Human Rights & Artificial Intelligence

23rd Informal ASEM Seminar on Human Rights
29-31 October 2025, Copenhagen, Denmark

Concept Note

Artificial intelligence (AI)[i] now affects nearly almost all aspects of our lives. It shapes how people access information, interact with devices and share personal information, but AI also affects as fundamental aspects of our lives such employment, education, housing and credit. While AI offers significant opportunities for development and innovation, it also has wide-ranging impacts on society and poses serious potential risks for human rights, rule of law and democracy. Such risks associated with AI have already begun to compound on top of existing inequalities, resulting in further harm to already marginalised groups [ii] and vulnerable persons.[iii]

The AI used tools and instrument can interfere with fundamental rights such as privacy, equality, non-discrimination and freedom of expression, but with its rapid expansion, AI may have adverse effects on other human rights too. AI tools are increasingly used in child protection situations, making sentencing recommendations in criminal cases, and assessing asylum applications, which can have significant implications on other freedoms and rights established under the international human rights framework. Meanwhile, AI raises a wide range of legal, ethical, and technical issues that cross jurisdictional lines, making them challenging to address and regulate. Additionally, given the complexity of artificial intelligence-based decision-making, the provision of remedy has not been sufficiently established and clarified in situations when AI systems cause harm, losses and injustices.

Concerns about the human rights implications of AI have led to calls for more multistakeholder approach to AI regulation that will apply to both the government and private sectors to govern the application and design of AI technologies.

The United Nations (UN) has been at the forefront of addressing the complex interplay between AI and Human Rights and has, for example, laid a foundational framework for the ethical governance of AI with the **UNESCO Recommendation on the Ethics of Artificial Intelligence** adopted unanimously by all UNESCO member states in 2021. Furthermore, the recent establishment of the **UN High-Level Advisory Body on Artificial Intelligence** marks a significant step forward in the global AI policy that that requires a holistic approach including ethical considerations and human rights. As a further step in protecting human rights in digital age, it has also been proposed to establish a **UN Special Rapporteur on AI and Human Rights** to complement existing efforts and to provide the 'agility, authority and competence required to address emerging challenges.[iv]

In response to the rapid evolution of artificial intelligence, initiatives have also been taken at the national and regional level to address the ethical implications of the use of AI. Several countries are looking into passing national regulations on AI, or setting up specialised agencies to help ensure the development of fair, inclusive, non-discriminatory, safe, secure and trustworthy AI[v] while regionally and at the European Union and Council of Europe levels, binding instruments have been set forth, including **Regulation EU 2024/1689 of the European Parliament and of the Council** of 13 June 2024 laying down harmonised rules on AI and the **Council of Europe's Convention on AI, Human Rights, Democracy and Rule of Law** (2024).

While the new regulatory instruments have the potential to enhance the AI governance and go someway to protecting people from the harms of AI, more could be done to, for example, improve **private sector accountability**[vi] and to strengthen the application of the **UN Guiding Principles on Business and Human Rights** in areas relating to the digital space and new technologies. This is also the case in Asia where governments have hesitated to pursue regionwide rules for AI. For example, at the ASEAN level, the recently agreed **ASEAN Guide on AI Governance and Ethics** (2024) emphasise values and principles for governments and businesses rather than mandating binding measures.[vii] At the same time, however, some of the AI regulation in Asia is exploring new areas of AI policy not yet included in the global discourse, such as indigenous peoples' data sovereignty[viii].

By bringing together key stakeholders from the ASEM Partner countries, academic, civil society, and national human rights institutes, the **23rd Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights** will provide a multistakeholder platform to discuss the challenges and opportunities associated with the interaction of human rights and AI and provide insights into how legal and human rights issues related to AI are being addressed in the Asia-Europe context, focusing notably on privacy, equality, and remedies for harm. It will further aim to identify areas for capacity-building and alliances between different stakeholders working on AI governance and human rights across Asia and Europe and develop recommendations for actions that governments, civil society organisations, national human rights institutes and the private sector can take to ensure that human rights are the foundation for AI governance in future. As an aspiring world leader in responsible and ethical use of AI, Denmark will provide a fitting location for regional discussions on this important and timely topic.

