INGO OING
CONFERENCE OF INGOs
OF THE COUNCIL OF EUROPE
CONFERENCE DES OING DU
CONSEIL DE L'EUROPE

The information society – progress made and the threats facing public authorities and NGOs

Report on the thematic debate at the Conference of INGOs of the Council of Europe

27 January 2017, Room 1, Palais de l'Europe

Moderator: Anna Rurka – President of the Conference of INGOs of the Council of Europe

Opening

Anna Rurka, President of the Conference of INGOs, welcomed:

- the Chair of the Rapporteur Group on Democracy (GR-DEM) of the Committee of Ministers, Ambassador Jurevičienė, for the joint opening of the debate;
- the deputies from the Permanent Delegations of France, Iceland, Czech Republic, Denmark, Finland, Serbia and Sweden;
- the Chair of the CDDH, Brigitte Konz;
- the guest experts, Sébastien Fanti, Lawyer at the Valais Bar Association, elected to the post of Data Protection and Transparency Officer of the canton of Valais in Switzerland, and Jedrzej Niklas from the Panoptykon Foundation (Poland), Alexander Seger, Head of the Cybercrime Division, and Silvia Grundmann, Head of the Media and Internet Division – Information Society and Action Against Crime Directorate, Council of Europe;
- the representative(s) of the Secretariat.

She highlighted the importance of the subject of the debate and stressed the need not only to think about the overall impact of digital technology on human rights, education and democracy, but also, in particular, to debate the accessibility of technological progress and to see how every citizen could be protected and protect themselves against the threats which could easily compromise their right to privacy. She then gave the floor to Ambassador **Jurevičienė**, Chair of the Rapporteur Group on Democracy (GR-DEM) of the Committee of Ministers, and highlighted the good contacts that had developed between the Committee of Ministers and the Conference of INGOs. The Ambassador confirmed the importance of regular dialogue between the GR-DEM and the Conference of INGOs in forging ties, pointed out that the subject of the debate was central to current concerns and mentioned the conference on online freedom of expression to be held in Cyprus in April 2017, during the Cypriot chairmanship of the Committee of Ministers. In her view, the tools developed for the Internet Governance Strategy should make it possible to apply the same rights "online" as offline. Repressive measures could have a chilling effect, and attention must be paid to over- and under-regulation. It was necessary to properly implement the existing recommendations, which were important tools for the defence of democracy, namely:

- Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors, adopted on 30 April 2014;
- PACE Resolution 2035 (2015) on protection of the safety of journalists and of media freedom in Europe, PACE Resolution 2141 (2017) Attacks against journalists and media freedom in Europe;
- PACE Resolution 2060 (2015) and Recommendation 2073 (2015) on the protection of whistle-blowers;
- The Council of Europe Convention on Access to Official Documents, signed on 18 June 2009, which required only one additional ratification for it to enter into force;
- Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms concerning unlawful interference;

In conclusion, she stressed the importance of strengthening democracies online.

Standards and tools developed by the Council of Europe: Internet Governance Strategy (2016-2019) and the Human Rights for Internet Users guide

Silvia Grundmann, Head of the Media and Internet Division – Information Society and Action Against Crime Directorate, DG I, also thanked all of the Ambassadors for their willingness to engage in dialogue with civil society. She explained that the Steering Committee on Media and Information Society (CDMSI) was working on e-standards which would be submitted to the Committee of Ministers for approval. If they were adopted, the member states would be required to abide by the recommendations, but they would also need support to enable them to implement all of the standards. Two main sources were available to them:

- Internet Governance Strategy 2016-2019 "Democracy, human rights and the rule of law in the digital world".

- The Human Rights for Internet Users guide (available in English, French, Albanian, Arabic, Bulgarian, Dutch, German, Greek, Italian, Portuguese, Russian, Serbian, Spanish, Turkish and Ukrainian), which was essential for civil society and dealt with the rights and duties of Internet-using citizens, while helping governments with policy development. It was based on the case-law of the European Court of Human Rights and consisted of three sections:
    - standard recommendations to the member states;
    - a guide for citizens;
    - an explanatory memorandum, or genesis ("why and how").

The CDMSI sought to support the implementation of Council of Europe standards:

- It drafted annual reports for the Secretary General of the Council of Europe, who was very active in the field of information and regularly raised issues with the member states. The challenges were still enormous;
- It studied the situation in the 47 member states (accessible online for each country) and analysed the filtering, blocking and taking down of documents.

It would be desirable to identify funds in order to raise the awareness of judges and journalists.

Alexander Seger, Head of the Cybercrime Division of the Council of Europe, explained:

- that cybercrime was threatening the three fields of activity of the Council of Europe;
- that billions of pieces of data were stolen or blocked and that less than 1% of cases were prosecuted in the courts.

