authoritarianism; instead, both democracies and commercial products have witnessed troubling implementation and technological offerings that undermine privacy or civic zone. Law enforcement and third-party actors have utilised commercial biometric companies to develop

massive image databases raising legal and ethical issues in the United States and within the rest of Europe. Cases such as the Clear view AI, in which a company scraped billions of pictures of the internet to form a database of faces to be searched have caused a series of data-protection enforcement proceeding and fines in the tens of millions of dollars under the EU General Data Protection Regulation (GDPR) (Impact International , 2025) . It proves that democratic law-enforcement mechanisms are nonetheless still grappling with effective regulations of cross-border and company-led surveillance (CNIL/EDPB actions). These instances demonstrate that such instances of private public combining of surveillance can put the civil liberties of citizens at risk unless democratic institutions enhance supervision, openness and legal limits (EDPB, 2022; Privacy International, 2021). The U.S. presents a mixed picture. On one hand, there's robust civil society pushback and some state laws limiting biometric surveillance (e.g., Illinois' Biometric Information Privacy Act). On the one hand, this can be checked by the strong civil society opposition and even state legislations on biometric surveillance restrictions (e.g., Biometric Information Privacy Act of Illinois). Conversely, massive data brokers, commercial predictive policing sellers, and risk-assessment software (COMPAS in criminal justice) have proven to be discriminatory and secretive (Angwin et al., 2016).

- **Global Covid 19 Surveillance**

Governments have implemented computer AI to cameras, video management software, and mobile phones together with technology companies and institutionalised biometric monitoring of pandemics, including the current world COVID pandemic. Some are of the view that incorporating AI based surveillance technology has been a game changer however others criticise the fact that surveillance technologies based on artificial intelligence have unforeseen or desired negative consequences especially on the life of citizens and their potential to help enforce anti-democratic policies and abuse the principles of privacy and human rights (Saheb , 2022). Some of the digital tools had provided insightful epidemiological data, but most of the deployments had brought acute privacy and human-rights issues. Most of the applications in use or under consideration have an

impact on individual privacy that democratic societies would normally consider to be unacceptably high (Bengio et al., 2020). There have been a number of privacy issues linked to the contact tracing apps as the apps are actually monitoring information such as the location of the users and their interactions with others Experimental surveys have shown the unwillingness of citizens to share data because they are concerned with their privacy (Afroogh et al., 2022). Digital contact tracing applications have been experiencing problems; lack of high penetration of mobile phones, absence of user adoption, and privacy concerns among others (Shahroz et al., 2021).

• Transnational Data Surveillance (e.g. Google, Facebook)

Transnational technology platforms accumulate and aggregate personal information in large amounts (including geographic location tracking, profile pictures, communications made on social media, etc.) and create detailed user profiles through the information collected that allows the corporation to effectively advertise, recommend products, and optimise engagement with users. Through this method of extracting user data for corporate gain, referred to as *surveillance capitalism*, there are extraterritorial privacy implications since many of these global companies do business in multiple countries (or are based in) and therefore may be subject to being forced (or paid) to supply user data to state or private entities (Zuboff, 2019).

• Middle East and North America and Pegasus style spy-ware

Another example of the vectors used is commercial spyware (e.g. NSO Group Pegasus): targeted system compromise and devices are used to spy on journalists, activists, and opposition activists. Such tools are applicable in eavesdropping communications and tracking device location-threatening press freedom, confidentiality and safety of civil society participants. The governments have used such spyware against dissidents, and these spywares were revealed by investigations, thus the calls to impose export limits and bans.

• Global South and Transnational Diffusion of Surveillance Tech

Capacity limitations in the ability to regulate complex technologies and defend rights in the virtual domain are an issue faced by many Global South countries. Such an

unequal division presents the opportunity of creating digital colonialism in which data and other surveillance technologies are organised by rich nation corporations and foreign states (Couldry and Mejias,2019).

