Policy options and regulatory mechanisms for managing radicalization on the Internet

Paris, 30 September 2016

"[…] I firmly believe that in a free democratic society, freedom of speech and expression is one of the most prized freedoms which must be defended and upheld at any cost and this should be particularly so in the land of Voltaire. It is indeed unfortunate that in the world of today, when science and technology have advanced the frontiers of knowledge and mankind is beginning to realize that human happiness can be realized only through inter-dependence and cooperation, the threshold of tolerance should be going down. It is high time man should realize his spiritual dimension and replace bitterness and hatred by love and compassion, tolerance and forgiveness."

Justice Prafullachandra Bhagwati

Dan Shefet

(Individual Specialist)

ACKNOWLEDGEMENTS

The author wishes to thank the following for their support, valuable advice and input throughout the drafting of the Report:

Dr. Indrajit Banerjee and his team in UNESCO's Knowledge Societies Division

The UNESCO Delegates and Ministries of Justice/Interior of countries that have participated in the Country Survey.

Alexander Linden, Honorary advisor to the French Supreme Court

Janice Duffy, Researcher, Australia

Pavan Duggal, Supreme Court Lawyer, India

Tom Høyem, Former Minister in Denmark under Poul Schlüter

Francesca Musiani, Researcher at the CNRS Institute for Communication Sciences and Member of the French National Assembly's Commission on the Law and Rights in the Digital Era

Sami Mahbouli, Lawyer at The Tunisian Supreme Court and Columnist

Sabine Leutheusser-Schnarrenberger, Former Minister of Justice under Angela Merkel

Marc Randazza, First Amendment Attorney, United States

Viswa Sadasivan, CEO of Strategic Moves (Consultancy agency in Singapore) and former member of the Singaporean Parliament

Mr K. Shanmugam, Minister for Home Affairs and Minister for Law, Singapore

Veronika Wand-Danielsson, Ambassador of Sweden to France

Fareed Yasseen, Ambassador of Iraq to France

David Wright, Director of UK Safer Internet Centre

"Since wars begin in the minds of men, it is in the minds of men that the defense of peace must be constructed" (UNESCO Constitution, 16 November 1945).

TABLE OF CONTENTS

INTRODUCTION

If we look back over the past 9 months preceding the date of this report (30 September 2016) there have been some 1320 terrorist attacks causing 11202 fatalities around the world.[1]

Awareness of the role of the Internet as a facilitator or catalyst of radicalization has grown over the years (as it will be seen from Section 1 on The International Community's Policy on Internet Radicalization).

Recently both the FBI and President Obama publicly expressed the view that the perpetrator of the attack on a club in Orlando on 16 June 2016 had been radicalized by the Internet[2].

Numerous initiatives have been taken to identify the roots and causes of radicalization and the elaboration of efficient legal as well as sociological, psychological, political and educational responses.

The atrocious acts committed by different terrorist groups have led several countries to take drastic legal measures aimed at protecting the right to life as enshrined in the International Convention on Civil and Political Rights, Art. 6.1 and other values supported by the international community. These measures may in some cases encroach upon correlative human rights and in particular freedom of speech, the right to information and the free practice of religion.

The State of Emergency Decree in France is an example of such legislation which took effect on midnight 13 November 2015 immediately after the Bataclan Tragedy.

The Decree ultimately led to a call for Constitutional change and the State of Emergency was extended till January 2017 after yet another terrorist attack in Nice on 14 July 2016.[3]

Almost all countries around the world have taken steps to fight radicalization

In this Report we shall analyze the legal measures taken specifically against online radicalization adopted by 32 countries representing the six geographical regions of UNESCO. We shall also analyze international treaties, European directives and resolutions at a regional and international level in an attempt to identify grounds of a common understanding and a consensual approach to measures against online radicalization by the international community.

At the international and regional level, the United Nations, the Council of Europe, the East African Community, the Organization of American States, the Association of South East Asian Nations, the African Union and the League of Arab States have passed resolutions and adopted treaties providing for harmonization of laws, the creation of new criminal offences and the establishment of rules governing jurisdiction and cooperation by way of information sharing and coordination of resources (Section 1).

The Report seeks to address the following legal questions and challenges in particular:

---

[1] According to Storymaps (2016). Available at: http://storymaps.esri.com/stories/2016/terrorist-attacks/ [Accessed 30 September 2016].

[2] Pilkington, E.; Roberts, D. (2016): "FBI and Obama confirm Omar Mateen was radicalized on the internet", The Guardian. Available online at: https://www.theguardian.com/us-news/2016/jun/13/pulse-nightclub-attack-shooter-radicalized-internet-orlando [Accessed 30 September 2016].

[3] On 16 November 2015 president Francois Hollande initiated the first of 4 extensions of the State of Emergency. A bill to change the constitution for "The protection of the nation" was passed on 23 March 2016, but constitutional change has not yet been enacted. Source : http://www.liberation.fr/france/2015/11/16/francois-hollande-annonce-une-revision-de-la-constitution_1413859).

The conditions under which legal regulation of content may be implemented while meeting international human rights standards and in particular those protecting freedom of speech, non-discrimination and the free practice of religion. We shall seek to define the perimeter within which it may be recognized under international law that "radicalizing content" is excluded from freedom of speech protection (Section 3).

Section 3 is broken down into a subsection on "**General Principles of Freedom of Speech**" including the caveat covering abuse (Section 3.a), "**Internet and Freedom of Speech**" (Section 3.b) and "**Specific Restrictions of Freedom of Speech**" (Section 3.c).

Any attempt to regulate content on the Internet or any other medium will face the challenge of the protection accorded to freedom of speech and freedom of information (the latter being a collective freedom rather than an individual freedom).

It is critical to analyze to what extent restrictions of freedom of speech with regard to radicalizing content may be consistent with existing and broadly recognized limitations based on the general abuse caveat or specific content restriction mandates.

A number of international instruments (on a regional and international level) as well as international case law and national legislation/case law based on Media Law, Advertising Law (tobacco, medicine etc.) Crime Prevention Law (child pornography, money laundering, gambling, terrorism), Intellectual Property and Defamation Law (non-exhaustive examples) all ultimately lead to restrictions of freedom of speech. These existing specific (and broadly accepted) limits to free speech will be analyzed in Section 3.c.

In Section 2 we shall attempt to arrive at a viable, comprehensive and predictable **definition of** "**Radicalizing Content**".

The attempts to identify/formulate an efficient and appropriate definition will not be confined to the analysis of legal instruments and jurisprudence, but will also take into account academic definitions applied in sociological and psychological studies as well as the definitions proposed by specialized agencies and Non-Governmental Organizations (preceding the analysis, comparison and identification of the key features of the phenomenon of radicalization leading to a legal definition of "radicalizing content", we shall however turn to the "**International Community's Policy on Online Radicalization**" (Section 1)).