With regard to cybercrime, there was an urgent need to find evidence of conspiracy to carry out terror attacks and prevent more children from being abused (grooming).

States must prosecute offences, and could rely on a "triangle":

- the Budapest Convention (No. 185) and the additional protocols thereto (which had been ratified by Senegal, Mauritius, Canada, the Dominican Republic and the USA), which was "the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security". It also contained a series of powers and procedures such as the search of computer networks and interception. It established procedural powers and international co-operation;
- the Cybercrime Convention Committee, which brought the States Parties to the Convention together and whose aim was to facilitate the use and practical implementation of the Convention, the sharing of information and scrutiny of any future amendments to legislation.

Background

Sébastien Fanti, Lawyer at the Valais Bar Association (Switzerland) elected to the post of Data Protection and Transparency Officer of the canton of Valais, and member of the International Association of Lawyers (UIA, an INGO holding participatory status with the Council of Europe and active through a network of lawyers dealing with advanced technologies and Internet governance) voiced clear support for digital education for children and for the integration of robotics education into daily life. In his view, it was time to change and to establish clearly what was acceptable and what was unacceptable. People had a choice and did not have to remain at the mercy of the giants (Google, Microsoft, etc.). It was necessary to try to be pragmatic and protect citizens' rights, while also being vigilant and developing protective reflexes. There was a need to set limits, establish safeguards in relation to robotics, algorithms and the Internet, and prevent points of friction from developing.

- Learning processes should be changed to make them consistent with effective and presumed use (coding – "tuning" plan). Children must be encouraged to use the tools of the future, rather than "Word", which was set to disappear. Learning needed to be changed and made compatible with what the future would be. There was an urgent need to join forces so as to avoid duplication and strengthen safeguards. It could not be said where technological development (artificial intelligence) would stop, and there was an urgent need to improve and encourage reflection;
- Should e-prosecutors not be appointed, to whom complaints could be referred "online" and who could remind people of the law where necessary? A legal defence platform could be considered;
- "Sextortion" and other e-offences were committed from countries in Africa where there was little protection;

- Rules came along too late (after billions of pieces of data had been stolen, recorded and analysed without anyone's knowledge!) and it was important not wait for something to go wrong before acting.

Individuals were responsible, had a choice and must initiate changes. Citizens needed to be offered a "strong digital status". The strength of a democracy was measured in terms of its weakest citizens, and this link in the chain did not have the means to defend itself at the moment.

A virtuous approach was needed (for example, for each robot which replaced a person, training must be offered through a retraining fund). In Sébastien Fanti's view, the time had come for the Council of Europe and NGOs to lead the way and initiate a change in practice which was necessary to prevent people from being pigeon-holed because of their non-integration into a digital society which was currently creating elites but neglecting its most vulnerable members. The time had come to start a virtuous circle to restore equality of opportunity and offer everyone the same professional and personal opportunities to take advantage of technological advances.

New technologies, privacy and surveillance from the perspective of human rights organisations

Jedrzej Niklas described the Panoptykon Foundation as a Polish NGO dedicated to human rights issues in relation to digital technology. Its aim was to teach citizens how to use confidentiality tools when using the Internet and make them aware of the legal and ethical aspects of technology.

Technology had two facets:

- It could help to support/protect human rights;
- It could have the negative effect of surveillance. The great majority of people were not aware of the scale of surveillance. People were increasingly being monitored and categorised by big companies which held an incredible amount of information about them. Individuals' privacy was being intruded upon without their knowledge in order to monitor their lives and obtain data for various reasons. These had initially been commercial, but increasingly for reasons of "public security" and under the pretext of "risk management", everything was being monitored, filmed and recorded, from the supermarket to the car park, and often elsewhere;
  The algorithms used took decisions about our lives. People were "categorised", which affected their lives against their will. Individuals could no longer access given websites because the algorithms had calculated a certain profile for them. New tools were being developed. The most vulnerable people were those who were under the most surveillance. Migrants, for example, were placed against their will in a "second-class" category which was under greater surveillance. However, algorithms could get things wrong. In the United States, there were people who were regarded as "suspicious" due to system errors. This created a latent climate of mistrust and fear. These "walls" being built masked the real problems and led to unjustified suspicions and a climate which was not conducive to inclusion. All too easily, people allowed their freedom to be taken away without thinking about the real consequences (surveillance cameras had never deterred those who really wanted to commit a crime).

  So it was necessary to take action to ensure ethical data protection.

