Digital technologies can greatly facilitate the exercise and enjoyment of human rights and fundamental freedoms, boost participatory and democratic processes and facilitate social and commercial activities. But also, they carry with them human rights challenges that require prompt and balanced solutions.

The Council of Europe engages in setting standards, promoting democracy and the rule of law by fostering multi-stakeholder dialogue to ensure a sustainable, people-centred and human rights-based approach to the challenges of the digital environment.
Council of Europe at IGF 2022

Adis-Ababa, Ethiopia, 28 November to 2 December 2022

28 November, 15.20-16.20 CET

Regulatory challenges of addressing advanced technologies (AI and Metaverse)

AI is a very promising technology that can enable humanity to make great strides forward in terms of science and business or help societies to organise themselves more efficiently and provide better service to their citizens.

Yet at the same time, this technology can take humanity to a very dystopic place – a truly “Big Brother” society where human rights and fundamental freedoms are trampled underfoot; where democratic processes are ruthlessly manipulated, where the rule of law has been replaced by the rule of algorithm.

How should a legally enforceable international regulation look like, particularly in relation to those aspects of AI which touch directly or indirectly on human rights, democracy and rule of law.

The Metaverse is one example of a new generation of media platforms supported by AI technology, which is currently undergoing rapid developments. The Metaverse with its potential for total immersion in an alternative universe – besides all the fun parts – comes with a whole set of issues relating to rule of law and human rights.

The session will explore such questions as: what impact does such an innovative technology have on the human brain and where can it lead? how to address these and other concerns without stifling technological innovation – while promoting and protecting the human rights and freedoms of all individuals, not just in Europe but around the World?

Jan Kleijssen, Director, Information Society - Action against Crime, Directorate General Human Rights and Rule of Law of the Council of Europe will be keynote speaker for the panel on the Regulatory challenges of addressing advanced technologies.

29 November, 11:50-12:50 CET

Open Forum #65 on Promoting democratic culture online through digital citizenship education

The digital world provides an environment that is fundamental to democratic processes and practice, including the dissemination and mediation of information online. It constitutes an important platform for intercultural dialogue through social media and is the context in which citizens increasingly exercise their rights to participate socially, economically and politically. In 2019, the Council of Europe’s Committee of Ministers adopted Recommendation CM/Rec(2019)10 which incorporates a set of guidelines to member States asking them to develop and promote digital citizenship education and make it a priority for policymakers. According to the Recommendation, the digital environment provides an unprecedented means for people to express themselves, to assemble and participate, and opens new opportunities to improve access and inclusion. The text underlines the importance of empowering “learners” by providing the means to acquire the skills and competences for democratic culture, and by enabling them to tackle the challenges and risks arising from the digital environment and emerging technologies. This Open Forum will discuss the principal ways in which the Council of Europe’s Recommendation has sought to promote digital citizenship education through the acquisition of competences for learning and active participation in digital society, and the promotion and protection of human rights, democracy and the rule of law in cyberspace.

30 November, 14:15 - 15.15 CET

Open Forum #75 Combating Hate Speech – Answering the H & 5 W’s Questions

Co-organised session by the Council of Europe and the United Nations Office on Genocide Prevention and the Responsibility to Protect.

Hate speech is a rising phenomenon posing a direct threat to democracy and human rights. Therefore, the Council of Europe has recently adopted a Recommendation on combating Hate Speech containing a set of guidelines for the member States and other key stakeholders towards a comprehensive strategy to combat it. Member States are called to implement adequately calibrated and proportionate measures covering legislative frameworks and non-legal measures, such as education and counter-speech, to assist those targeted by hate speech, conduct monitoring and ensure national and international co-operation. In June 2019, the Secretary-General of the United Nations launched the UN Strategy and Plan of Action on Hate Speech aiming to give to the UN the room and the resources to address hate speech and committing to address and counter it in a holistic way and in full respect with international human right standards.

Both the Council of Europe and the UN recognize that, in addition to State authorities, a wide range of key actors, including the Internet industry, can play a crucial role to prevent and fight hate speech. They should therefore seek effective ways to implement a coherent and co-ordinated response. Following a presentation of the available standards, the discussion will focus on most challenging aspects of implementation. Discussing the 5 W’s questions, participants will explore how to translate standards into practice and achieve concrete results.

1 December, 11.50-13.20 CET

Workshop on Cyber-attacks and e-evidence: attribution and accountability

Cybercrime is causing trillions of Euros in damage and harm, is disrupting the functioning of critical infrastructure that societies rely upon, is extorting public and private sector organisations through ransom, is attacking election processes and democratic institutions, is violating the fundamental rights of individuals and is even leading to serious injury or death through attacks on health institutions. How to ensure attribution and accountability of cyberattacks and other types of crime with a digital footprint? Who should care about the e-evidence and what are the challenges and available tools to secure it? How to guarantee that human rights and rule of law requirements are met? Following examples of recent cyberattacks, the workshop will discuss these and other questions. You are invited to join our deliberations in Addis Ababa or online.