Hereafter the Report will focus on the more practical aspects of monitoring and enforcement in Section 4: "**Online Law Enforcement and Liability**" which is divided into Section 4.a on the "Regulability of Cyberspace" and 4.b on "**Jurisdiction and Extraterritoriality**" followed by Section 4.c on "**Internet Specific Law**", 4.d on "**Private Sector Enforcement and Liability**" allowing us to delimit the range of Parties that may be held accountable for dissemination of radicalizing content and Section 4.e on "**State Responsibility for Private Actors**".

Recent technological developments and terrorist use of the Internet's spectacular potency bear testimony to the fact that governments and law enforcement agencies are no longer able to meet their obligations to protect their citizens against the nefarious consequences of radicalizing content.

Governments have no choice but to solicit or obligate the private sector to cooperate. The private sector wields unprecedented power and control over the infrastructure, architecture and future development of the Internet.

It is therefore legitimate to raise the question whether (and to what extent) the private sector should be under a legal obligation to actively contribute towards the struggle against "radicalizing content".

In the process of answering this question we shall study analogous situations involving private sector responsibility for public services ("outsourcing" of public services, obligations and prerogatives). We find such examples for instance in the field of money laundering, where the private sector has duties ranging from simple diligence and reporting obligations to those of specific action the violation of which carry substantial penalties. This is the subject dealt with under Section 4.d.

Section 5 deals with specific "**Filtering and Blocking mechanisms, Encryption and Counter-Narrative**".

We shall describe the technical options available to content restriction and analyze the legality of their application (procedural guarantees and conditions).

Finally, **Policy Recommendations** will be made on the extent of State and Internet Service Provider[4] accountability, dispute resolution mechanisms, treaty cooperation and specific measures that could be adopted (Section 6).

First we need briefly to describe how the Internet is being used for radicalization purposes and to what extent the Internet actually serves as a catalyst or facilitator of radicalization. This is the subject of the following "**Introductory Chapter**".

The Report's analysis and conclusions are not confined to current events of radicalization. The Report seeks to approach the phenomenon of radicalizing content in the abstract related to any kind of online incitement to perpetrate terrorist acts irrespective of the ideology or creed in question.

The Report is prepared for UNESCO's Communication and Information Sector. The opinions expressed are those of the author and do not necessarily reflect the views of UNESCO or its Communication and Information Sector.

[4] Internet Service Providers ("ISPs"): For the purpose of this Report "ISPs" include search engines, host servers, infra-structure providers (including telecom and broadband providers), access providers, communication service and information providers. Thus a broad definition is applied.

Methodology

The methodology chosen for the Report is that of a qualitative empirical approach.

Empirical data is collected through the Country Questionnaire/Survey (Annex 1) covering 32 countries[5] as well as Non-Governmental Organizations, International Organizations and academia.

The Questionnaire seeks to identify legislative initiatives on a country basis countering online radicalization while at the same time reconciling - often - conflicting human rights (in particular freedom of speech, religion and right to life).

In addition, international legal instruments, resolutions, directives, case law and jurisprudence will be analyzed in an attempt to identify consensus and trends governing online content regulation, cooperation and liability.

The Internet and Radicalization

▪ Brief History of Online Activism

One of the early examples of political activism on the Internet was the Zapatista-movement in Mexico.[6] The Acteal massacre in Chiapas (1997) was disseminated immediately on the Internet resulting in worldwide demonstrations.

The Zapatista movement demonstrated that the Internet had become a catalyst of action (the "war of words" had moved into the Internet). The Rand corporation qualified the use of the Internet by the Zapatista movement as "Digital Zapatism" and notions like "Floodnet" and "Virtual Sit-ins" were coined.

Peace Net appeared in 1986. It enabled political activists to communicate and coordinate action and created a web platform for activism. Peace Net later joined the Institute for Global Communication and the Association for Progressive Communications ("a group of computer activists serving progressive causes in more than 130 countries").[7]

The Electronic Disturbance Theater (created in 1998) further developed "electronic civil disobedience" as a new way of giving "a voice" to opposition against government.[8]

---

[5] Covering the following 32 countries: Denmark, United Kingdom, Tunisia, Albania, Hungary, India, Australia, Germany, Seychelles, Israel, Slovakia, Spain, Sweden, Iraq, Canada, Singapore, Kenya, Japan, Egypt, Brazil, Poland, United States, New Zealand, China, Argentina, Nigeria, United Arab Emirates, France, Tanzania, Russia, Norway and Belgium.

[6] Lacey, M. (2007): "10 Years Later, Chiapas Massacre Still Haunts Mexico", The New York Times. Available at: http://www.nytimes.com/2007/12/23/world/americas/23acteal.html?_r=0 [Accessed 27 September 2016].

[7] Drew, J. (2013) *A Social History of Contemporary Democratic Media*. New York, United States: Routledge.

[8] Wray, S. (1998): "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics", paper presented at The World Wide Web and Contemporary Cultural Theory

Later a plethora of websites have surfaced preaching various ideologies and messages inciting **violent** action. Stormfront is one such example exhorting white supremacy.[9]

▪ The Internet's Contribution to the Radicalization Process

There is growing concern that the Internet operates as a catalyst for radicalization and violence. Whether the main impact is one of "self-radicalization" or the dissemination of information, instructions or communication is still open to debate.

The true extent of Internet radicalization *i.e.* impact and causality remains unclear. It seems however that research conducted so far supports the theory of a correlation between exposure to online radicalization and the endorsement or commission of radicalized acts in the offline world.[10]

Conference, Drake University, November 1998. Available at: http://switch.sjsu.edu/web/v4n2/stefan/ [Accessed 27 September 2016]: "*The phrase "*Electronic Civil Disobedience*" was coined by a group of artists and theorists called the Critical Art Ensemble. In 1994 they published their first book that dealt with this subject, "*The Electronic Disturbance,*" followed two years later by "*Electronic Civil Disobedience and Other Unpopular Ideas.*" Both of these works are devoted to a theoretical exploration of how to move protests from the streets onto the Internet*." The Electronic Disturbance Theater introduced Civil disobedience also against private corporations in the campaign against Lufthansa in 2005 ("Deportation Class Action").

[9] See also: http://www.resist.com/ [Accessed 27 September 2016]; https://www.stormfront.org/forum/ [Accessed 27 September 2016]; http://www.godhatesfags.com/ [Accessed 27 September 2016]; http://www.jewwatch.com/ [Accessed 27 September 2016].