Gaps and the need for the Unified Global Framework

• Fragmentation of Rules

The existing frameworks of AI regulatory frameworks across the world are highly fragmented, as nations choose to take different approaches towards it, which are uneven or partial. Most states, especially with less technological power, possess poor or old AI legislation that cannot follow the fast innovation. Several nations within the Global South have procured foreign AI surveillance systems from leading geopolitical institutions without being granted full access to source codes, algorithm parameter settings, or rights to the management of data (Abiade,2025).

• Cross Border Challenges

Cooperation between states is required to prevent cross-border harms from AI deployment, including surveillance and algorithmic decision-making. This relationship establishes a kind of digital clientelism, in which recipient countries can be reliant on the technological ecosystem of the vendor state (Abiade, 2025). Social media websites, cloud services, and data analytics AI providers regularly handle data across national boundaries, making them difficult to account for and oversee. Artificial intelligence surveillance is frequently implemented in multiple jurisdictions, and this use raises some doubts about the legality and security of privacy (Saheb, 2022). Because of abuses between states, particularly in the context of internationally established surveillance systems, global solidarity and concerted government is an immediate necessity. The cooperation between states is necessary to ensure that harms of AI implementation on cross-border basis such as surveillance or algorithmic decision-making do not occur (Council of Europe, 2024).

• Unequal Impact

The Global South is particularly vulnerable to countries with structural inequalities, low regulatory capacities and relying on AI surveillance systems built by other countries. The use of foreign-constructed AI surveillance platforms has been adopted

in many states (Abiade, 2025). People of colour experience the unequal exposure to surveillance technologies and involvement in the policymaking process (John et al.,2025). Unless ethics and human rights are explicitly incorporated into the creation and implementation of AI technologies, they run the risk of recreating the historical biases. States and organisations need to make sure that all the stakeholders, especially those who are underrepresented, are included in AI governance systems (UNESCO,2021).

• Enforcement and Accountability Gaps

The absence of a unified enforcement mechanism can be considered as one of the biggest challenges of the present AI governance. Although there are many national regulations, ethics codes and even statements, there is no world organisation that has the authority to enact compliance, control cross-border harms, and even obligate actors, whether they are states or individual companies to violations. The solution to these shortcomings is the creation of a single and enforceable international system. The suggested AI, Data, and Human Rights Convention (which is proposed to be called the Munich Convention on AI, Data, and Human Rights) is one such effort to adopt a framework. The necessity of a unified and binding international framework it is namely due to the lack of binding, universal obligations in the current governance practice (Alexander Kriebitz and Caitlin C. Corrigan, 2025). Additionally, the absence of a universal enforcement tool leaves states free to adopt human rights protection selectively, implement poorly or avoid it, due to the preference given to national sovereignty or economic gains. This relationship is detrimental to cross-border or multinational AI operations. Consequently, there is an immediate necessity to seal these accountability loopholes with creating a single global framework preferably a binding international treaty establishing minimum standards on transparency, protection of data, non-discrimination, user rights (including explanation, remediation, and right to opt out) as well as cross-border cooperation to enforce.

Why is a Unified Global Framework Needed?

There has been an initiative by international organisations like UNESCO, OECD, and the UN under AI. But their activities are usually isolated and non-authoritative.

There is no international organisation that governs AI globally and has universal policies to exercise authority and enforce the same (Santos, n.d). The utilisation of AI, it is dangerous especially in such critical areas as criminal justice, healthcare, finance and public policy. The ethical issues are necessary to solve to make sure of the responsible development and utilisation of the AI technology to support fairness, responsibility, and human rights respect (Ghoshal,2025). Considering the above-mentioned gaps and challenges, a global framework with a unified approach, based on human rights and coordinated across the jurisdictions, would have the following advantages:

1. *Uniformity and legal predictability:* A common set would minimise regulatory arbitrage, give minimum protection in any location, and would make compliance easier by developers and companies operating on an international scale.

