Meeting Report

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GOVERNING GENERATIVE AI: CLOSING THE GAPS TO PROTECT HUMAN RIGHTS

PREPARED BY THE COUNCIL OF EUROPE
COMMISSIONER FOR HUMAN RIGHTS

Strasbourg, 27 February 2026

CommHR(2026)21

CONTENTS

Background

On 6 and 7 November 2025, the Council of Europe Commissioner for Human Rights brought together a group of experts from civil society organisations working on artificial intelligence (AI) to discuss the risks of generative AI (GenAI) and the gaps in governance. Each expert brought specific expertise spanning children's rights, racism and freedom of expression, among others, to provide different angles for the discussion. The Commissioner chaired the meeting.

The consultation aimed to identify the human rights risks connected to the deployment of GenAI and the main gaps in current governance frameworks in Europe regarding the development of GenAI technology. It also looked at how to strengthen AI governance in compliance with human rights law and standards. The consultation centred on two main themes:

Theme 1: Human rights risks stemming from the deployment of generative AI
Theme 2: Identifying gaps in Europe's governance frameworks and how to close them

The agenda can be found at Annex I and a list of participants is provided at Annex II to the report.

Disclaimer

This report provides a non-exhaustive overview of the consultation's main points and conclusions in the form of a chairperson's summary. The views and opinions expressed in the report reflect the discussion among participants and do not necessarily represent a position or policy of the Council of Europe Commissioner for Human Rights.

DISCUSSION AND CONCLUSIONS

Theme 1: Human rights risks stemming from the deployment of generative AI

1. The human rights challenges and risks brought by AI – including generative AI (GenAI) – fall into three categories: sector-specific risks, for example, those relating to data privacy, bias and discrimination; risks based on the quality of the product, such as the reliability of outputs produced by large language models (LLMs); and the weaponisation of AI systems – for example, the deliberate act of using AI to spread politically motivated disinformation through artificially produced or manipulated digital content (synthetic media), such as deepfakes and other generative tools.

2. An issue of increasing concern is the use of AI in the military sector. The growing use of AI systems in ongoing conflicts is presented to the public as a positive development which reduces risks in combat. However, the use of automated AI systems to identify targets in conflicts transfers the risk of error to the technology. This presents two main problems. Firstly, there is an issue of reliability: the lack of (sufficient) human oversight or intervention can lead to fatal mistakes. This leads to the second problem, which is a shift in liability: when a machine acts autonomously, responsibility for its mistakes becomes unclear, making it harder to identify who should be held accountable. Due to security and confidentiality concerns, the military and security sectors often fall outside the scope of current regulations and public scrutiny, resulting in reduced oversight. Automation of AI systems used in combat therefore raises significant ethical and practical concerns. The direct risks to human rights, including the right to life, require greater scrutiny and accountability within the sector.

3. GenAI, in particular, plays a major role in the spread of disinformation in international conflicts. Civil society has raised significant concerns about the degradation of information quality caused by the spread of disinformation and low-quality, AI-generated content (such as AI slop), which have been used as tools in hybrid warfare. This is evident in the context of Russia's war of aggression against Ukraine, where myriad websites posing as newspapers have emerged, with the intention of dominating information flows. This creates information overload, making it more difficult for individuals to distinguish fact from fiction.

4. This pollution of the media ecosystem also occurs in everyday contexts. AI-driven information overload corrupts the media environment, undermining how people consume and engage with content and often eroding trust in information. For instance, election interference through disinformation campaigns has become widespread in recent years. AI – including synthetic media, such as deepfakes – has been used to amplify disinformation at scale and manipulate public opinion, with the goal of influencing election outcomes. Very large online platforms (VLOPs) contribute to this phenomenon and current efforts to regulate AI-generated content lag behind real-time needs.

