



Expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy

CONCEPT NOTE

The expert seminar is expected to be held in the **last week of May 2020**. Exact date will be communicated in the coming weeks. Due to the COVID-19 pandemic and to ensure the broadest participation the seminar **will be held online**. It will be conducted over **two half days**.

I. INTRODUCTION

1. In operative paragraph 10 of resolution 42/15, the Human Rights Council requested the Office of the United Nations High Commissioner for Human Rights "to organize, before the forty-fourth session of the Human Rights Council, a one-day expert seminar to discuss how artificial intelligence, including profiling, automated decision-making and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy".

II. BACKGROUND

2. The right to privacy is recognized, inter alia, in Articles 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Political and Civil Rights. It is also an essential requirement for the realization of other human rights, including the right to freedom of opinion and expression and the right to peaceful assembly. It is a core foundation of democracies and its respect constitutes an important element for a thriving civil society.

3. As noted by the Human Rights Council, “the use of artificial intelligence that requires the processing of large amounts of data, often relating to personal data, including on an individual’s behaviour, social relationships, private preferences and identity, can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioural prediction or the scoring of individuals” (Resolution HRC/RES/42/15).
4. The right to privacy in recent years has attracted increasing attention from the United Nations General Assembly, the Human Rights Council and human rights mechanisms. Attention was drawn to surveillance policies and practices of governments as well as State and business practices that increasingly rely on the collection, use, sharing and processing of personal data. The impact of privacy-invasive technologies on freedom of expression, peaceful assembly, access to health and welfare services have also been raised.
5. Since the first General Assembly resolution on the right to privacy in the digital age (resolution A/RES/68/167) introduced by Brazil and the Federal Republic of Germany, the General Assembly and the Human Rights Council have adopted a number of consensual resolutions reaffirming the importance of the right to privacy and addressing concerns related to arbitrary or unlawful interferences therein. Special rapporteur mandate holders and treaty monitoring bodies have raised specific concerns related to the impact of states and businesses laws and practices on the right to privacy. Recommendations relating to the right to privacy in the digital space have also been formulated by Member States through the Universal Periodic Review. (See background documents.)
6. The use of artificial intelligence (AI) can contribute greatly to the promotion and protection of human rights. However, the implications of the use of AI technologies on the right to privacy for the individual and in increasing sectors of society are yet to be adequately addressed by States, businesses enterprises, civil society and international organisations. The design, development, deployment and evaluation of AI technologies must be in accordance with the obligations of States under international human rights law and the responsibilities of business enterprises, in accordance with the UN Guiding Principles on Business and Human Rights. These include obligations to refrain from using AI in ways that violate the right to privacy or other human rights and to ensure that any interference with the right to privacy complies with the principles of legality, necessity and proportionality.
7. Further, AI applications that rely on personal data or otherwise interfere with individual’s right to privacy may “lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights” (Resolution HRC/RES/42/15). Hence, the right to privacy is a gateway for the promotion and protection of other human rights impacted by AI.

III. EXPERT SEMINAR

3.1 Goal

8. The expert seminar will bring together States, relevant United Nations bodies, funds and programmes, intergovernmental organizations, treaty bodies, special procedures mandate holders, regional human rights mechanisms, civil society organizations, academia, national human rights institutions and other relevant stakeholders. Participation of practitioners with specific experience related to the right to privacy and artificial intelligence will be encouraged.
9. The seminar will be a platform for an in-depth discussion of the impacts of AI on the enjoyment of the right to privacy. It will give stakeholders an important opportunity to analyse the key roles that privacy plays in safeguarding other human rights affected by AI. It will also seek to articulate safeguards and processes that States, businesses and international organisations are required to put in place to promote and protect the right to privacy in the digital age.