2. *Equity and inclusion:* An international framework, created through collaboration with various areas (including Global South, marginalised groups, indigenous communities) might provide AI governance with a variety of propositions and promote digital solidarity.

3. *Human rights protection:* An international regulated framework of AI can promote the protection of fundamental rights (privacy, non-discrimination, access to remedy, autonomy) by ensuring the protection of human rights globally.

4. *Sustainable global collaboration to govern AI:* As AI technologies data supply chains, computer infrastructure, deployments are augmented with international borders, international cooperation is the only way to effectively manage risks and ensure fair benefits.

Challenges in Achieving Global Framework

1. Diverging National Interest

- **Geopolitical Competition and Technological Advantage**

AI is regarded as a source of a strategic, economic, or military advantage in various states. This renders them unwilling to give up regulatory independence or embrace

binding global standards which may hamper their competitive advantage. In addition to regulating technological advancements, AI governance should also consist of ethical standards, risk management methods, accountability mechanisms and institutions that promote harmonisation of differing national interests. Key areas of tension in AI include geopolitical competition; differences in regulatory capabilities; Digital Sovereignty; Ethical Pluralism; and Uneven Distribution of Technological Power (Khatoon et al.,2025). Due to this reason, states can oppose international norms that constrain their regulatory freedom or even denominate their ability to use AI in national interests - building an institutional barrier to a prospective, enforceable human-rights- based system of AI surveillance.

2. Corporate Power and Global Tech Industry Influence

The creation and implementation of AI is highly concentrated in few tech firms worldwide and developed economies. This is an imbalance of power which makes these actors have excess influence not only technically and economically, but also politically. The current governance paradigms are centred on compliance and risk management, and tend to be technical and operative in nature, i.e. performance, accuracy, and scalability. Nevertheless, such technical orientation may eclipse fundamental ethical issues such as fairness, transparency and inclusiveness (Batool et al., 2023). Due to such a structural imbalance that is characterised by a privatised company established not only the technology but even the norms, such efforts at establishing an actual global, human-rights based AI surveillance model are sabotaged in their preliminary stages by corporate control over norm-setting, standards of deployment, and compliance regimes.

3. Enforcement Difficulty and Technical Opacity

One of the biggest obstacles to AI surveillance accountability and regulation is the complexity and obscurity of AI systems. According to the research on governance, most of the currently existing regulatory activities do not address key questions concerning who is responsive, what matters are governed, when governance is present, and how compliance is observed and only a small part of the AI governance studies offer a full-scale response to all of these queries (Batool et al., 2023). It

implies that the governance is in fragments and unfinished and considerable loopholes exist in the ethical regulation and the protection of human-rights. Governance mechanisms often focus on technical and operational compliance, including risk management, performance and scalability, rather than embedding by design human-rights, fairness, or transparency. There is a "principle implementation gap" between ethical principles and the ethical/enforceable/auditable real world (Tidjon & Khomh, 2022).

4. Inequality Between Nations

One of the problems that postpones a universal human-rights system of AI surveillance is the profound and structural disparity among countries in their ability to create, control, or regulate AI what has been termed as a global AI divide. The technological infrastructure, institutions, regulation, human resource capabilities of many countries in the Global South often do not support the development, implementation, or management of advanced AI systems, which place them in a significantly limiting position in establishing global AI governance, and are subjected to AI systems and norms imposed globally that may not respond to local socio-cultural contexts or demands. When it comes to the economically disadvantaged nations, they tend to be financially, politically and technically unable to obtain any efficient AI governance policy, and regulators operating in these regions are grossly underfunded. (World Economic Forum, 2024). Besides, institutional and infrastructural voids are transferred into underrepresentation of global norm and standard setting bodies. According to the argument of the authors of a policy brief, the majority of policies and practices concerning artificial intelligence have been formulated and produced by the Global North - widening the divide between the countries that shape the agenda of global student AI regulation and the countries that are not (LaForge et al., 2024).

Proposals and Recommendations for Global Framework

The growing role of artificial intelligence (AI) in global economies, society, and politics notes the imperative need to have a unified regulatory framework (Ghoshal, 2025).

