

*”The Internet, Youth and  
Radicalization”:*

# **An overview of the legal perspectives**

*9th session, Intergovernmental Council for the Information for All Programme, May 31th 2016*

**Speaker: Dan Shefet**

# Outline

- **Introduction**
- **The Problem / Challenge**
- **Current Legal Framework**
- **Survey / Questionnaire**
- **Specific Legal Problems**
- **Policy Recommendations**

*“When individuals of ambiguous affiliation are capable of undertaking actions of increasing ambition and intrusiveness, the very definition of state authority may turn ambiguous...*

*The danger is compounded by the plausible deniability of those suspected of such actions and by the lack of international agreements for which, even if reached, there is no present system of enforcement. A laptop can produce global consequences.”*

*“It will not be possible to conceive of international order when the region through which states’ survival and progress are taking place remains without any international standards of conduct and is left to unilateral decisions...*

*Absent articulation of some rules of international conduct, a crisis will arise from the inner dynamics of the system....*

*Order should not have priority over freedom. But the affirmation of freedom should be elevated from a mood to a strategy”.*

*“...Are these networks going to be the first institutions in human history liberated from occasional abuse and therefore relieved of the traditional checks and balances?”*

# Human Rights Council 2016/NGO Submission

- *”This joint written submission raises serious concerns regarding the potential impact of initiatives to counter and prevent ”violent extremism” (PVE) on the enjoyment of human rights and fundamental freedoms”*
- *”...criminalising or otherwise prohibiting or sanctioning conduct without a clear definition is incompatible with the principle of legality, a basic rule of law precept.”*
- *””Violent extremism” and related terminology such as ‘radicalisation’ are poorly defined concepts, which open the door to human rights and other abuses”*
- *”...many PVE initiatives have a significant potential to threaten the human rights to equality and freedom from discrimination, the right to privacy, and the freedoms of expression, association, and religion or belief”.*

Joint UNESCO and Government of Quebec organised conference  
to be held in Quebec (Canada) on October 31th/November 1st  
2016:

***”Radicalization, Internet and Youth: Acting and  
Preventing Together”***

*Report on:*

*”Policy options and regulatory mechanisms for managing  
radicalization on the Internet”*

# Sustainable Development Goal 16

- Sustainable Development Goal 16 (“SDG 16”) is dedicated to the promotion of peaceful, just and inclusive societies and accountable institutions and in particular for the purposes of the Report, SDG 16 includes the following:

*Significant reduction of all forms of violence and related death rates everywhere*

*Promotion of the rule of law at the national and international levels and ensuring equal access to justice for all*

*Ensuring public access to information and protection of fundamental freedoms, in accordance with national legislation and international agreements*

*Strengthening of relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime*

*Promotion and enforcement of non-discriminatory laws and policies for sustainable development*

# International instruments I

- The International Covenant on Civil and Political Rights (ICCPR)
- The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)
- Universal Declaration of Human Rights (UN, 1948)
- Vienna Declaration and Programme of Action (World Conference on Human Rights, 1993)
- Declaration of Human Duties and Responsibilities (UNESCO, 1998)
- Universal Declaration on Cultural Diversity (UNESCO, 2001)
- International Covenant on Civil and Political Rights (ICCPR)
- International Covenant on Economic, Social, and Cultural Rights (ICESCR)
- Convention on the Elimination of All Forms of Racial Discrimination (ICERD)

# International instruments II

- Convention on the Elimination of All Forms of Discrimination Against Women
- Convention on the Prevention and Punishment of the Crime of Genocide
- Geneva Convention Relative to the Protection of Civilian Persons in time of War
- Additional Protocol of June 8<sup>th</sup> 1977 (Victims of non-international Armed Conflict, Protocol II)
- UN General Assembly Resolution “Measures to eliminate international terrorism” A/RES/70/120
- Report of the Secretary – General (April 27<sup>th</sup> 2006) “Uniting against terrorism: recommendations for a global counter-terrorism strategy”
- Plan of Action to Prevent Violent Extremism, Report of the Secretary-General (December 24<sup>th</sup> 2015)
- UN General Assembly Draft resolution (February 9<sup>th</sup> 2016) Secretary-General’s Plan of Action Prevent Violent Extremism”
- Resolution 2250 (2015) Adopted by the Security Council on December 9<sup>th</sup> 2015