Discussions with the audience:

- Question: Should people not be afraid of digital education for children, technological progress and the integration of robots into their daily lives leading to the gradual disappearance of oral communication, writing and reading?
  Answer: Nobody had the right to deprive children and young people of the opportunity to familiarise themselves with technologies which they would need in the information society. It was therefore necessary to include the opportunity to learn at all costs, without this doing away with conventional means of communication;
- The far-reaching changes in the way that information was produced and consumed called for special consideration of youth and education. The angles of Internet governance and protection of privacy could only have an impact to the extent that all citizens, starting with the youngest, were adequately equipped to deal with these changes and this new environment. And at the moment, they were not. Digital tools were supposed to provide "equality" of opportunity, but people were not ready to give access to the weakest. Civic and citizens' education must reflect changes in society and provide education about the media, education about digital tools and education about critical thinking and the related tools. Given governments' disengagement from these issues and also a woeful lack of innovation and failure to consider these new issues, the vacuum of responsibility was, unfortunately, having to be filled increasingly by NGOs, especially those running youth and non-formal education projects. This had to be borne in mind and taken into account in the work of the Conference of INGOs, which needed to engage in advocacy;
- In terms of concrete action, AEGEE / European Students' Forum (a member of the Conference of INGOs) was currently conducting a European Citizens' Initiative across the European Union to renew civic and citizens' education in Europe, which the whole of the Conference must support;
- Society was profiled by what was served up to people on the Internet. It was necessary to prevent social exclusion and consider a holistic approach which also included a theological perspective (see the Church of Scotland publication);
- Co-operative freeware was needed: people could work in "open source" applications, such as "Threema", for the modest price of €20, and should be careful regarding clouds;
- Vigilance was needed to protect citizens from extremist parties. The Internet must not be a tool for populists spreading "acceptable racism" targeted at certain groups of citizens;
- Critical thinking education must be based on abilities and collaborative learning processes... Education would not change quickly enough;
- Misuse of private data, either for "commercial" reasons or through state monitoring, should be stopped. The limits of power needed to be defined very clearly;
- The challenge was enormous. Aberrations and exaggerations did a lot of harm. It was necessary to move towards a "digital habeas corpus" to enable appeals to be made to an entity independent of states, a kind of "special court" that could also compensate victims;
- In reality, no computer or data could stop a terrorist;
- Data protection laws must be able to help prosecutors, who could only make decisions on the basis of laws;
- Would technological solutions at source not be more effective than laws?

Governments must take responsible, ethical, brave and firm decisions about accepted/rejected tools (e.g. Apple School was banned in schools in Switzerland; Windows 10 was banned in Switzerland; Microsoft had finally accepted that at the global level, processes should be controlled in "open source"). Candidates in elections should give signed confirmation that they accepted rules of ethics. States urgently needed to work together to develop shared legal frameworks. Documents were not enough, laws needed to be enforced. INGOs should put themselves at the forefront, as they had a very important role to play.

<u>Summary</u>

- It was high time that civil society acted and co-operated with states to maintain a balance that respected human rights. It was necessary to work together with digital giants (Google, Facebook, Microsoft, etc.) to guarantee and preserve people's rights. It was also necessary to develop more responsible behaviours and protection reflexes, set limits, especially for algorithms and robotics, build capacities and establish an e-legal platform for the defence of citizens, and even consider setting up an entity independent of states to which complaints could be made if harm was caused;
- States must prosecute cybercrime offences, even if these offences could be "uncomfortable" for them;
- Excessive surveillance conducted under the pretext of "risk management" must be rejected;
- There needed to be ethical data protection which was not detrimental to the inclusion of vulnerable persons and did not spread "acceptable racism" targeted at certain groups of citizens;
- All citizens must be adequately equipped to deal with the changes and this new environment. High-quality digital education must take account of changes in society and guarantee that <u>everyone</u> had access to media education and education about critical thinking and digital tools to make learning compatible with humankind's future and ensure integration into a digital society which did <u>not</u> neglect its most vulnerable members;
- Citizens must be encouraged to use co-operative freeware to work in open source;
- The Conference of INGOs had a duty to address these issues in its work and would not fail to remind governments to take ethnical, brave and firm decisions.

Didier SCHRETTER, special adviser on communication and representative of the Conference of INGOs on the Steering Committee on Media and Information Society (CDMSI) of the Council of Europe, thanked all of the speakers for the high-quality debate about a very complex issue. He explained the context surrounding the launch of a wider debate as part of the work being done within the Conference of INGOs and other organs of the Council of Europe. Civil society must grasp the key issues that raised questions so that it could debate them, draw the necessary conclusions and resolutely defend its rights to privacy and freedom of expression. It was necessary to incorporate all aspects into an overall approach and to have the relevant expertise in order to act in a positive, creative and constructive manner. Acting bravely in co-operation with all partners was the right way to move forward.