Expected Outcomes

- Increased awareness and understanding of the human rights implications of AI technologies.
- Identification of policy and regulatory gaps and recommendations for an AI governance framework that advances the respect, protection and fulfilment of all human rights.
- Strengthened collaboration between stakeholders to develop inclusive, rights-respecting AI policies and practices.

Target Audience

- Government representatives, policymakers, and regulators.
- Civil society organisations and human rights practitioners.
- Academics, researchers, and AI practitioners.
- Representatives of national human rights institutes and ombudsmen offices.
- Private sector representatives developing and deploying AI technologies.

About the Organisers

The Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights series was launched in 1997 to strengthen relations between civil society actors and governments in Asia and Europe on human rights issues. The Seminar series is co-organised by the Asia-Europe Foundation (ASEF), the Raoul Wallenberg Institute (nominated by the Swedish Ministry of Foreign Affairs), the Philippine

Department of Foreign Affairs, the Swiss Federal Department of Foreign Affairs, and the Ministry of Foreign Affairs of the People's Republic of China, with support of the European Union.

The 23rd Informal ASEM Seminar on Human Rights (ASEMHRS23) is hosted and supported by the Ministry of Foreign Affairs of Denmark.

Working Groups and Cross-Cutting Questions

Participation in the 23rd Informal ASEM Seminar on Human Rights will take place in 3 simultaneous working group discussions (on Day 2) on the following sub-themes:

1. Privacy and Data Protection:

This working group of the Seminar addressing the growing impact of Artificial Intelligence (AI) on privacy and data protection. With AI systems becoming more reliant on vast amounts of data, they are accumulating sensitive personal information, raising significant concerns about privacy breaches and misuse. AI may be used to collect data, including sensitive, personal data, yet it may also be used to create profiles of people based on which decisions can be made regarding issues essential to their lives, such as healthcare, employment, social benefits, and access to justice. By analysing extensive datasets of user information, such as browsing history, social media interactions, AI algorithms[ix] can also generate highly targeted advertising and political messaging that can manipulate and exploit individual vulnerabilities.

While AI holds the potential to revolutionise many sectors by automating tasks and improving decision-making, ensuring a balance between protecting national security and public interest and the safeguarding of privacy is an urgent challenge. It is equally important to recognise that different people may face different privacy concerns when it comes to AI, for instance, people from racially marginalised backgrounds may have heightened human rights concerns when it comes to the right of privacy. Privacy violations can put those groups at risk of ostracisation, discrimination or physical danger.[x]

The right to privacy is a fundamental human right, recognised in Article 12 of the **Universal Declaration of Human Rights,** Article 17 of the **International Covenant on Civil and Political Rights**, and other human rights frameworks[xi]. This right is critical for ensuring a balance of power between the state and the individual and is regarded as one of the cornerstones of democratic societies.[xii] Moreover, as the world becomes increasingly data-driven, the right to privacy is crucial in ensuring that both online and offline human rights are respected and upheld.

The human right to privacy, which applies to all individuals, mandates that personal data be processed in a fair, lawful, and transparent manner, with the consent of individuals or other legitimate legal bases.[xiii] Data should be kept for specific purposes, securely, and retained only for a limited time, with heightened protection for sensitive data. Individuals must know when their data is being processed and have rights to correct, erase, or limit its use.[xiv] Privacy should be protected by the law against arbitrary and disproportionate surveillance and unlimited profiling, and data should not be transferred internationally unless equivalent privacy standards are upheld.

In practice, however, AI systems and businesses often depend on large-scale data collection, including personal data, to optimise services and maximise profits. Companies, particularly in the tech sector, gather vast amounts of information, often through the so-called Internet of Things (IoT)[xv], in both public and private spaces. Data brokers acquire, merge, and sell this data, frequently without full transparency and putting privacy at risk. Despite some existing legal frameworks,[xvi] these data undertakings remain largely unregulated, leaving individuals vulnerable to privacy

violations. A notable example is the Facebook and Cambridge Analytica scandal, where 87 million personal Facebook profiles were collected and used for political advertising without consent between 2013 and 2018. However, this is just one of many privacy breaches that have occurred over the years.