1. Global Treaty or Convention

One of the more pressing suggestions that is being made by researchers and government officials is a worldwide and binding agreement on AI, information and privacy. The regulatory environment is still disjointed and both, initiatives which are western led and uneven enforcement. A single and enforced international system is badly required to overcome these drawbacks. The so-called Convention on AI, Data, and Human Rights (which is drafted as the Munich Convention on AI, Data, and Human Rights) is one of the attempts at such a framework. It is an international proposal to enable AI governance to stay in line with human rights, as developed through the efforts of more than 50 experts across the world (Kriebitz et al., 2025). The necessity to act is evoked by the growing influence of AI and both the speed of political and technological developmental progress. The UN Human Rights Council (UNHRC) is well placed to be on the forefront of spearheading global debates on an AI governance binding convention, based on human rights. Based on its existing mandate to the enforcement of human rights internationally, the UNHRC has a history of effectively integrating human rights concepts into international systems such as the adoption of United Nations Guiding Principles on Business and Human rights and the acknowledgment of the right to clean, healthy and sustainable environment. By taking specific steps to promote a convention on AI and human rights, the UNHRC can contribute to international agreement and actively develop the future of AI in the way that would give priority to the values and principles contained in the key documents of the international human rights law (Kriebitz et al., 2025). As an example of a possible form of such a treaty, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law by *Council of Europe* is an illustration of how a legally binding treaty governing AI lifecycle activities might look like. Parties to the Convention are bound to make sure that the activities of artificial intelligence systems in the sphere of their lifecycle remain completely centred on the human rights, democracy and the rule of law (Council of Europe, 2024).

2. Principles for Global Solidarity

The foundation of any international agreement or system must be a framework of ethical and human-right principles that govern the States, the private parties as well

as other stakeholders. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) provides such a normative tool at the global level. (UNESCO, 2021). The most important principles inspired by the said Recommendation and capable of underpinning a human-focused global system, are:

- *Fairness and Non-Discrimination:* The AI systems should be free of any biases inside or outside; they should be processes enhancing equity and social justice (UNESCO, 2021).
- *Human Oversight and Agency (Do No Harm):* Humans should still have significant control over the AI decision-making process, particularly, in cases when the decisions have an impact on rights, liberties, or essential interests (UNESCO, 2021).
- *Privacy and Data Protection:* The information in AI systems should be managed in a manner that recognises the right to privacy and data-protection of people (UNESCO, 2021).
- *Accountability and Responsibility:* Developers, deployers, States should be held accountable and responsible in legal and ethical responsibilities of harms caused by applications of AI; it should have institutional controls to check, monitor, and recompense impacts (UNESCO, 2021).
- *Inclusiveness, Justice and Solidarity:* AI governance must encourage equal access and prevent global inequalities; others must benefit and protect low- and middle-income states too (UNESCO, 2021).

Such principles are a big testament to global agreement on the concept of human-centred AI, and they offer normative guidance on which a global treaty can be established and followed (Jobin et al., 2019; UNESCO, 2021).

3. International Cooperation Mechanisms

To turn a global AI treaty into reality, it is necessary to establish international cooperation mechanisms, which will be able to control the adherence, establish a dialogue, and share knowledge. One potential solution is the establishment of a

permanent multilateral forum, possibly through the auspices of the UN, in which the states, the civil society, technical experts, and human rights lobbyists meet on regular basis. It could become a forum that might serve as a "Conference of the Parties" (as in most treaties) to allow periodic review and peer exchange of best practices and coordinate them. Appreciating the importance of nurturing co-operation between the Parties to this Convention and of co-operating with other States whose values it holds in common (Council of Europe, 2024). As a priority, a universal legal system stating of general principles and rules which regulate the operations in the lifecycle of artificial intelligence systems that successfully safeguard shared values and take advantage of some advantages of artificial intelligence to advance these values in a way that is conducive to responsible innovation (Council of Europe, 2024). Further, that there is both movement within the scholarly and policy community toward UNHRC led global governance of AI is evidenced by the fact that already, several international control efforts are underway, including the push to have an international convention on AI and human rights (via the Munich Convention draft).

