**AT Contribution to the questionnaire on new and emerging digital technologies**

**and human rights**

**Core questions (for all stakeholders) - Question 2**

**What are some of the key human rights challenges arising from new and emerging digital technologies? How can these risks be mitigated? Do new and emerging digital technologies create unique and unprecedented challenges or are there earlier precedents that help us understand the issue area?**

In order to provide a well-functioning law enforcement system, law enforcement authorities need to rely on digital technologies and have to take new and swiftly evolving technologies into account when developing new legislative measures in criminal procedural law. While it is necessary to fill gaps arising from new technologies, it might also lead to risks regarding human rights.

In order to rule out the possibility of human rights violations, the legislator takes additional measures to ensure legal protection regarding investigative methods that rely on new technologies as a source of evidence (disclosure of data on transmission of messages, localisation of technical devices, event-specific data storage and surveillance of (encrypted) communication).

These measures usually follow the pattern of „the higher the interference with fundamental rights, the higher the safeguards”. Investigative acts require – amongst other additional safeguards depending on the specific act – a certain threshold of the alleged crime, an order by the prosecution authority with approval by the court, effective legal remedies for persons affected by the investigative measures and the possibility to request independent judicial review.

**Specific questions for States – Question 2**

**How are new and emerging digital technologies affecting the protection and promotion of human rights in your country? What unique challenges or advantages does your country have in responding to the issue? What are the lessons or best practices that can be shared?**

Please refer to answer to question 2. of the core questions.

With regard to criminal procedural law, the most recent challenge Austria is facing is the possibility of surveillance of encrypted communication. In order to have a system in place enabling law enforcement authorities to keep track with ever-emerging communication technologies, the legislator saw the necessity to establish this measure. Section 135a of the Austrian Criminal Code of Procedure will enter into force next year and will be accompanied by the highest safeguards standards.

Furthermore, the large social media platforms have become an essential element of public debate and act as important gatekeepers for citizens seeking, receiving or communicating information. Content that is not indexed or highly rated by any Internet search engine is less likely to reach or be seen by a large audience. Therefore, the algorithms used are of crucial importance for the way in which the right to freedom of expression can be exercised. For many users, it is unclear on which criteria algorithmic decision-making processes are based. Furthermore, in the context of elections, it was evident that with the help of algorithms people from certain groups were specifically addressed and that attempts to manipulate public discussions with automated bots have occurred.