States, as part of their human rights obligation, must refrain from violating the right to privacy and to take active measures to safeguard its enjoyment. This duty is also reflected in the **Guiding Principles on Business and Human Rights**, which emphasise the duty of States to protect against adverse human rights impacts involving private companies. [xvii] However, with the rapid development and adoption of AI tools, keeping track of companies' compliance with human rights is becoming increasingly challenging. The AI regulations are also struggling to keep pace with the rapid changes in technology.

Working group questions:

1) What are the primary **human rights risks** associated with the collection, use, and sharing of personal data by AI systems?
2) Do you think **privacy laws** are currently keeping up with the pace of technological innovation? Why or why not?
3) Are there effective **legal and regulatory frameworks** to protect individual privacy in AI deployment, and where are the gaps?
4) How **transparent** are AI-driven decision-making processes, and how can transparency be improved?
5) Should the **right to have full control over one's own data** be a human right?
6) How can a State balance safeguarding **national security and public interest** with the protection of individual rights, particularly privacy?

2. Equality and Non-Discrimination:

AI typically functions by applying standardised rules to categorise or treat individuals, rather than evaluating each person based on their unique qualities or circumstances. Numerous studies have highlighted the risks that AI and automated decision-making systems[xviii] pose to the principles of equality and non-discrimination - whether in employment[xix], access to goods or services across public and private sectors[xx], public security policies [xxi] or even in prediction the likelihood of individuals committing benefit or tax fraud[xxii]. Furthermore, though technologies such as facial recognition[xxiii] and language modelling[xxiv], AI systems tend to exacerbate existing social inequalities by targeting already vulnerable groups[xxv] , exhibiting prejudice against racial and ethnic minorities, and showing bias toward a Western male-dominant perspective.[xxvi] For example, the study by the Berkeley Haas Center for Equity, Gender and Leadership analysed 133 AI systems across different industries and found that about 44 per cent of them showed gender bias, and 25 per cent exhibited both gender and racial bias.[xxvii] Significant gender bias was also reported in the study by UN Women and UNU Macau in 2024 , which explored the connections between AI, digital security and the women, peace and security agenda in South-East Asia.[xxviii]

AI makes it difficult to assess whether discrimination has occurred. Compared to traditional forms of discrimination, automated discrimination is more abstract and unintuitive, subtle, intangible, and difficult to detect.[xxix] An individual usually becomes aware of discrimination by comparing their

treatment, or its outcome, with that of other people. Furthermore, individuals may not have any accessible way of finding out whether they have been disadvantaged by AI, or how.

Several features of AI systems may cause them to make biased decisions. First, AI systems rely on training data to develop the decision-making algorithm. This is an iterative process, and its success relies on the quality and depth of the input dates, as well on the trainers' ability to identify and address any deficiencies. Consequently, if the training data are insufficient, the algorithms may make predictions that are systematically discriminatory for groups that are unrepresented or underrepresented in the data. [xxx]

Secondly, a common form of bias in artificial intelligence tools arises from the way in which algorithms are designed. If bias is ingrained in design choices, an algorithm can lead to biased outcomes, even if the data fed into the algorithm are perfectly representative. Sometimes, the backgrounds or perspectives of algorithm designers may lead them to incorporate unconscious biases, including racial or sexist biases, in their algorithm designs. [xxxi]

Thirdly, AI systems function within a specific context: if deployed in social conditions that hinder the enjoyment of rights by certain groups, an AI system can perpetuate bias.[xxxii] Without human oversight, AI is currently incapable of replicating contextual concepts of fairness.[xxxiii]

The digital technology sectors have been criticised for their lack of diversity, a problem further compounded by the absence of inclusive consultation in the development of artificial intelligence systems, which contributes to challenges in algorithmic design.[xxxiv] Currently, women make up approximately 30% of the AI workforce[xxxv], while the representation of other diverse groups is even lower.[xxxvi] According to Stinson and Vlaad (2024), "the culture of AI lionizes lone genius figures, devalues nontechnical expertise, and has earned a reputation for being unsafe for both women and racial minorities".[xxxvii]