4. Capacity Building and Inclusive Dialogue

The implementation of a global AI framework, which will observe human rights, can only be successful when every nation, particularly those in the Global South, can engage in a meaningful way. This entails investing in digital infrastructure, technologically, artificially intelligence literacy and advocacy of digital rights. Capacity building and inclusive dialogue should also be the objectives of a human rights based convention. In order to meet the challenges of AI in human rights respect the government, institutions and technology actors need to work together and request that the UN Global Dialogue on AI Governance and the Independent International Scientific Panel on AI incorporate human rights in their mandates, structures, deliberations, priorities and outputs, with large, diverse multi stakeholder participation in all of them, including stakeholders in underrepresented areas and groups(Freedom Online Coalition,2025). While many researchers and practitioners in the field of governance may feel that discussing a global governance framework is not feasible, particularly given the sensitivity surrounding this issue, we feel strongly that, at the very least, an initial effort should be made to conceive of how a global

governance framework could be developed and implemented incrementally. Otherwise, an increasingly competitive relationship between corporations and states could culminate in a zero-sum game, leading to a "race" to the lowest common denominator e.g., lack of social and/or environmental responsibility (Niazi,2024).

Conclusion

The use of AI assisted surveillance is a global cross-border challenge to human-rights. Majority of laws are insufficient since the one world; one struggle requires a combined perspective to protect rights. Artificial intelligence surveillance is presenting unparalleled threats to human rights in all jurisdictions. Case studies of China, American and EU countries shows that uncontrolled use of surveillance technologies may violate the privacy, expression, equality and human dignity (UNESCO,2021). Amongst the most intrusive digital surveillance technologies is the biometric surveillance equipment such as the facial recognition software which allows the government to find and track people in a social environment or isolate them due to their physiological or behavioural traits. These technologies threaten the right to privacy, right to assembly, right to speak, right to religion and non-discriminatory rights (Amnesty International,2020). Existing initiatives, including the ethics recommendation of UNESCO, the GDPR and AI Act of the EU, or the convention of the Council of Europe, are important steps, but are isolated effort. This study insists that universal human rights framework on AI is the only way that human security in AI age is adequately protected. The type of structure would work to align standards (based on tools such as the UNESCO Recommendation and the Council of Europe Convention). It is up to humanity to decide between creating a sound international system of human rights regulation of AI surveillance prior to the stage when surveillance systems become truly universal and omnipresent, or risk the future where people become subject to mass surveillance and the notions of individual privacy, autonomy and freedom are part of the past. The global community needs to devote itself to the creation of binding regulation structures, provision of financial support, empowering the civil society, and putting human rights above the technological growth objectives as well as security concerns.

References

1. Abiade, S. F. (2025). Algorithmic sovereignty and the new security dependencies: How foreign AI surveillance technologies reshape domestic autonomy in the Global South. *World Journal of Advanced Research and Reviews, 27*(2), 162–180. https://doi.org/10.30574/wjarr.2025.27.2.2845

2. Afroogh, S., Esmalian, A., Mostafavi, A., Akbari, A., Rasoulkhani, K., Esmaeili, S., & Hajiramezanali, E. (2022). Tracing app technology: An ethical review in the COVID-19 era and directions for post-COVID-19. *Ethics and Information Technology, 24*(3), 30. https://doi.org/10.1007/s10676-022-09659-6

3. Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics, 2*(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

4. Amnesty International. (2020, September 21). *EU companies selling surveillance tools to China's human rights abusers*. https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/

5. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). *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

6. Ashar, F. (2024, February 19). *U.N. High Commissioner for Human Rights cautions against AI*. The Stanford Daily. https://stanforddaily.com/2024/02/19/un-high-commissioner-for-human-rights-cautions-ai/