[10] In the words of the International Center for the Study of Radicalization and Political Violence (ICSR) (2009):
"It seems obvious … that the Internet can have a role in intensifying and accelerating radicalization. In fact, one may argue that the Internet is of particular benefit to marginal and/or illegal groups and movements, because it facilitates the formation of (virtual) communities which would be more 'risky', if not impossible, to establish in the real world."
A research report written by Mitchell D. Silber and Arvin Bhatt, Senior Intelligence Analysts ("The Homegrown Threat") concludes that:
"The Internet is a driver and enabler for the process of radicalization […] *the Internet provides the wandering mind of the conflicted young Muslim or potential convert with direct access to unfiltered radical and extremist ideology"*
The Internet, with its thousands of extremist websites and chat-rooms, is a virtual incubator of its own. In fact, many of the extremists began their radical conversion while researching or just surfing in the cyber world".
Other research confirms this analysis:
Social media effectively connects people with different sources of information and brings the individual into the event so he or she can watch it unfold as it happens. This increases an emotional reaction within the individual to become an involved and radical supporter. (p. 177)
Chat rooms are also useful social media tools. Al-Qaida uses PalTalk and sets up a chat room to communicate. It also is an open forum where anyone can join the conversation and become recruited and radicalized into the al-Qaida ideology. (p. 177).
Source: Thompson, R. L. (2011): "Radicalization and the Use of Social Media", *Journal of Strategic Security*, Volume 4, No. 4, Winter 2011, Article 9, p. 167. Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1146&context=jss [Accessed 27 September 2016].
See also: Von Behr, I.; Reding, A.; Edwards, C.; Gribbon L. (2013): Radicalization in the digital era The use of the internet in 15 cases of terrorism and extremism", RAND. Available at:
http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf [Accessed 30 September 2016]: *"(The) shift in terrorist behavior largely reflects society's expanding digital footprint, where everyday activities move seamlessly between online and offline domains. [...] the Internet features in most, but not all, terrorism cases" (House of Commons Home Affairs Committee, 2012)".*
See also: The psychological process and phases of Online radicalization are detailed in the study "Radicalization in the West: The Homegrown Threat" (2007) performed by Arvin Bhatt and Mitchell Silber, members of the New York City Police Department. Available at: http://eurabia.parlamentnilisty.cz/UserFiles/document/NYPD.pdf [Accessed 27 September 2016]:
"*The Internet plays an important role during the radicalization process. As individuals progress through the various stages, their use of the Internet evolves as well. In the Self-Identification phase, the Internet serves chiefly as the person's source of information about Islam and a venue to meet other seekers online. With the aggressive proliferation of the Jihadi-Salafi ideology online, it is nearly impossible for someone to avoid this extreme interpretation of Islam. During the Indoctrination phase those Undergoing this self-imposed brainwashing devote their time in the cyber world to the extremist sites and chat rooms—tapping into virtual networks of like-minded individuals around the world who reinforce the individual's beliefs and commitment and further legitimize them. At this stage, individuals or the groups they are in are likely to begin proliferating Jihadi-Salafist ideology online along with consuming it. The Internet becomes a virtual "echo chamber" –acting as a*

Political awareness of the translation of online radicalization into offline action has been expressed with increasing emphasis on the correlation.[11]

As the French Ministry of Interior declares: "*It is necessary to dismantle highly organized recruiting groups aimed at our youth, which methods of indoctrination on the Internet are extremely effective."* […] *digital networks are said to have become the first enablers of these radicalization phenomena and of the engagement in jihadism; some observers even stating that 99% of indoctrination happens on the Internet*" [the author's translation]. [12]

In the United Kingdom the Home Affairs Committee House of Commons expresses the same views:

"Guidance issued by the National Counter Terrorism Security Office states that the Internet has "transformed the way that terrorist organisations can influence and radicalise people". It says that it has enabled groups such as Daech to "reach a larger global audience, with broader and dynamic messages" which means that "vulnerable people can easily be exposed to extremist materials that are readily accessible online, and radicalised by extremist views."[13]

---

radicalization accelerant while creating the path for the ultimate stage of Jihadization. In the Jihadization phase, people challenge and encourage each other's move to action. The Internet is now a tactical resource for obtaining instructions on constructing weapons, gathering information on potential targets, and providing spiritual justification for an attack."
See also: Charvat, J. (2010): "Radicalization on the Internet", Defence Against Terrorism Review, Vol. 3, No. 2, Fall 2010, Congressional Research Service, p. 75. Available at: http://www.coedat.nato.int/publication/datr/volumes/datr6.pdf [Accessed 27 September 2016]:
"Recruitment is one area which has benefited tremendously from the advent of the Internet.
They can ask questions on forum sites as well as engage in real-time conversations in chat rooms. Terrorist groups will have links to these from their own websites in order to get potential supporters. They will often participate in chat rooms to find out who might be susceptible to the terrorist message".
A terrorist groomer would wait and look for such posts and begin engaging the vulnerable mind to the terrorist cause. Forums have the same problems as chat rooms – you only know what the other person says about themselves and not if it is true"

[11] In France the Informational Report No. 3964 conducted by Rapporteur Member of Parliament Kader Arif under the presidency of Member of Parliament Jean-Frédéric Poisson on ISIS' resources was published on 13 July 2016 reads:
"A. The leading role of the digital vector
While ISIS rejects with virulence all occidental values, the organization uses tools developed by American companies, notably social media as a means of transmission. Internet is not only a vector, that is an amplifier of an existing phenomenon, it appears to also contribute to the process of radicalization and facilitates the taking of action […].
They follow the "pulls and push factors" theory frequently mentioned Under the Mission's hearings: while pull factors rely on specific ISIS related elements that attract persons in way of radicalization or already radicalized (ideology, feeling of recognition, to belong…), push factors are everything that causes a person to flee the society in which it lives (feeling of frustration, inequality…).
[…]
"3. *ISIS' expertise in social media*
The value of social media is all the greater given that ISIS masters, in depth, how it works and know how to put it to use. ISIS knows that on the Internet it is vital to constantly propose new contents. *According to Jean-Yves Latournerie, formerly in charge of countering cyberthreats: every single day, three new videos related to ISIS are uploaded on social media such as Facebook or YouTube, their "*distribution*" being ensured on the Twitter platform*." [The author's translation]

[12] Ducol, B. (2015) : Devenir jihadiste à l'ère numérique : Une approche processuelle et situationnelle de l'engagement jihadiste au regard du Web. Québec: Université Laval, p. 2.