Human rights law, grounded in the **International Covenant on Civil and Political Rights**, offers a framework of equality and non-discrimination standards for evaluating the use of AI. It requires that all individuals' rights be respected and ensured 'without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'.[xxxviii] The law entails prohibitions against not just direct discrimination, but indirect and structural discrimination too. The obligation to ensure non-discrimination applies across areas of government policy and influence, including the development and application of artificial intelligence technologies. However, enforcing this principle has proven challenging in practice.

This working group will explore the challenges AI poses to equality and non-discrimination from a human rights perspective and discuss ways to uphold these principles in practice. Below are guiding questions to explore in this working group:

Working group questions:

1) How do AI systems contribute to or help reduce **discrimination** in areas such as **criminal justice, healthcare, and employment**? Can you provide any examples from your country?
2) How can AI systems be designed to minimise **biases** that reinforce **systemic inequalities**, and are states playing their part in ensuring **accountability** for AI-driven systemic bias?
3) To what extent are **human rights assessment frameworks** effective in guiding companies and states to identify, prevent, and mitigate discriminatory impacts of AI technologies?

4) What strategies can enhance the representation and **inclusion of marginalised groups, particularly women**, in AI development and deployment?

5) What steps should a State take to ensure equality and non-discrimination in AI-related benefits and risks, particularly so that **marginalised groups** are not treated unfairly?

6) What are some good practices for ensuring **Indigenous participation** in the development of AI tools to prevent systemic biases and reduce harm in sectors like healthcare, education, and the justice system?

7) How can **AI literacy** be improved for both users and developers to better recognise and address discrimination in AI systems?

3. Remedies and Reparation of Harms (Access to Justice):

The right to remedy is a core tenet of the international human rights system, and the need for victims to have access to an effective remedy is recognised in international human rights instruments like the **Universal Declaration of Human Rights (UDHR)** and the **International Covenant on Civil and Political Rights (ICCPR)**. International human rights law requires both governments and companies to provide an 'effective remedy' in the event of breach of their obligations and responsibilities. This comprises effective reparation, appropriate accountability for those responsible, as well as measures to prevent recurrences.

The availability of remedies is essential for ensuring that human rights and ethical principles have meaningful impact, particularly in the face of competing commercial interests. Yet, little attention has been given on establishing effective mechanisms to address harms caused by AI. At present, **there is no clear or consistent pathway for individuals to seek redress when their human rights are violated by AI systems** [xxxix]Moreover, for judicial and non-judicial bodies – as well as individuals pursuing claims – to fully assess the human rights impacts of AI, they must have access to relevant and sufficient information. However, AI developers and deployers often withhold such information under claims of confidentiality or proprietary protection, creating significant barriers to accountability and undermining access to effective remedies.[xl]

Cases concerning the human rights impacts of AI systems brought before both judicial and non-judicial bodies have highlighted the urgent need for redress and remedies, while also revealing the inadequacy of existing legal frameworks to fully address such harms. Many of the cases pursued have relied on data protection laws, suggesting that a broader range of human rights violations linked to AI may go underreported[xli] . This underreporting highlights the critical need for greater access to information and expertise and awareness to better identify and respond to AI -related human rights harms. For individuals to effectively file complaints, they must have sufficient information to understand how decisions affecting them were made and the role AI played in that process. This includes access to data on how the AI was designed, tested and intended to function, as well as how it performed in the specific case. Furthermore, transparency around involvement of human decision-making or oversight is essential to ensure accountability and uphold the right to remedy. [xlii]

The availability of remedies for AI-related human rights violations differs considerably across regions and countries. In Europe, established regulatory frameworks – such as the recently adopted **EU AI Act** and **Council of Europe Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,** provide individuals with more defined legal pathways to seek

redress for issues such as data misuse and discriminatory impacts. [xliii]In contrast, in many parts of Asia, legal and institutional responses to the human rights implications of AI are still evolving, with fewer established accountability mechanisms and limited avenues for individuals to pursue remedies when their rights are affected.