7. Batool, A., Zowghi, D., & Bano, M. (2024). *Responsible AI governance: A systematic literature review*. arXiv. https://doi.org/10.48550/arXiv.2401.10896

8. Bengio, Y., Janda, R., Yu, Y. W., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S., & Sharma, A. (2020). The need for privacy with public digital contact tracing during the COVID-19 pandemic. *The Lancet Digital Health, 2*(7), e342–e344. https://doi.org/10.1016/S2589-7500(20)30133-3

9. Bennett, W. (2014, October 15). *U.N. Special Rapporteur report on mass digital surveillance and Article 17 of the ICCPR*. Lawfare. https://www.lawfaremedia.org/article/un-special-rapporteur-report-mass-digital-surveillance-and-article-17-iccpr

10. Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

11. Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

12. El Fadel, N. (2025). Facial recognition algorithms: A systematic literature review. *Journal of Imaging, 11*(2), 58. https://doi.org/10.3390/jimaging11020058

13. ENNHRI. (n.d.). *Key human rights challenges of AI*. https://ennhri.org/ai-resource/key-human-rights-challenges/

14. European Data Protection Board. (2022, October 19). *The French SA fines Clearview AI EUR 20 million*. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

15. Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/publications/79902

16. Freedom Online Coalition. (2025, June). *Joint statement on artificial intelligence and human rights*. https://freedomonlinecoalition.com/joint-statement-on-ai-and-human-rights-2025/

17. Ghoshal, R. (2025). Establishing global ethical standards for AI: A roadmap for regulatory harmonization. *International Journal for Multidisciplinary Research, 7*(2). https://www.ijfmr.com/papers/2025/2/40167.pdf

18. Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology, 35*(1), 3. https://doi.org/10.1007/s13347-022-00497-4

19. Hillman, J. E. (2021, November 17). *Techno-authoritarianism: Platform for repression in China and abroad*. Center for Strategic and International Studies. https://www.csis.org/analysis/techno-authoritarianism-platform-repression-china-and-abroad

20. Human Rights Watch. (2019, May 1). *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-surveillance-app

21. ImpACT International. (2025, July 22). *AI and surveillance are reshaping global human rights protections rapidly*. https://impactpolicies.org/news/553/ai-and-surveillance-are-reshaping-global-human-rights-protections-rapidly

22. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

23. John, A. M., Panachakel, J. T., & Anusha, S. P. (2025). *Navigating AI policy landscapes: Insights into human rights considerations across IEEE regions*. arXiv. https://doi.org/10.48550/arXiv.2504.19264

24. Kashefi, P., Kashefi, Y., & Ghafouri Mirsaraei, A. (2024). Shaping the future of AI: Balancing innovation and ethics in global regulation. *Uniform Law Review, 29*(3), 524–548. https://doi.org/10.1093/ulr/unae040

25. Khatoon, H., Chandio, L. A., & Soomro, Z. H. (2025). AI governance: A challenge for global cooperation. *Journal of Media Horizons, 6*(5), 423–428. https://doi.org/10.5281/zenodo.17309766

26. Kriebitz, A., Corrigan, C., Pevkur, A., Pierok, A., Horzyk, A., Lombana-Diaz, C., Brand, D., Hattoh, D., Daou, F., Crawley, F., Fayad, G., Jaja, I., Tafur, K., Awad, M., O'Sullivan, M., Malcheva, M., Amasiadi, N., Lynch, N., Walker, N., & Cheng, W. (2025). *Promoting and advancing human rights in global AI ecosystems: The need for a comprehensive framework under international law*. ResearchGate. https://www.researchgate.net/publication/389164731_Promoting_and_Advancing_

Human_Rights_in_Global_AI_Ecosystems_The_Need_for_A_Comprehensive_Framework_under_International_Law

27. LaForge, G., Muggah, R., & Seiler, G. (2024, August 28). *Bridging the AI governance divide*. New America & Igarapé Institute. https://www.newamerica.org/planetary-politics/policy-papers/bridging-the-ai-governance-divide