[13] National Counter Terrorism Security Office, (26 November 2015) "Guidance Online radicalization". Available at: https://www.gov.uk/government/publications/online-radicalization/online-radicalization [Accessed 27 September 2016].
See also: Home Office, Department for Culture, Media & Sport, Speech: "Baroness Shields calls for united action in tackling online extremism", published 23 May 2016. Available at: https://www.gov.uk/government/speeches/baroness-shields-calls-for-united-action-in-tackling-online-extremism [Accessed 27 September 2016]: "*noted that the younger generation are "more technologically literate than their parents and teachers" and are particularly susceptible to online influences because they are "almost constantly connected to the digital world* […] *extremists who influence them are from this same social media-connected peer group, and offer a "powerful, straightforward and simple" narrative: "join us and claim your place in history* […]. *The use of the Internet to promote radicalization and terrorism is one of the greatest threats that countries including the UK face.*"

The Internet allows efficient and cost free dissemination of gratuitous vindications to a receptive and often disenfranchised public.[14] Counter-factual manipulation, conspiracy theories, pseudo historic narratives and various methods of allurement flourish on the Internet and within the targeted audience there are no checks and balances, no moderators. Terrorists are generally good at propaganda.[15]

Andrew Keen in his book "*The Internet is not the Answer*" argues that:

"*The Internet has compounded hatred toward the very defenseless people it was supposed to empower.* […] *Hatred is ubiquitous on the Internet. "Big hatred meets big data", writes the Google data scientist Seth Stephens-Davidowitz about the growth of online Nazi and racist forums that attract up to four hundred thousand Americans per month.* […] *ISIS's effective use of social media highlights the core problem with the Internet. When the gatekeeper is removed and anyone can publish anything online, much of that "content" will be either propaganda or plain lies.* […]*."* [16]

---

[14] The Brookings Institution think tank has estimated that Islamic State supporters operated at least 46,000 Twitter accounts between September and December 2014 (Stempel J., Frankel A., (2016): "Twitter sued by U.S. widow for giving voice to Islamic State", *Reuters*. Available at: http://www.reuters.com/article/us-twitter-isis-lawsuit-idUSKCN0US1TA [Accessed 27 September 2016].

[15] "*The Internet promotes solidarity among members.* […] *Although interviewees stated that there are some 'Computer Nazis' who are only active online, most members however take it to the 'next level',* i.e. *joining a rally or concert, meeting with groups, planning and executing 'actions', which was said to be inseparable from being a 'true' member of the movement* […]. *A former administrator of a right-wing extremist online project among the interviewees estimates: "I think that 70% to 80% of the networking is done via the Internet*"; Source: Koehler D., (2014): "The Radical Online: Individual Radicalization Processes and the Role of the Internet", Journal for Deradicalization, Volume 2014/15 No. 1, pp. 118, 128).
See also: Von Behr, I.; Reding, A.; Edwards, C.; Gribbon L. (2013): "Radicalization in the digital era The use of the internet in 15 cases of terrorism and extremism", RAND. "*The perceived anonymity of the Internet was a key factor and created the following opportunity: "the Internet… (as a medium) allows those that would otherwise be scared of being seen with the wrong people to get engaged, and one which makes the whole process more invisible to the authorities*."
Raffaello Pantucci has argued, "*The increasing prevalence of the Internet and the easy availability of extremist material online have fostered the growth of the autodidactic extremist*." (Pantucci, R., (2011): "A typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists", *Developments in Radicalization and Political Violence*. Available at:http://www.trackingterrorism.org/sites/default/files/chatter/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf [Accessed 27 September 2016].
See also: Institute for strategic Dialogue (2011): "Radicalization: The role of the Internet, A working Paper on the PPN". Available at: https://www.counterextremism.org/resources/details/id/11/ppn-working-paper-radicalization-the-role-of-the-internet [Accessed 30 September 2016]: "*By emulating established media news outlets, they are beginning to narrow the credibility gap between themselves and the established news media, so that more people will tune into their radical Islamist version of world affairs. One of the new trends is the use of social media by extremists and terrorist networks. These platforms have lower technical and financial barriers to entry, and have the added bonus of reaching much wider constituencies than is likely via a dedicated website. Facebook offers a new type of mass interpersonal persuasion and YouTube motivates individuals to contribute by uploading videos or commenting on others'. These forums also have the added bonus of making users harder to identify; their real IP addresses are not compromised, as they are not required to fill in verifiable personal details. One jihadist site contains a detailed invitation to use popular American web forums to distribute jihadist films and disinformation about the war. The invitation is accompanied by tips on how to present yourself, which parts of the forum to use, what type of discussions to look for or initiate and what topics to avoid. As part of this strategy, jihadists are urged to:*
• 'Invade' social network sites such as Facebook by setting up groups with radical views and to seek to gather users with the 'right' attitude;
• 'Invade' file-sharing sites like YouTube by placing various clips with extreme content;
• Infiltrate popular Islamist websites in order to attempt to convert them into militant sites in line with the closed websites by spreading extremist contents on the discussion forums of these sites.
Finally, there are many possibilities for fundraising by and for jihadists on the Internet, whether through direct and open fundraising initiatives on websites or through e-commerce and online fraud. But as yet, there is little evidence of fundraising happening online in practice."
See also: Von Behr, I.; Reding, A.; Edwards, C.; Gribbon L. (2013): "Radicalization in the digital era The use of the internet in 15 cases of terrorism and extremism", RAND: A recent empirical study of 242 European jihadists from 2001-2006, on the effects on the Internet on radicalization, found that there is a correlation between jihadi web sites and propaganda on the Internet and rapid radicalization. A feature which supports the notion of the Internet as an accelerant in radicalization is the fact that it offers a 'one-stop shop' The role of chat rooms in particular increases this acceleration effect, as extremists can exchange with like-minded individuals 24/7, regardless of borders.

[16] Keen A., (2015): *The Internet is not the answer*, Atlantic Monthly Press, pp. 149, 151, 153 and 155.

The United Nations has expressed strong concerns on the risks of Internet incitement leading to violent extremism:

"*Strategic communications, the Internet and social media*
The manipulative messages of violent extremists on social media have achieved considerable success in luring people, especially young women and men, into their ranks. While violent extremists have demonstrated some sophistication in their use of old and new media tools, it is equally true that we who reject their message have largely failed to communicate to those who are disillusioned and disenfranchised a vision of the future that captures their imagination and offers the prospect of tangible change."[17]

Irrespective of the need to conduct further research into the radicalization process, causation and impact it may be concluded that there is both scientific and political consensus as to the existence of a correlation and the danger it harbours.

[17] Report of the Secretary-General (2015), The United Nations Global Counter-Terrorism Strategy: "Plan of Action to Prevent Violent Extremism" (A/70/674). Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674 [Accessed 27 September 2016].

Section 1: The International Community's Policy on Internet Radicalization

Faced with the threat of radicalization, leading to the spread of terrorism throughout the world, the international community has taken a number of initiatives and passed consequential resolutions involving restrictions and content monitoring on the Internet.