In both region, there remains a general hesitance to impose strong regulatory obligations on the private sector[xliv], reflecting a broader challenge in aligning technological innovation with human rights protections.

Nonetheless, international human rights law, which most ASEM member countries have ratified, continues to apply across Asia and Europe and provides a common normative framework for assessing and addressing the impacts of AI on fundamental rights. However, enforcement of these standards is often lacking. Thus, to make this framework effective in practice, it is essential to raise awareness, enhance its usability, to invest in building literacy and providing training on human rights for all actors involved in the development, deployment, regulation and oversight of AI systems.

Working group questions:

1) Can **existing human rights instruments**—like the right to a fair trial or the right to an effective remedy—adequately address harms from AI systems, or are new legal tools needed?
2) What mechanisms currently exist for **holding AI developers and deployers accountable** for rights violations, and how effective are they?
3) How should remedies be designed to address not only individual harms, but also **systemic or collective impacts** caused by AI systems?
4) What role should **transparency and explainability** play in enabling individuals to seek redress? Is a lack of explainability itself a violation of rights?
5) How can **affected communities** participate in the development and deployment of AI to ensure fairer outcomes and that technology aligns with the values and needs of the people it serves?
6) What role can **ombuds institutions, data protection authorities, or national human rights institutions** play in providing or facilitating remedies for AI-related harms?
7) How can member states effectively invest in **AI literacy** among the general public—especially in schools and marginalised communities—to ensure a well-rounded understanding of both the functioning of AI and its potential human rights impacts?

Guiding questions

In addition to the sub-theme-specific questions, the following cross-cutting questions will guide discussions across all working groups:

1) What are the main **human rights risks** linked to the deployment of AI systems by both state and private actors?

2) How can AI systems be made more transparent to ensure **accountability** and **trust** among users? Are there **positive practices** in policies, regulations, or business practices that can be modelled to protect human rights in AI deployment?

3) How effective are **ethical guidelines** in preventing human rights violations caused by AI, considering the lack of legal binding and oversight, allowing companies to choose whether or not to adhere to them?

4) How can stakeholders, including **marginalised and vulnerable communities**, be meaningfully included in AI governance discussions and decision-making processes?

5) Are **civil society organisations and NGOs** sufficiently equipped to address the human rights implications of AI, and what support do they need to strengthen their role in this space?

6) How can **NHRIs**, as a bridge between government and civil society and with the ability to collaborate with other institutions and organisations, play a key role in addressing the diverse human rights impacts of AI development and deployment? Can you share any examples of good practices from NHRIs working on AI?

7) What approaches have proven successful in integrating **human rights education** into the AI development process?

8) How can **international, regional, and national regulatory frameworks** work together to address the cross-border implications of AI technologies?

9) How do approaches to **AI governance in Asia and Europe** differ, and what can be learned from these regional experiences to develop more effective, inclusive policies? What are some practical avenues for collaboration between the two regions to promote responsible and globally coherent AI governance?

10) Would the establishment of an Office for the **Special Rapporteur on Human Rights and AI** be an effective way to enhance oversight and accountability in addressing AI-related human rights violations?

11) How might the **future of human rights** be shaped by the evolving capabilities and deployment of AI technologies, and what proactive measures should be taken to safeguard these rights?

