Regional Preparatory Meeting Europe, agenda item 5c:
Oral intervention delivered By Tanja Fachathaler on behalf of
the Alliance of NGOs on Crime Prevention and Criminal Justice
Vienna, 26 March 2025

Madam Chair, thank you for giving me the floor.

Speaking on behalf of the Alliance of NGOs I would like to express our appreciation for the opportunity to intervene here before you today.

Digitalisation leads to ground-breaking technologies, but not every innovation means progress. Especially when it comes to new investigation tools, we need to take a very close look as technology has the potential to severely undermine our core values, our freedoms and to violate our rights.

One worrying example is the **use and proliferation of commercial spyware**. The deployment of such technologies represents a severe invasion to privacy and a breach of data protection, allowing unrestricted access to personal communications, location data, and other sensitive information on devices. Pegasus, Predator or, more recently, Paragon Solution's Graphite, are all examples of highly invasive spyware technologies that have been used against human rights defenders, lawyers, politicians, journalists, opposition voices, and civil society members around the world. Cases in various countries, including here in Europe, have shown that the use of commercial spyware is extremely susceptible to misuse.

The proliferation of commercial spyware is recognized by a number of states as a global threat to human rights.
Yet such development is likely going to be accelerated by the new Cybercrime Convention. In several articles, the treaty fails to exclude the collection of stored or intercepted data which was accessed through the use of commercial spyware. As was highlighted in previous NGO interventions, a lot will depend on how the Convention is implemented, once it enters into force. The respect for and protection of human rights have to be at the very centre - in particular as the Cybercrime Convention itself lacks major safeguards.

In fighting new and emerging forms of crime, due regard needs further be given to **existing jurisprudence**. In Europe, the ECHR in a ruling of February 2024 clearly emphasized that the decryption of private communications without adequate safeguards constitutes an unlawful interference with the right to privacy. The attempt to demand a "backdoor" from an instant messaging service, which would have made it possible to decrypt users' messages, was judged to be a clear violation of fundamental rights. The court is very clear: **Encryption is essential for the protection of privacy**, as it prevents not only state authorities but also criminal actors from accessing sensitive personal data.

Real-time **remote biometric identification systems** are another example of such a dangerous development that is being promoted as security-enhancing. The system uses AI to identify people – usually from a remote location. This can be done by **recognising a person's face, body shape or**

movement characteristics. This biometric data is then compared with a reference database. And all this is done without the knowledge or active involvement of the person concerned.

The use of such systems in public spaces not only increases state control over citizens, but also threatens anonymity. Even if the use of such systems is limited to particularly serious criminal offences, such measures create a climate of constant control.

In light of this, we support previous speakers' emphasis on focusing on human rights on our way forward. We recommend that harmful technologies, like the ones I just mentioned, be rejected and alternative measures be used which uphold and strengthen human rights.

Thank you.