The United Nations, in its "Plan of Action to Prevent Violent Extremism" (24 December 2015) expresses that:

"Violent extremism is a diverse phenomenon, without clear definition. […] *These groups' message of intolerance — religious, cultural, social — has had drastic consequences for many regions of the world. Holding territory and using* ***social media*** *for the global and real-time communication of their ideas and exploits, they seek to challenge our shared values of peace, justice and human dignity* […] *in recent years,* ***online tools*** *have served as an additional, and more accessible, pathway to group membership."* [the author's emphasis] [18]

At the European Union level policy statements on the Internet's role in radicalization and terrorism have been formulated on several occasions.

An example is the Communication from the Commission "Preventing Radicalization to Terrorism and Violent Extremism: Strengthening the EU's Response" (15 January 2014):

---

[18] Report of the Secretary-General (2015), The United Nations Global Counter-Terrorism Strategy: "Plan of Action to Prevent Violent Extremism" (A/70/674). Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674 [Accessed 27 September 2016].
See also General Assembly (2006), The United Nations Global Counter-Terrorism Strategy: Resolution 60/288. Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terr%20ARES60288.pdf [Accessed 27 September 2016].
The U.N. Security Council Resolution 1456 (2003) on combating terrorism. Available at: http://dag.un.org/bitstream/handle/11176/25388/S_RES_1456%282003%29-EN.pdf?sequence=3&isAllowed=y [Accessed 27 September 2016], reaffirms that: *"terrorism in all its forms and manifestations constitutes one of the most serious threats to peace and security;*
[…] *– it has become easier, in an increasingly globalized world, for terrorists to* ***exploit sophisticated technology, communications and resources*** *for their criminal objectives* […]*."* [the author's emphasis]; Source: Further, in its Resolution 2250 (2015) the Security 1252nd meeting of the Ministers' Deputies Council expresses:
"[…] *concern over the increased use, in a globalized society, by terrorists and their supporters of* ***new information and communication technologies, in particular the Internet,*** *for the purposes of recruitment and incitement of youth to commit terrorist acts, as well as for the financing, planning and preparation of their activities, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts* […]*."* [author's emphasis]. Source: U.N. Security Council (2015), Resolution 2250 (2015). Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2250.pdf [Accessed 27 September 2016].
The General Assembly already adopted the United Nations Global Counterterrorism Strategy on 8 September 2006.
It includes a full section on: **"Internet Policies"**
Recent years have shown ***an increasing use of the Internet*** *by violent extremists as a means of spreading propaganda, raising funds, recruiting new members, and communicating with their activists. Violent extremists have also used* ***the Internet*** *as a virtual training camp by establishing various forms* ***of online****, private, person to person or group communication to exchange experience and knowledge. Violent extremists have successfully* ***turned the great virtues of the Internet*** *– low cost, ease of access, lack of regulation in many parts of the world, vast potential audience, and fast communication and flow of information – into a means to achieve their goals and attract recruits. The question of how to limit terrorist* ***abuse of the Internet*** *has been contentiously discussed in different parts of the world for some time* […]."

*"With the growing concern about **online radicalization** and the noticeable increase in openly extremist groups in Europe, more and more Member States are facing threats from radicalization. Throughout the EU, the risk of radicalization leading to extremist violence is growing, and Member States would benefit from increasing their efforts to effectively respond to these challenges. Radicalization crosses national boundaries in many ways. For example, **the use of chat rooms, social media, and other online tools** often has an international dimension. The type of threats Member States face are often similar, so it can be effective to take action at the EU level.* [the author's emphasis] [19]

---

[19] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions: Preventing Radicalization to Terrorism and Violent Extremism. Strengthening the EU's Response (15 January 2014). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0941&from=EN [Accessed 27 September 2016].

See also: EU Counter-Terrorism Coordinator (2016), Note 6785/16 to Council of the European Union on the State of play on implementation of the statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015. Available at: http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/en/pdf [Accessed 27 September 2016].

"The EU Counter-Terrorism Coordinator (March 4th 2016) summarized the current situation as follows:

– EU Internet Referral Unit (IRU**)**

The EU has maintained its focus on combatting radicalization online. The EU IRU at Europol, which is now part of the ECTC has identified 3,351 items of potentially violent/extremist content, triggering 2,037 referrals and 1,793 removals. The referral success rate is 88%. Pro-active engagement with Internet service providers continues. Since its establishment on 1 July 2015, 144 contributions from 26 Member States have been received.

– EU Internet Forum

On 3 December 2015, the Commission hosted the first Ministerial-level meeting of the EU Internet Forum between JHA Ministers [Justice and Home Affairs] senior representatives from the world's leading social media companies. Participants agreed that DAECH and other extremist groups were exploiting the Internet to spread propaganda, seek new recruits, and to encourage acts of violence. They also agreed on the importance of having effective mechanisms in place between Government and industry to remove terrorist content promptly […]*."*

The EU has focused on Internet induced radicalization in a number of resolutions and initiatives.

In its Communication on *"Preventing Radicalization to Terrorism and Violent Extremism" (January 15th 2014)* the Commission states: *"terrorist groups and extremists are capitalizing on advances in technology to find new ways of engaging with disaffected youth, taking advantage of social networking sites, online video channels and radical chat rooms. They are spreading their propaganda more widely, more rapidly, and more effectively."*

In The European Commission's "STAFF WORKING DOCUMENT amending Framework Decision 2002/475/JHA on combating terrorism)" the impact of the Internet on radicalization is described in the following terms:

Modern information and communication technologies play an important role in the development of the threat which is currently represented by terrorism: they may serve as a means of dissemination of propaganda aiming at mobilization and recruitment as well as instructions and online manuals intended for training or planning of attacks, addressed at current and potential supporters. The Internet, in particular, may serve as one of the principal boosters of the processes of radicalization and recruitment: it is used to inspire and mobilize local networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. The dissemination of terrorist propaganda and terrorist expertise through the Internet has therefore empowered terrorists, making the terrorist threat grow. […]*."* Source: Commission staff working document (2007), Accompanying document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on combating terrorism Summary of the impact assessment {COM (2007) 650 final} {SEC (2007) 1424}. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007SC1425&from=EN [Accessed 27 September 2016].

See also: The Council of Europe in its Council framework decision 2008/919/JHA of November 2008 describes the correlation between the Internet and radicalization in the following terms:

(4) The Internet is used to inspire and mobilize local terrorist networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. Activities of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism have multiplied at very low cost and risk.

Source: Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0919&from=EN [Accessed 27 September 2016].