ENDNOTES

[i] Referring to a variety of techniques that vary in complexity and share a common outcome: the imitation of human cognition or decision-making. UNESCO TVETipedia Glossary.
[ii] https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
[iii] For example, against persons with disabilities. See e.g. https://documents.un.org/doc/undoc/gen/g21/397/00/pdf/g2139700.pdf
[iv] https://aire.lexxion.eu/article/aire/2024/1/13
[v] Including Australia, UK, China and India.
[vi] See e.g. ENNHRI-statement-of-concern-on-AI-Convention-at-CAI-plenary.pdf
[vii] See https://asean.org/book/asean-guide-on-ai-governance-and-ethics/
[viii] See e.g. Australia's Voluntary AI Safety Standard: https://www.industry.gov.au/publications/voluntary-ai-safety-standard/10-guardrails
[ix] Understood as a set of instructions or rules that enable machines to learn, analyze data and make decisions based on that knowledge.
[x] See Office of the United Nations High Commissioner for Human Rights, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, UN Doc A/HRC/56/68 (2024), para 16
[xi] Including article 16 of the Convention on the Rights of the Child, article 22 of the Convention on the Rights of Persons with Disabilities, and article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights)
[xii] A/HRC/39/29, para. 11.
[xiii] See Simple Guide on the International Covenant on Civil and Political Rights (ICCPR) – an overview of Articles 1 – 27., p. 30. Centre for Civil and Political Rights (CCPR Centre) Available here: ICCPR_easy_to_read_commentary_WEB.pdf
[xiv] See Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (2014), para 20
[xv] System of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (UNESCO TVETipedia Glossary)
[xvi] The General Data Protection Regulation (GDPR) sets guidelines for the collection and processing of personal information from individuals residing in the EU and also applies to organisations outside the EU that target or collect data related to EU citizens. In Asia, e.g. China and Singapore have developed regulations regarding data collection by IoT.
[xvii] A/HRC/48/31, para. 10
[xviii] Automated decision-making (ADM) refers to processes where decisions are made solely by automated systems, without significant human intervention
[xix] Allhutter, D. et al. (2020), 'Algorithmic profiling of job seekers in Austria: how austerity politics are made effective', Frontiers in Big Data, 21 February 2020, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2020.00005/full (accessed 5 April 2025) ; see also https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G/ (Accessed 5 April 2025)
[xx] In 2017, the Finnish Non-Discrimination Ombudsman took a case to the National Non-Discrimination and Equality Tribunal against a bank concerning use of automated decision-making in granting loans. The automation was based on a system in which loan applicants were scored on the basis of their place of residence, gender, mother tongue and age was ruled to be discriminatory. See https://yhdenvertaisuusvaltuutettu.fi/en/artificial-intelligence-and-equality
[xxi] Bonnett, G. (2018), 'Immigration NZ using data system to predict likely troublemakers', RNZ News, 5 April 2018, https://www.rnz.co.nz/news/national/354135/immigration-nz-using-data-system-to-predict-likely-troublemakers (Accessed on 5 April 2025)
[xxii] This was the case with the Dutch government's use of System Risk Indication (SyRI)—an algorithm designed to identify potential social welfare fraud, which in 2020 was ruled by the Hague's District Court to be in violation of of the European Convention on Human Rights (ECHR)2 for an interference with the exercise of the right to private life to be necessary and proportionate. The court also found the system was discriminatory and only used in so-called 'problem neighbourhoods'. See e.g. Adamantia Rachovitsa, Niclas Johann, The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case, Human Rights Law Review, Volume 22, Issue 2, June 2022, ngac010, https://doi.org/10.1093/hrlr/ngac010
[xxiii] According to Cambridge dictionary, technology that makes it possible for a computer to recognise a digital image of someone's face.
[xxiv] Language modeling, or LM, is the use of various statistical and probabilistic techniques to determine the probability of a given sequence of words occurring in a sentence. Language models analyze bodies of text data to provide a basis for their word predictions. (What Is Language Modeling? | Definition from TechTarget). AI-based language technology—large language models, machine translation systems, multilingual dictionaries, and corpora—is currently limited to three percent of the world's most widely spoken, financially and politically backed languages, favoring certain languages or dialects over others. See e.g. Helm, P., Bella, G., Koch, G. et al. Diversity and language technology: how language modeling bias causes epistemic injustice. Ethics Inf Technol 26, 8 (2024). https://doi.org/10.1007/s10676-023-09742-6