3.2 Methodology

10. Due to the COVID-19 pandemic and to ensure the broadest participation the seminar will be held online. The modalities as well as the technical details on which on-line platform will be used and how to join the meeting will be circulated in the coming weeks. Furthermore, OHCHR is currently discussing with UNOG technical modalities for the provision of interpretation on an “if available” basis.”
11. The seminar will encourage the exchange of international, regional and national experiences and best practices concerning AI applications and the protection and promotion of the right to privacy in the digital age.
12. Experts representing diverse backgrounds and perspectives will introduce the themes of the different sessions and interact with participants in order to guide the moderated discussions. Participants, including experts and practitioners from States and civil society and other relevant stakeholders, will be invited to share their views, experiences and good practices.
13. In order to allow a broad range of perspectives and issues to be considered at the seminar, OHCHR encourages the submission of written contributions pertinent to the sessions. Please send them to privacy-seminar@ohchr.org.

3.3 Sessions

14. The expert seminar will be structured in 4 sessions of 90 minutes each. Each session will have one chair/moderator and 3 to 4 panellists.

Session I: Setting the scene: what are the challenges to privacy that are specific to AI?

15. This session will identify the specific risks to the right to privacy presented by AI, including profiling, automated decision-making and machine-learning technologies. What is it that makes AI particularly threatening for privacy?
16. The participants will discuss topics such as:
 - The risks to the right to privacy linked to the use large amounts of data that is typical for many AI approaches.
 - The implication on the right to privacy of the inference and prediction abilities of AI.
 - The identification of people by AI and the ensuing enhanced tracking and surveillance capacities.
 - The manipulation of people's behaviour based on AI.

Session II: Privacy to enable the protection of other rights affected by AI

17. The session will focus on the importance of upholding the right to privacy and on how privacy interference by AI applications (by governments and business enterprises) can threaten the enjoyment of other human rights.
18. It will look particularly into:
 - Right to freedom of expression (including to seek and receive information): what role does the processing of personal data by AI play in delivering and filtering information, including for content curation and moderation purposes and targeting of information (including disinformation)?
 - Rights to health, and welfare: what are the safeguards necessary to ensure that AI applications on health data (including in the context of the responses to COVID 19) respect human rights? How to ensure that the digitalisation of welfare does not infringe the right to privacy?
 - Right to freedom of assembly and freedom of movement: what are the human rights implications of AI application to identify individuals in public spaces (physical and online) (e.g. facial recognition in public spaces, predictive policing, social media monitoring)?
 - The rights and overarching principles of equality and non-discrimination and the challenges posed by the use of AI to these.

Session III: Legislative and regulatory responses

19. This session will be dedicated to a discussion of existing legal and regulatory frameworks and possible future approaches of States to the governance of AI. Questions raised will include:

- How do modern data protection principles and the right to privacy apply to AI applications? What are the strengths and weaknesses of existing data protection and privacy laws (including how AI applications undermine traditional protection strategies such as anonymization, data minimization, purpose specification, retention, and how it challenges the distinction personal/non-personal data)?
- Emerging legal frameworks for the regulation of AI applications. What are emerging regulations of AI that seek to respect the right to privacy? What are the criteria and parameters for the banning or strictly limiting of particular AI applications ('red lines')?
- Can these legislative and regulatory frameworks be 'future proofed'? How to address future threat scenarios?

Session IV: Design, Human Rights Due Diligence and Safeguards in AI applications

20. This session will set out the procedural steps and technological solutions that states and businesses should take to prevent violations of the right to privacy when using AI, and address and remedy them, where they occur.

21. In particular the participants will examine:

- The type of human rights due diligence that should be carried out prior to development and deployment of AI applications, also exploring standards of privacy impact assessment and privacy by design and by default.
- The governance of data sharing and the principles that should be applied when procuring/relying on AI applications that process personal data.
- The transparency measures required to allow meaningful independent oversight and the exercise of the right to redress by individuals affected by AI.
- How these safeguards can be made 'future proof', including by exploring future threat scenarios.

IV. BACKGROUND DOCUMENTS

- Human Rights Council, resolution 42/15, the right to privacy in the digital age
- Report of the Office of the High Commissioner on the right to privacy in the digital age, U.N. doc. A/HRC/39/29
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on artificial intelligence, U.N. doc. A/73/348
- Report of the Special Rapporteur on the right to privacy, U.N. doc. A/74/277
- Report of the Special Rapporteur on extreme poverty and human rights, U.N. doc. A/74/493
- Report of the UN Secretary-General's High-level Panel on Digital Cooperation