Session II - Organised groups and their new ways of communicating

Speech by the Federal Minister

Ladies and Gentlemen,

Looking at the theme of this session, one can see at first glance how complex it is. This is also borne out by the content of the three keynote speeches: right-wing extremism on the Internet, cybercrime of all kinds and the risks it poses for children and young people, and street crime. New means of communication also undoubtedly bring new challenges and dangers. The Council of Europe and its member states have already responded to this situation. The Council's Convention on Cybercrime and its Protocol can rightly be regarded as milestones in the development of a body of law. Another Legal development in this field was also advanced by the fact that the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse criminalises grooming, or the "solicitation of children for sexual purposes" as the offence is called in the Convention. At the time of the Convention's signature in 2007 this was still new territory, and the possibility of making a reservation was accordingly provided. Four years later the European Union included an, in essence, identical offence in the Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography – but no longer with the possibility of a reservation, which therefore makes the provision mandatory. In the process of implementing these requirements in Austria a further step was taken in recognising that such behaviour must be punished not just when the child was approached over the Internet, but also where contact was made in the event of physically, for instance if someone stood in front of a school and distributed flyers

which advertised a modelling competition or the opportunity to take part in a photo shoot, but the perpetrators' real intent was sexual exploitation. In Austria the offence was accordingly broadened to include this aspect, with effect from 1 January this year. Our criminal law has therefore travelled through cyberspace back to real life.

May I make one clarification in this regard: the theme of the session is very openly worded. It is apparently not confined to organised *criminal* groups or to the misuse of new ways of communicating in order to commit crimes. However, I think it necessary to add that we have these issues in mind when we address this theme in our capacity as Justice Ministers of the Council of Europe member states,.

The right to respect for private correspondence, including emails, text messages and telephone conversations, freedom of opinion, which includes the freedom to receive and impart information and ideas, and freedom of association and of assembly are all enshrined in the European Convention on Human Rights, and in Austria they rank as constitutional law. They are the pillars that support our free democracies and, as such, are irremovable. All these basic rights are nonetheless subject to a statutory reservation. They can therefore be restricted by means of legislation. However, this does not mean that the legislator has carte blanche. In principle, interference with basic rights is permissible only where it is indispensable or necessary in a democratic society for specific purposes, such as national security, the prevention of crime or the protection of the rights of others. A lower yardstick of admissibility, for instance that interference would be quite handy for the purposes of a prosecution or would make things easier or cheaper, is in itself not sufficient.

In this connection, the European Court of Human Rights says that there must be a "pressing social need". The legislator accordingly does not have carte blanche to

impose restrictions on communication in cyberspace. However, calls for complete freedom on the Internet, such as those made, above all, at its very beginning and those made more recently in connection with the issue of protecting intellectual property, must also be resisted.

At all events the times are long gone when the new media and means of communication were often regarded with scepticism and suspected of being used primarily by people who also had criminal purposes in mind. The times are also long gone when the Internet could be dismissed as a plaything for "techno-nerds" or the like. Nowadays one need only see how children handle smartphones.

In Austria the proportion of Internet users in the population as a whole is currently around 78%, and in the 16 to 24 age bracket it is even 98%. Already an estimated 80% of 6 to 11 year-olds, in those households where they have the opportunity, are Internet users. No business or administrative entity could exist nowadays without making use of information and communication technology.

In my opinion that has three implications. Firstly, there must be a secure framework, which requires that the necessary infrastructure and its maintenance must be guaranteed. This concerns not only technical infrastructure, but also an area of legal certainty on the Internet. Secondly, it means that any government intervention in this area does not affect just a few people, but ultimately impacts us all. Accordingly, the measures must be taken in a discerning way and be as purposive as possible. For example, it would make no sense to ban encryption software simply because it is also used by organised criminal groups to conceal their conspiratorial communications. Similarly, it would be somewhat excessive to prohibit the possession of several mobile phones simply because it is a current practice of

criminal organisations to resort to frequent changing of mobile phones, so as to make themselves harder to trace. On the other hand, such widespread availability also means that the new means of communication are nonetheless *also* used if not preferred by criminals, whether because the communication technology is of direct use in the commission of offences or because it can be utilised merely to organise "conventional" crimes.

For the investigation and prosecution either of "conventional" offences in committing which information and communication technology has been utilised, or of specific cybercrime offences, a similar situation applies as for the actual legislation punishing and prohibiting these offences. The investigating and prosecuting authorities must in no way find themselves cut off. They must have the right equipment and also the training to ensure that the possibilities afforded by technical progress are not exploited more in the committing than in combating crime. However, as already mentioned, this is subject to one restriction. Where technical surveillance and tracking can be achieved only at the cost of considerable interference with basic rights, a very strict proportionality test must be applied and the measures, albeit technically feasible, must perhaps not be implemented. Freedom is not just freedom to commit crimes. Freedom means in particular being able to enjoy the guarantees of fundamental rights as established in the European Convention on Human Rights. I think we need to place ourselves squarely against the background of the human rights tradition of the Council of Europe when we consider how to respond to the use of new communication technologies by organised groups.