[xxv] See https://unu.edu/macau/news/new-un-research-reveals-impact-ai-and-cybersecurity-women-peace-and-security-south-east (accessed 5 April 2025)
[xxvi] Global Civil Society Launches Manifesto For Ethical AI. Press Release.December 4, 2023. Available at https://aippnet.org/wp-content/uploads/2023/12/Global-civil-society-launches-manifesto-for-ethical-AI.pdf (Accessed on 11 April 2025)
[xxvii] https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity
[xxviii] https://unu.edu/sites/default/files/2024-05/Artificial%20Intelligence%20and%20the%20Women%2C%20Peace%20and%20Security%20Agenda%20in%20South-East%20Asia.pdf
[xxix] Wachter, S., Mittelstadt, B. and Russell, C. (2020), 'Why Fairness Cannot be Automated: Bridging the Gap between EU Non-Discrimination Law and AI', Computer Law & Security Review, 41(2021): 105567, https://www.sciencedirect.com/science/article/abs/pii/S0267364921000406
[xxx] See Office of the United Nations High Commissioner for Human Rights, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, UN Doc A/HRC/56/68 (2024), para 14
[xxxi] Ibid; See also https://www.unwomen.org/en/articles/explainer/artificial-intelligence-and-gender-equality
[xxxii] As was the case e.g. in a landmark ruling in a case brought by Ed Bridges who challenged South Wales Police's use of live facial recognition in public in 2020. Civil liberties groups raised concerns that facial recognition technology is less accurate for people of color and women. See https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/
[xxxiii] Kate Jones: AI governance and human rights. Resetting the relationship. Research paper. Chatham House. Published 10 January 2023. Updated 19 January 2023. Available here: AI governance and human rights | 06 Remedies in AI governance: the contribution of human rights
[xxxiv] Office of the United Nations High Commissioner for Human Rights, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, UN Doc A/HRC/56/68 (2024), para 14.
[xxxv] https://www3.weforum.org/docs/WEF_GGGR_2023.pdf, page 7 (accessed on 11 April 2025)
[xxxvi] According to New York University study in 2019, only 2.5% of Google's workforce is black, while Facebook and Microsoft are each at 4%. Only a little data exists on trans workers or other gender minorities in the AI field.
[xxxvii] Stinson, C., & Vlaad, S. (2024). A feeling for the algorithm: Diversity, expertise, and artificial intelligence. Big Data & Society, 11(1). https://doi.org/10.1177/20539517231224247 (Original work published 2024)
[xxxviii] International Covenant on Civil and Political Rights, Article 2(1)
[xxxix] Kate Jones: AI governance and human rights. Resetting the relationship. Research paper. Chatham House. Published 10 January 2023. Updated 19 January 2023. Available here: AI governance and human rights | 06 Remedies in AI governance: the contribution of human rights
[xl] Prof. Frederik Zuiderveen Borgesius (2018) *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*; Directorate General of Democracy, Council of Europe. Report available here: Discrimination, artificial intelligence, and algorithmic decision-making
[xli] Council of Europe Commissioner for Human Rights (May 2023): Human rights by design future-proofing human rights protection in the era of AI, page 29. Available here: https://rm.coe.int/follow-up-recommendation-on-the-2019-report-human-rights-by-design-fut/1680ab2279
[xlii] Kate Jones: AI governance and human rights. Resetting the relationship. Research paper. Chatham House. Published 10 January 2023. Updated 19 January 2023. Available here: AI governance and human rights | 06 Remedies in AI governance: the contribution of human rights
[xliii] Although these come with limitations too. E.g. The CoE convention has been criticised for its vague implementation guidelines concerning redress and remedy (see e.g. https://www.amnesty.eu/wp-content/uploads/2024/04/Amnesty-International-Recs-draft-CoECAI-11042024.pdf) while for the EU AI Act, it remains unclear how effectively it will enable authorities to enforce compliance and hold violators accountable (see e.g. EU's AI Act fails to set gold standard for human rights - European Disability Forum).There is also growing concern that these recently introduced regulations may exclude the private sector from meaningful accountability and oversight.
[xliv] For example, the recently introduced Convention on Artificial Intelligence and human rights, democracy and the rule of law by the Council of Europe does not oblige parties to the Convention to apply the provisions of the treaty to the private sector.