28. Lau, T. (2020, April 1). *Predictive policing explained*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

29. Malik, M. R. (2025). Artificial intelligence and the right to privacy: A human rights dilemma in the age of surveillance. *Dialogue Social Science Review (DSSR), 3*(9), 1–6. https://dialoguessr.com/index.php/2/article/view/950

30. Mantelero, A., & Esposito, M. S. (2024). *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*. arXiv. https://doi.org/10.48550/ARXIV.2407.20951

31. Murray, D., & Fussey, P. (2019). Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data. *Israel Law Review, 52*(1), 31–60. https://doi.org/10.1017/S0021223718000304

32. Negri, P., Hupont, I., & Gómez, E. (2024). *Face recognition: To deploy or not to deploy? A framework for assessing the proportional use of face recognition systems in real-world scenarios*. arXiv. https://doi.org/10.48550/arXiv.2402.05731

33. Niazi, M. (2024). *Universal convention on artificial intelligence for humanity*. Digital Policy Hub Working Paper, Centre for International Governance Innovation. https://www.cigionline.org/static/documents/DPH-paper-Niazi-2.pdf

34. OECD. (2019). *AI principles*. https://www.oecd.org/en/topics/sub-issues/ai-principles.html

35. Prabhakaran, V., Mitchell, M., Gebru, T., & Gabriel, I. (2022). *A human right-based approach to responsible AI*. arXiv. https://arxiv.org/pdf/2210.02667

36. Privacy International. (2021, May 27). *Challenge against Clearview AI in Europe*. https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe

37. Ronit Matar, & Murray, D. (2025). Re-thinking international human rights law's approach to identity in light of surveillance and AI. *Human Rights Law Review, 25*(3), ngaf016. https://doi.org/10.1093/hrlr/ngaf016

38. Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: A social science perspective. *AI and Ethics, 3*(2), 369–379. https://doi.org/10.1007/s43681-022-00196-y

39. Santos, E. A. (n.d.). *Global governance of artificial intelligence*. Diplomacy & Law. https://www.diplomacyandlaw.com/post/global-governance-of-artificial-intelligence

40. Shahroz, M., Ahmad, F., Younis, M. S., Ahmad, N., Kamel Boulos, M. N., Vinuesa, R., & Qadir, J. (2021). COVID-19 digital contact tracing applications and techniques: A review post initial deployment. *Transportation Engineering, 5*, 100072. https://doi.org/10.1016/j.treng.2021.100072

41. Steering Committee for Human Rights. (2025, March 28). *Drafting Group on Human Rights and the Environment (CDDH-ENV)*. Council of Europe. https://rm.coe.int/steering-committee-for-human-rights-drafting-group-on-human-rights-and/1680b50bd2

42. Stroehlein, A. (2023, October 3). *No safe place for your face?* Human Rights Watch. https://www.hrw.org/the-day-in-human-rights/2023/10/03

43. Tidjon, L. N., & Khomh, F. (2022). *The different faces of AI ethics across the world: A principle-implementation gap analysis*. arXiv. https://doi.org/10.48550/arXiv.2206.03225

44. UNESCO. (2021a). *Recommendation on the ethics of artificial intelligence*. https://unesco.org.uk/site/assets/files/14137/unesco_recommendation_on_the_ethics_of_artificial_intelligence_-_key_facts.pdf

45. UNESCO. (2021b, November). *UNESCO adopts first global standard on the ethics of artificial intelligence*. https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence

46. World Economic Forum. (2024). *Generative AI governance: Shaping a collective global future*. https://www3.weforum.org/docs/WEF_Generative_AI_Governance_2024.pdf

47. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

48. Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and legal analysis of artificial intelligence systems in law enforcement with a study of potential human rights violations in Indonesia. *The Easta Journal Law and Human Rights, 2*(3), 176–185. https://doi.org/10.58812/eslhr.v2i03.283