The European Parliament subscribes to this analysis in its "Communication from the Commission to the European Parliament and the Council concerning Terrorist recruitment: addressing the factors contributing to violent radicalization" of September 29th 2005**:**

"…some media – notably radio, satellite television and the Internet - disseminate propaganda which contributes to violent radicalization. Typically, this conveys a reductionist and conspiratorial worldview where inequity and oppression are dominant and entire countries, religions or societies are depicted in a way which denies them human dignity and presents them as collectively guilty."

UNESCO (October 2015) endorses these views and expresses "*concern about the rise in violent extremism and the worldwide challenge of recruitment and radicalization to violent extremism of youth on social media, in communities, and in schools."*[20]

Clearly the international community has demonstrated not only awareness of the correlation, but has also taken substantial steps involving law enforcement, education and policy initiatives to contain the dangers created by online radicalization.

The present Report deals with those measures that are and may be directed against **radicalizing content** and its dissemination. It does not deal with radicalization as such.

Section 2: Definition of Radicalizing Content

2.a. Definition as a Legal Requirement

It is a basic principle embodied in several legal instruments over decades that nobody may be prosecuted or convicted of a crime unless it has not been publicly recorded and adequately expounded (*nulla poenem sine lege* or the "Principle of Legality"). This principle is enshrined in a number of international human rights instruments *e.g.* The European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 7), The Universal Declaration of Human Rights (Art. 11), The International Covenant on Civil and Political Rights (Art. 15), The Arab Charter on Human Rights (League of Arab States) (Art. 15), The African Charter on Human and People's Rights (Art. 7), The Cairo Declaration on Human Rights in Islam (Art. 19), The ASEAN Human Rights Declaration (Art. 20) and The American Declaration of the Rights and Duties of Man (Art. 26). The principle includes a prohibition against retroactive effects of Penal Law.

For the purposes of this Report it is therefore critical to arrive at a legally adequate definition of "radicalizing content" which given the universality of the Internet must be susceptible to international consensus.

Secondly, the media can play a role in facilitating recruitment into terrorist groups, by giving expression to terrorist views and organizations and facilitating the contact between radicalized individuals, e.g. via the Internet."
The Council of Europe in its **"**Conclusions on cooperation to combat terrorist use of the Internet**"** institutes the "Check the Web" mechanism (Brussels, 29 May 2007, 8457/3/07, REV 3, ENFOPOL 66) and concludes that:
"1. The Internet use plays a significant role in the logistic, operational and communication network of terrorist organizations. Terrorists use the Internet not only as a means to communicate and spread propaganda, but also to radicalize, recruit and train terrorists, to spread instructions on how to carry out concrete offences and to transfer information, as well as for terrorist financing purposes.
2. The EU has made it one of its primary goals to tackle the Internet as a basis for radicalization and recruitment to terrorism. The prevention of radicalization processes and the recruitment of potential terrorists is one of the main pillars of the fight against terrorism. Accordingly, the strategy and action plan for combating radicalization and recruitment to terrorism (Doc. 14781/1/05 and Doc. 14782/05) contain measures to combat the terrorist use of the Internet in this regard".
Source: Article 36 Committee (2007), Note 8457/3/07 to COREPER / Council on Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web"). Available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%203 [Accessed 27 September 2016].

[20] Executive Board, UNESCO (2015), UNESCO's Role in Promoting Education as a Tool to Prevent Violent Extremism, 197 EX/46. Available at: http://unesdoc.unesco.org/images/0023/002348/234879e.pdf [Accessed 27 September 2016].

2.b. Examples of Definitions

As a preliminary comment, it should be noted that no explicit and consensual definition of "radicalizing content" (or "radicalization") can be found in existing international legal instruments despite the significant number of such instruments dealing with terrorism and other related concepts and despite various resolutions and extensive literature on the subject.

Notwithstanding this lack of definition, the term is employed not only in treaties, but also in domestic laws for instance in Labor Law and Penal Law.

There seems to be consensus that from a legal and to a certain extent psychological perspective radicalization is a more abstract and broad phenomenon than its related concepts of "terrorism" and "violent extremism".

Radicalization describes a **process** that most likely leads to acts often qualified as terrorism or extremism but not necessarily (the violent acts that may result from radicalization may in some instances arguably be qualified as "insurgency", "rebellion", "civil war" or even "war").

Most definitions applied in research on the subject or in guidance to law enforcement agencies relate to the process or the act/the commission of radicalization.

Contrary to "radicalization", "terrorism" is directly or indirectly defined in several resolutions and treaties.

The Council of the European Union defines *"*terrorism" as *"intentional acts that were committed with the aim of seriously intimidating a population, or unduly compelling a government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization"* (European Commission 2006).[21]

The National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database defines "The Terrorist Act" as*:* […] *"an intentional act of violence committed or threatened by a nonstate actor; it is committed with the purpose of attaining a political, economic, religious, or social goal; it is designed to coerce, intimidate, or convey a message to an audience beyond its immediate victims; it is committed outside the context of legitimate warfare and violates the conventions outlined in international humanitarian law; it is unambiguous in meeting this criteria but not necessary carried out successfully."*[22]

[21] Rahimullah, R.; Larmar, S.; Abdalla, M. (2013): "Understanding Violent Radicalization amongst Muslims: A Review of the Literature", *Journal of Psychology and Behavioral Science*, Volume 1 No. 1, p. 19. Available at: http://www98.griffith.edu.au/dspace/bitstream/handle/10072/59871/93055_1.pdf?sequence=1 [Accessed 27 September 2016].

[22] Stern, J. and Berger, J.M. (2015) *Isis: The state of terror*. New York, NY, United States: Ecco Press, p. 302.

The United Nations has no internationally-agreed definition of terrorism, violent extremism or radicalization.[23] One of the reasons seems to be the difficulty in accommodating the concerns voiced by the Organization of the Islamic Conference which explicitly exclude armed struggle for liberation from occupation and the struggle for self-determination (as per the Arab Terrorism Convention of 22 April 1998 and the Terrorism Convention of the Organization of the Islamic Conference of July 1999).

The United Nations Security Council has however, in its resolution 1566 (2004), developed three cumulative criteria to characterize "terrorism" *(i) intent; (ii) purpose; and (iii) specific conduct, consisting of the following: i. Criminal acts, including against civilians, committed with the intent of causing death or serious bodily injury, or the taking of hostages; ii. Regardless of whether motivated by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, with the purpose of provoking a state of terror in the general public or in a group of individuals or particular individuals, intimidating a population or compelling a government or an international organization to carry out or to abstain from carrying out any act; and iii. Which constitute offences within the scope of, and as defined in, the international conventions and protocols relating to terrorism."*[24]

In the EU we find these criteria incorporated into the proposal for a Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism (13 June 2002):

> *"Article 3* […] *offences*
> […] *which, given their nature or context, may seriously damage a country or an international organisation are defined as terrorist offences where committed with the aim of one or more of the following:*
> *(a) seriously intimidating a population;*
> *(b) Unduly compelling a Government or international organisation to perform or abstain from performing any act,*
> *(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation."*[25]

---

[23] OSCE (2014), Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach. Available at: http://www.osce.org/atu/111438?download=true [Accessed 27 September 2016]: "*Violent extremism is a diverse phenomenon, without clear definition."*

[24] Resolution analyzed by the OSCE (2014), "Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach". Available at: http://www.osce.org/atu/111438?download=true [Accessed 27 September 2016].