# Regional instruments

- The American Convention on Human Rights
- American Declaration of the Rights and Duties of Man
- The African Charter on Human Rights and Peoples' Rights
- Cairo Declaration of Human Rights in Islam
- Maputo Protocol
- The Arab Charter on Human Rights
- The ASEAN Human Rights Declaration
- Charter of Fundamental Rights of the European Union
- European Convention on Human Rights
- EU Directives and Regulations

# Other sources of law

- Audiovisual Media Services Directive
- Electronic Commerce Directive
- Consumer Right Directive
- Digital Millennium Copyright Act
  - *”Why does personal integrity deserve less protection than personal creativity?”*

# Council of Europe

## Convention on the Prevention of Terrorism

### Article 5 – Public provocation to commit a terrorist offence

1 For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

# **Council of Europe Convention on the Prevention of Terrorism**

## **Article 6 – Recruitment for terrorism**

1 For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.

# Budapest Convention on Cybercrime

2 ... the term "child pornography" shall include pornographic material that visually depicts:

- a a minor engaged in sexually explicit conduct;
- b a person appearing to be a minor engaged in sexually explicit conduct;
- c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

# Survey: The questions I

- Is the act of radicalization as such a penal offence in your country?

*In the affirmative please list citations to the relevant statutes/regulations including a specific reference to the definition of radicalization employed.*

*In the negative does your country apply penal sanctions against radicalization on the basis of analogy from other offences e.g. “hate speech”, “incitement to hatred”, “apology for genocide”, “solicitation of murder” or defamation law?*

- Does your country extend penal liability on internet radicalization to intermediaries and if so on the basis of a general theory of complicity or media law or a specific statute or regulation?
- Can legal entities: companies, associations or a group of persons be held criminally liable under your country’s laws and regulations on internet radicalization?

# Survey: The questions II

- Does your country apply a specific statute of limitation on penal liability for radicalizing content starting for instance from the first date the content in question was published?
- Which of the following technological remedies does your country allow judges or law enforcement agencies to order/apply for the purposes of countering internet radicalization: Take down notices, Lowering/hiding page ranking, Filtering Blocking, Right of response, Rerouting Denial of access and defensive hacking, Refusal of access (on author, host and user), Suspension of ISP license, Others.
- Please provide statistics on take downs and similar remedies in your country

# Survey: The questions III

- Has your country put in place user platforms where radicalization content may be reported by the internet community?
- Has your country introduced legal obligations or “soft law” obligations and corporate governance guidelines covering ISPs, search engines, social media, hosts and platform liability in the field of online radicalization including their cooperation with law enforcement agencies, content review? In the affirmative please provide citations.
- Has your country adopted a strategy/policy on countering internet radicalization (similar for instance to the UK Contest program). In the affirmative please list the specific legislative and regulatory measures that have been adopted pursuant to said strategy/policy?



# Survey: The questions IV

- Does your country allow extradition of authors and accomplices charged with internet radicalization in other countries?
- For the purposes of countering online radicalization has your country introduced specific:

*Enforcement tools, orders/injunctions (e.g. fast track procedures, derogations from prior warrant requirements and the application of investigative measures which may be applied specifically to the area of internet radicalization on an administrative basis).*

*Specific tribunals/administrative bodies with oversight authority including the application of the remedies listed under point 5 above?*

# Survey: The questions V

- Does your country allow judicial and or administrative decisions/measures to have extraterritorial effect e.g. orders to delist all domains names as opposed to restricting such decisions/orders to local domain names (i.e. global reach). Does your country subscribe to a jurisdiction criterion based on nationality (of author, ISP or potential victims) or access to site (focused or general) in the field of online radicalization? Can orders against ISPs, search engines, hosts, social media and platforms be enforced against the subsidiary of said company based in your country (daily penalties, suspension of license etc.)?
- How does your country ensure that human rights (freedom of speech and religion and right to privacy in particular) are not violated in the process of investigating and enforcing counter radicalization efforts online?

# Specific legal problems

- Territoriality and jurisdiction
- Global reach
- Enforcement (local subsidiaries/daily penalties)
- Statute of limitation
- Special procedural laws
- Extradition
- International cooperation
- Administrative measures and judicial control
- Complicity and joint and several liabilities (including ICT's)
- Risk of abuse/censorship
- Impact on human rights and fundamental freedoms

# Policy recommendations

- User reporting mechanisms
- Private sector obligations
- Cyber Dispute Regulation Mechanisms
- Liability and complicity
- Mandatory pro-active technical measures
- Fast track procedures (judicial and administrative)
- Real time or effective judicial oversight ex post

**Thank you for your attention**