Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE

Input Session III:

„What Should States Do to Promote an Open Internet?“

©

Hannes Tretter

Professor for Fundamental and Human Rights Law,
Research Centre Human Rights, University of Vienna
Co-director, Ludwig Boltzmann Institute of Human Rights (BIM)

“What are the limits and also the scope of state responsibilities to balance an open and secure Internet?” The legal frame

- According to international and European human rights standards as well as the case-law of the ECtHR and CJEU, the freedom of opinion, expression and information is an indispensable condition for the development of human beings, the participation in public debates, and therefore a cornerstone for a free and democratic society.
- Insofar, States are obliged to guarantee this right – namely to respect, protect and promote it. That includes also the right to use the existing communication technologies and to have free access to them.
- However, these rights are not of an absolute character, they may be restricted by domestic law if this is necessary in a democratic society in order to preserve public interests and freedoms and rights of others.
- The dogmatic principle of proportionality enables to find a fair balance between the opposing rights and interests.

Threats and limits

- **The free and open use of the Internet is increasingly threatened by**
  - attacks against its technical infrastructure and its use by States, companies and individuals, damages or misappropriations of data bases, blocking of websites, extortions, etc.
  - spreading fake news, untrue or half-true information – “just for fun”, to earn money, or in order to track certain ideological, political or other objectives intending to affect or manipulate people.
  - invocations to commit terrorist acts or other forms of violence.
  - recruiting of terrorists, financing and promoting radical, violent and or fundamentalist movements and organisations which don’t comply with the fundaments and values of legitimate States, and subverting their governments and/or societies,
  - hate speech.
- All mentioned threats may be defeated according to the exception clauses of all relevant international and European human rights conventions, if the measures taken against are provided for in domestic law and are proportional to the legitimate aim pursued.

Opposing rights and interests
How to protect them

- Respective expressions and information quite often interferes with following rights and interests:
  - maintenance of the fundaments, principles and basic values of a State and its society,
  - stability and functioning of a State and its institutions,
  - State integrity and national security,
  - public safety and prevention of disorder or crime,
  - fundamental rights of citizens, *inter alia* personal integrity, privacy, protection against defamation, right to (objective) information, etc.
- Very often respective internet accounts, blogs and websites are blocked – with the problematic effect that one cannot distinguish between legal and illegal postings, what would be in contrast to freedom of expression and copyrights.
- In contrast, a proportional reaction would be the deletion of respective internet-postings why this alternative should be given preference.
- However, deletion needs mutual administrative and/or judicial assistance by State authorities, based on trust and legal certainty.

"What could the OSCE do to promote such a balance, taking into account different national approaches?"

- It is clear that an open and secure Internet cannot be achieved by domestic measures alone because it is a global technology without frontiers.
- Around and after 1990, the OSCE showed that it can be a "trend- and standard setting organisation", promoting democracy, rule of law and human rights → remember the Vienna Concluding Document 1989, or the Copenhagen Meeting of the Conference on the Human Dimension.
- Therefore, the OSCE should try to develop commitments to establishing standards for an open and secure Internet within its region. Beside the OSCE Decisions 1106 and 1202 on confidence-building measures, guidelines for such an initiative could be, *inter alia*, the
  - EU Directive 2016/1148 on security of network and information systems
  - EU General Data Protection Regulation 2016/679
  - CoE Convention on Cybercrime (the "Budapest Convention") 2001
  - CoE Recommendation 1997/20 on Hate Speech and EU framework decision 2008/913/JI against racism/xenophobia
  - UN Convention for the Suppression of Financing of Terrorism

Some legal minimum requirements as OSCE standards

- Since within the OSCE region different national approaches exist with regard to the given topic, the OSCE should focus on the identification of minimum human rights and rule of law standards, among them:
  - The Internet shall be regulated only by democratically originated law.
  - According to the CoE Cybercrime Convention, States have to provide effective sanctions for offences against the confidentiality, integrity and availability of computer data systems as well as against acts of a racist and xenophobic nature committed by them.
  - Any surveillance and interference of the Internet shall be under control of the independent judiciary. There shall be no decisive power for the police or secret services, all measures have to be mandated by courts.
  - Effective remedies on the national level shall provide access to justice for anybody whose rights or interests have been affected.
- In addition, the OSCE should promote the elaboration of an "OSCE Convention for an Open and Secure Internet" establishing a regulating authority with discretionary competence to deal with complaints against final domestic decisions (poss. co-financed by digital service providers).

"How can civil society be involved effectively in addressing the balance between an open and secure Internet?"

- Access providers must not exercise a content-related control, what would amount to pre-censorship and would not only violate freedom of expression but also copyrights.
- Nevertheless, all digital service providers should adopt all necessary measures to comply with their human rights compliance in the frame of their service-oriented tasks and responsibilities.
- By contrast, OSCE should promote and support reliable and independent NGOs to take over monitoring, reporting and advising tasks.
- Cyber volunteers could play an important role in that regard, guided by regionally or internationally active NGOs which could provide assistance and knowledge in a democratically participative way.
  - Like ICANN, an US NGO that informs how to keep the Internet running smoothly (i.a. giving support at the allocation of domains).
- Such participation of civil society should be accompanied by region-wide political and human rights education, in particular of the youth, recalling the fundaments, principles and values of democratic societies as they find expression in the internationally recognised human rights provisions.

Thank you very much for your attention!

PPT available on:

http://bim.lbg.ac.at/