[25] *2. Intentional acts referred to in paragraph 1 are*
(a) Attacks upon a persons' life which may cause death;
(b) attacks upon the physical integrity of a person;
(c) kidnapping or hostage taking;
(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
(e) seizure of aircraft, ships or other means of public or goods transport;
(f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
(g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
(i) threatening to commit any of the acts listed in points (a) to (h).

Attempts at defining "radicalization" have been made by the European Commission in its "Communication to the European Parliament and the Council concerning Terrorist recruitment: addressing the factors contributing to violent radicalization" (September 29th 2005):

*"*Violent radicalization*" is the phenomenon of people embracing opinions, views and ideas which could* lead *to acts of terrorism as defined in Article 1 of the Framework Decision on Combating Terrorism.*[26]

In the United States, the Executive Order 13224 on Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism we find the following definition:
(d) the term "terrorism" means an activity that […]
(i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended […]
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

In various national laws "terrorism" is either defined or described indirectly while radicalization is rarely defined yet frequently met with penal sanctions by reference to analogy from other crimes[27]:

- Iraq's Counter Terrorism Law N°13 of 2005 defines terrorism as:
  "*Violence or threats, which aims to spread horror among the people or their lives and their liberty and their security at risk and endanger their property and possessions or motivates others for purposes of the implementation of a terrorist project individually or collectively."* (Art. 2.1) and in Art. 2.4): [the] *"Use violence or threat to stir up sectarian strife or civil war or sectarian infighting by arming citizens or by encouraging them to arm themselves and by incitement or funding."*

- The United Kingdom Terrorism Act 2000 defines "terrorism" as an *"action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system* […]*"*. The Act does not define "radicalization", but "extremism" is defined as "*vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs"* (Prevent Strategy, 2011, p.107).

The Terrorism Act of 2006 of the United Kingdom, Section 2 makes it a criminal offence to encourage terrorism (as defined in the Terrorism Act of 2000) by directly or indirectly inciting or encouraging others to commit acts of terrorism. This includes an offence of "glorification" of terror - people who "praise or celebrate" terrorism in a way that may encourage others to commit a terrorist act.

---

[26] Directorate-General for Internal Policies, European Parliament (2014), "Preventing and Countering Youth Radicalization in the EU", Study for the LIBE Committee. Available at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/IPOL-LIBE_ET(2014)509977_EN.pdf [Accessed 27 September 2016].
The European Parliament describes "radicalization" rather than defining it in its policy on online radicalization:
"Radicalization should not be analyzed as a form of pre-terrorism which could be disrupted before the shift to violence by an intensive surveillance of a community. It should not be analyzed as a linear process but as a relational dynamic".

[27] The following review is based on the official responses given by the countries to the Questionnaire and information retrieved by the author's own research team. For a full text of the Questionnaire and the answers, please refer to Annex 1.

Government's definition of "radicalization" as applied in the Prevent Strategy reads: *"radicalization is the process by which a person comes to support terrorism and forms of extremism leading to terrorism."*[28]

- Art. 6 of the Tunisian Constitution provides that the State *"agrees to prohibit and prevent apostasy accusations and incitement to hatred and violence and to halt them."*

- Art. 265 (c) of the Criminal Code of Albania punishes the act of "*inciting hatred or disputes between nationalities, races and religions*". The latter provides for up to 3 years' imprisonment for calls to participate in violent military actions in a foreign country (Law 98/2014).

- Art. 231 on *"Recruitment of persons for the purpose of committing terrorist acts",* Art. 232 (a) on the *"Promotion, public call and propaganda for committing offenses with terrorist purposes",* and Art. 265 (c) on *"Inciting hatred or disputes between nationalities, races and religions"* also apply by analogy.

- The Australian Criminal Code Act 1995 includes offences for conduct such as urging violence or advocating terrorism.

  Division 80.1 of the Commonwealth Criminal Code defines the following offences of urging violence and advocating terrorism:

  - Section 80.2A:
    Urging violence against groups—a person commits an offence if the person urges another person, or a group, to use force or violence against a group distinguished by race, religion, nationality, national or ethnic origin or political opinion intending that force or violence will occur.

  - Section 80.2B:
    Urging violence against members of groups—a person commits an offence if the person urges another person, or a group, to use force or violence against a person because they a member of a group distinguished by race, religion, nationality, national or ethnic origin or political opinion intending that force or violence will occur.

  - Section 80.2C:
    Advocating terrorism—a person commits an offence if the person advocates the doing of a terrorist act or the commission of a terrorism offence and is reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. The meaning of "advocates" includes to "counsel, promote, encourage or urge" the doing of a terrorist act or commission of a terrorism offence.

[28] Secretary of State for the Home Department (2011), *Prevent* Strategy, Presented to Parliament by Command of Her Majesty. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf [Accessed 27 September 2016].

- Under Section 130 of the German Criminal Code, criminal liability occurs where the offender, *in a manner capable of disturbing the public peace 1. incites hatred against a national, racial, religious group or a group defined by their ethnic origins, against segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population or calls for violent or arbitrary measures against them; or 2. assaults the human dignity of others by insulting, maliciously maligning an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population, or defaming segments of the population.*

  This includes publishing radicalization content on the internet ("Volksverhetzung"). If the person publishing the content uses propaganda material of unconstitutional organizations this may, in addition, constitute an offence under Section 86 or Section 86a (Using symbols of unconstitutional organizations) of the Criminal Code.
  Other provisions of the Criminal Code relevant for the prosecution of hate speech are: Section 185 and Section 111 (Public incitement to crime) under which anyone who publicly, in a meeting or through the dissemination of written materials (including audio-visual media) incites the commission of an unlawful act, shall be held liable as an abettor to that act;

  Section 130a (Attempting to cause the commission of offences by means of publication) under which anyone who disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (including audio-visual media) capable of serving as an instruction for certain severe unlawful acts and intended by its content to encourage or cause others to commit one of those acts, shall be liable. The same applies to anyone who disseminates or makes publicly available such material in order to encourage or cause others to commit such an act;

  Section 140 (Rewarding and approving of offences) under which anyone who 1. rewards or 2. publicly, in a meeting or through dissemination of written materials (including audio-visual media), and in a manner that is capable of disturbing the public peace, approves of one of certain severe unlawful acts after it has been committed or attempted, shall be liable;

  Section 241 para 1 (Threatening the commission of a felony) under which anyone who threatens a person with the commission of a felony against him or a person close to him shall be liable.