5. AI-generated content can be particularly harmful towards marginalised groups of people, including women, migrants and LGBTI people, contributing to the perpetuation of real-life discrimination and inequality. Algorithmic systems similarly contribute to this: for example, the use of AI-driven automated decision-making in public services has significant implications for marginalised people in sectors such as welfare, policing, and migration. Children are also significantly affected by algorithmic systems and chatbots. From attention and cognitive harms (so-called brain rot) to addictive use patterns and mental health issues, we are increasingly seeing the negative consequences for children stemming from the use of AI. Increased efforts are required to protect children from these risks, while ensuring meaningful, age-appropriate participation of children in decisions and policies that affect them.

6. AI uses vast amounts of data, including personal data. The storage of and access to this data raise many privacy concerns. Civil society highlights two main risks. First, stored personal data can be inaccurate: when AI systems, such as LLMs, generate inaccurate data on individuals, the data subjects might be unaware of it and therefore unable to seek rectification. Second, there is a risk of losing control over personal data: users often lack robust contractual protections, as many companies can update their policies at any moment and retain control over data. Individuals may use their right to object to their data being used for AI systems, but if the data has already been stored and used – particularly for AI training – then it cannot be easily removed. Opt-in consent models for data collection and processing can help prevent this. In addition, care must be taken with the integration of existing AI systems into different environments, such as AI assistants embedded in software or search platforms, which can grant access to private or confidential data without users' explicit permission. This can also occur through software updates, without the user being aware or having the opportunity to opt out.

7. The global environmental and social impacts of AI are an issue of growing concern within civil society. On the one hand, AI supply chains rely on mining minerals (sometimes under abusive conditions, including child labour), with the resulting environmental and health harms falling disproportionately on communities marginalised on racial and socio-economic grounds in mining regions, particularly in the Global South. On the other hand, data centres consume large amounts of water and energy. Moreover, the rate of use is rapidly increasing as demand for AI systems surges, and models become

larger and more complex, rendering them more power-intensive to operate. This is already having negative, albeit currently localised, environmental impacts on the communities where data centres are being located, including power outages, water shortages and health-related problems. As a result, there is increasing local awareness of AI's potential negative impacts, which may mobilise communities to push for policy and legislative changes.

8. Many other sectors require specific attention, including the use of AI in biometrics and surveillance. The widespread impacts of AI across private and public life mean that regulation is essential. The impact of AI must be assessed from the outset, and oversight and accountability are necessary to ensure that AI advances, rather than undermines, human rights.

Theme 2: Identifying gaps in Europe's governance frameworks and how to close them

9. The following section sets out some of the major challenges, as well as suggested solutions, for human rights-based governance. A lack of transparency in AI systems is hindering adequate human oversight. Meanwhile, the influence of the Big Tech industry risks impeding progress on human rights protections by shaping public narratives about AI – including through public relations and marketing campaigns that emphasise capabilities (sometimes misleadingly), while downplaying risks. This, in turn, is weakening understanding among policymakers and the public of AI's negative human rights impacts. Finally, existing regulations are currently poorly enforced, meaning that accountability and liability for AI-related harms remain limited.

10. In the current geopolitical context, technology companies have few incentives to voluntarily align their practices with the public interest. Experience indicates that regulation can play a crucial role in addressing this gap. For example, following the adoption of the Digital Services Act, numerous companies implemented structural changes, such as enhanced transparency, risk assessments, and strengthened content-moderation measures.

11. Currently, however, companies are pausing or reversing reform efforts due to uncertainty arising from anticipated regulatory changes. The number of private sector employees working on safety and human rights compliance has decreased. The most effective EU response, amid growing corporate influence which risks weakening human rights protections in the digital sphere, is robust enforcement of its existing regulations. This has been a key demand from civil society in recent years.

12. In this regard, there is widespread concern among civil society that safeguards and oversight could be weakened as the EU prioritises competitiveness. The European Commission's recently proposed Digital Omnibus package is presented as an effort to streamline and simplify EU digital legislation, including implementation of the AI Act, and reduce administrative burdens on businesses. However, civil society organisations warn that several provisions are vague and risk diluting human rights protections. For example, under the EU AI Act, as currently enacted, providers and deployers of AI systems must take measures to ensure, to their best extent, that their staff have a sufficient level of AI literacy. The Digital Omnibus proposes to reframe this as an obligation, on the part of Member States and the Commission, to *encourage* providers and employers to provide a sufficient level of AI literacy among their staff and other relevant actors. The proposal also allows, inter alia, for self-derogation from certain requirements applicable to high-risk AI systems in the AI Act. Civil society further underline that the

multiple simplification proposals are fragmented across instruments, hindering their ability to engage with the process in a timely and meaningful manner.

13. The debate over deregulation has additional implications for EU candidate countries, including those in the Western Balkans that are already aligning their legal frameworks with EU law. This concern is twofold. First, any later EU amendments would also need to be transposed into national law, potentially delaying the accession process. Second, the simplification agenda risks signalling to these countries that innovation should be prioritised over human rights protections – an alarming message that could undermine fundamental values in societies that are already fragile democracies.

14. The Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law provides a human rights-centred, binding baseline open to non-EU states, and is increasingly relevant as a foundation for civil society's advocacy engagement in EU candidate countries. There is a clear need to accelerate signature and ratification, particularly among non-EU states.

15. Civil society emphasises the importance of acting in a unified manner to push back effectively against the tech sector's deregulation narrative. A thriving civil society is essential to provide checks and balances on ongoing developments both in technology and its regulation. However, shrinking civic space is affecting those working on human rights compliance within the tech and AI sectors, while opportunities for civil society to meaningfully participate in AI decision-making and oversight remain limited.

16. Challenges persist in translating some of the existing EU AI Act requirements into technical standards, particularly around the obligation to ensure human oversight. This work is further complicated by the wide variety of AI uses and risk profiles across sectors, which makes generalised standards difficult to design and apply. The field of AI standardisation and regulatory practice is still nascent and there is little relevant case-law or precedent to provide guidance.

17. Civil society emphasises that any restrictions on the use of AI should be proportionate to the legitimate aim pursued and should not be applied as a blanket measure. For example, an absolute ban on social media for children may adversely affect their rights to participate in the digital environment and engage in civic life. Moreover, there is currently limited oversight of how service providers would introduce and implement such prohibitions under EU digital regulations. At the same time, authorities should require companies to ensure that AI products intended for children are safe by design. Certain manipulative algorithms – particularly those that exploit children – should be prohibited and the burden of proof should rest on companies to demonstrate that their products are safe.

18. Public authorities should also be prepared to prohibit certain uses of technology that undermine or seriously risk violating human rights. For instance, weapon systems whose effects cannot be sufficiently understood, predicted, or explained should be prohibited. Similarly, the use of autonomous weapons to select and engage human targets should be banned.

19. Transparency – including transparency of oversight – is paramount to ensuring human rights protection and must include access to data. At present, there are no clear legal bases or procedures enabling independent researchers or civil society organisations to conduct investigations into how AI systems are used in practice. These actors should be granted access to the data, documentation and

technical tools needed for effective oversight of AI systems and to complement institutional monitoring (with appropriate privacy and security safeguards). This must go hand in hand with ensuring that investigative journalists have the resources necessary to carry out their work. Transparency should also be strengthened in respect of public procurement of AI systems, which, for now, remains persistently opaque.

20. Another barrier to transparency is the limited public understanding of how personal data are collected, shared and processed by online services during everyday use. Greater investment in digital literacy should equip users to recognise common tracking practices, understand what data are stored, by whom, and for what purposes, as well as what rights and controls they have.

21. One avenue for protecting against human rights abuses arising from AI systems is through filing complaints with national data protection authorities. For example, complaints filed by a non-governmental organisation in four countries against Clearview AI – a company that processed individuals' biometric data derived from facial images – led data protection authorities to find that this processing of personal data lacked a legal basis. Enforcing such decisions against companies with no EU establishment nevertheless remains difficult. Authorities should also ensure that remedies are available and easily accessible to individuals.

22. To overcome current governance and enforcement challenges, European and international institutions should consistently call on technology companies to respect human rights principles, and work to close gaps across legal frameworks to ensure corporate accountability. State authorities have a duty to enforce the law regardless of the level of private sector investment in their national economies. At the same time, attention must be drawn to the significant resource constraints facing enforcement bodies, which hinder their ability to fulfil their mandates. The same applies to national human rights structures, including equality bodies, which are being assigned new oversight responsibilities without corresponding increases in resources. Authorities should ensure that these bodies are granted adequate human, financial and technical resources to effectively carry out their roles.

Key conclusions:

- Automated AI systems should be appropriately regulated and subject to meaningful human oversight, especially in military and security contexts, due to the high risks they pose to human rights.
- The degradation of information quality and information overload, which is amplified by AI systems, are changing how people consume and engage with content and eroding trust. AI is also scaling up the spread of disinformation, which is particularly harmful to certain groups of people, including children, migrants, women and LGBTI people.
- The use of personal data by AI systems raises significant privacy concerns. European policymakers should push for default opt-in consent models for data collection and processing to ensure greater user control over personal data. Contractual protections should prevent product or policy updates that incorporate AI without clear notice and explicit consent.
- The environmental and social impacts of AI are increasingly evident, including across global supply chains and in areas where data centres are being built. These impacts should form an integral part of awareness-raising and policy discussions about AI.

- Uses of AI that undermine or seriously risk violating human rights should be prohibited, and authorities should mandate safety-by-design for AI products intended for children.
- Meaningful participation of civil society in decision-making should be ensured and sufficiently funded to provide checks and balances on AI development and regulation. Access to data used by AI systems should be granted to independent researchers, journalists and civil society organisations, and transparency in public procurement should be strengthened.
- Consistent, robust enforcement of existing EU digital regulations is essential, with adequate resources allocated to oversight authorities, including national human rights structures.
- Investment in digital literacy and human rights-compliant standard-setting should be scaled up.

Annex I

PROGRAMME

GOVERNING GENERATIVE AI: CLOSING THE GAPS TO PROTECT HUMAN RIGHTS

Consultation with civil society organisations

Paris, 6-7 November 2025

Venue: Meeting Room 5, Council of Europe's Paris Office

55 Avenue Kléber, 75116 Paris

Thursday 6 November 2025

13:45 - 14:00 Arrival and registration

Meeting room 5, Council of Europe Paris office

14:00 - 14:10 Welcome address and introduction by Michael O'Flaherty, Commissioner for Human Rights

14:10 - 14:15 The work on AI and human rights by the Council of Europe

Hristijan Koneski, Adviser to the Commissioner for Human Rights

14:15 - 14:45 Tour de table

Brief presentation of participants and their work

14:45 - 15:45 Session I: Human rights risks stemming from the deployment of generative AI

This session seeks to identify the human rights risks connected to the deployment of generative AI, with a focus on disadvantaged groups and children.

Discussion

15:45 - 16:05 *Coffee break*

16:05 - 17:55 Continuation of discussion

18:00 *End of day one*

Friday 6 November 2025

09:00 - 09:05 Introduction

Sandra Veloy Mateu, Adviser to the Commissioner for Human Rights

9:05 – 10:40 Session II: Identifying gaps in regulation in Europe and how to close them

This session aims to identify the main gaps in current regulation in Europe regarding the deployment of generative AI technology and which implications these carry for

human rights, as well as to look out for solutions on how to close loopholes and strengthen AI governance in compliance with international human rights law.

Discussion

10:40 - 11:00 Coffee break

11:00 - 12:50 Continuation of discussion

12:50 - 13:00 Concluding remarks by Michael O'Flaherty, Commissioner for Human Rights

13:00 End of day two

****

Annex II

List of Participants

Appelman, Naomi	The Racism and Technology Center
Çetin, R. Buse	AI Forensics
Coppi, Giulio	Access Now
Dempsey, Mark	ARTICLE 19
Fedchenko, Yevhen	Stop Fake
Letouche, Manon	5 Rights Foundation
Ristić, Andrijana	Share Foundation
Sardeli, Kleanthi	NOYB (none of your business)

Council of Europe

O'Flaherty, Michael	Commissioner for Human Rights
Havula-Lorenzini, Anna	Assistant
Koneski, Hristijan	Adviser to the Commissioner
Veloy Mateu, Sandra	Adviser to the Commissioner