- *"Incitement to violence and disobedience of the law"* is prohibited under Section 89A of the Penal Code of the Seychelles:

  The act of radicalization is not as such a penal offence. […] Hate speech" and "incitement to hatred" are offences under S.55(1)(b) of the Penal Code of Seychelles. "Apology for genocide" is not an offence. "Solicitation of murder" is an offence under S.377A and S.381 of the Penal Code. "Defamation" is a criminal offence under Chapter 18 of the Penal Code. Additionally, a broad offence of "Incitement to violence and disobedience of the law" is provided for under Section 89A of the Penal Code. These are existing provisions in law independent of whether internet radicalization is an offence or not.

- The Penal Code of Israel includes a definition of "Incitement to violence and terror" (Sections 144D2-144D3). Section 144D2 provides a definition of the offence of prohibited publication: "*If a person publishes calls to commit an act of violence or terror, or praise, words of approval, encouragement, support or identification with an act of violence or terror,* then he is liable to five years'" imprisonment. This section also provides that a true and fair report of such a publication does not constitute an offence.

  - Enticement (Solicitation) (Section 30) of the Israeli Penal Code:
    If a person causes another to commit an offense by means of persuasion, encouragement, demand, and cajolery or by means of anything else that constitutes the application of pressure, he entices to an offense.

    The act of radicalization is not as such a penal offence, but Israeli criminal legislation contains several offences analogical to acts of radicalization.

  - Incitement to racism (Sections 144A-144D1):
    Section 144A – definition of racism: persecution, humiliation, degradation, a display of enmity, hostility or violence, or causing violence against a public or parts of the population, all because of their color, racial affiliation or national ethnic origin.
    Section 144B – definition of the offence of prohibited publication: If a person publishes anything in order to incite to racism, then he is liable to five years' imprisonment.

  - Hate offences (Section 144F):

  - Injury to religious sentiment (Section 173):
    The offence criminalizes publications that are liable to crudely offend the religious faith or sentiment of others.

  Defamation as well as incitement to genocide are also offences that can be applied analogically to acts of radicalization.

- Radicalization is considered to be included in the offences of extremism in Slovakia.

  Penal offences of extremism are specified in section 140(a) of the Criminal Code for instance: *"Penal offences of extremism are the Crime of Supporting and Promoting Groups Aimed at Suppression of Fundamental Rights and Freedoms."*

  The act of radicalization is not defined.

  Radicalization can however be *"subsumed under elements (subject of matter) of the offences of extremism."*

Penal offences of extremism are specified in Section 140(a) of the Criminal Code:

"Penal offences of extremism are the Crime of Supporting and Promoting Groups Aimed at Suppression of Fundamental Rights and Freedoms under § 421 and 422, Crime of Manufacturing of Extremist Materials to § 422a, Crime of Dissemination of Extremist Materials according to § 422 (b), Crime of Possession of Extremist Materials according to § 422c, Crime of Denial and Approval of the Holocaust and Crimes Committed in Political Regimes under § 422d, Crime of Defamation of Nation, Race and Belief under § 423, Crime of Incitement of National, Racial and Ethnic Hatred under § 424, Crime of Incitement, Defamation and Threatening to Persons because of their Affiliation to Race, Nation, Nationality, Complexion, Ethnic Group or Family Origin to § 424a and the offenses committed on specific motifs under § 140 point. d) and f)."

- In Spain the act of radicalization as such is not an offence, but the Criminal Code (Art. 575.2º) provides that "self-study to commit terrorist offenses" is criminalized as an expression of radicalization.: "*Any person who, with the same objective of enabling himself to carry out any of the offences defined in this Chapter (Terrorist Offences), carries out by himself any of the activities set out in the previous provision (instruction in military or combat matters, in technology for the development of chemical or biological weapons, in the manufacture or preparation of explosive, inflammable, incendiary or asphyxiating substances or apparatus)":*

  The Spanish Criminal Code also provides for offences such as incitement to hatred, hostility, discrimination or violence against individuals or groups because of their group membership, anti-Semitic or other reasons related to ideology, religion or belief, family status, belonging to an ethnic group, race or nation, national origin, gender, sexual orientation or gender-identity, illness or disability (Article 510.1º CC).
  Offence of dissemination of material that incites to the behavior described above (art.510.1b) CC).
  Offence of denial, trivialization or public glorification of genocide.
  There is an aggravated behavior when previous crimes are committed through a social media, internet or information technologies (Article 510.3 CC).
  Offence of incitement to commit any of the above offences or murder for discriminatory reasons aforementioned described (Article 17, 18, 22.4 and 138 CC).

- The Swedish Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crimes imposes specific criminal liability on those *who in a message to the public, urge or otherwise attempt to entice people to commit particularly serious crime (public provocation) or seek to induce another person, in a case other than that specified above, to commit or otherwise participate in particularly serious crime (recruitment).* 'Particularly serious crime' means inter alia terrorist offences, offences referred to in certain specified international agreements and other serious crimes if the intent is to intimidate a population or a group of population or to compel a government or an international organization to perform an act or abstain from acting.

  The Swedish Penal Code contains a provision on inciting rebellion. According to this provision a person who: *"orally, before a crowd or congregation of people, or in a publication distributed or issued for distribution, or in other message to the public, urges or otherwise attempts to entice people to commit a criminal act shall be sentenced for inciting rebellion"*.

- In Denmark, radicalization is not defined directly, but sections 114 c, 114 d and 114 e of the Danish Criminal Code are applicable for recruitment, training and dissemination of terror propaganda.

  - Section 114 c:

  (1) Imprisonment for a term not exceeding ten years is imposed on any person who recruits another person to commit or facilitate any act falling within section 114 or 114a or to join a group
  or an association for the purpose of facilitating the commission of illegal acts of this nature by the group or association. […]

  (2) Imprisonment for a term not exceeding six years is imposed on any person who recruits another person to commit or facilitate any act falling within section 114b or to join a group or an association for the purpose of facilitating the commission of illegal acts of this nature by the group or association.

  (3) Imprisonment for a term not exceeding six years is imposed on any person who accepts being recruited to commit any act falling within section 114 or 114a. […]

  - Section 114 d:

  (1) Imprisonment for a term not exceeding ten years is imposed on any person who trains, gives instruction to or otherwise teaches another person to commit or facilitate any act falling within section 114 or 114a knowing that such other person intends to use his skills for such purpose. […]

- In Tunisia, Art. 13 of the Law 26/2015 on countering terrorism and the repression of money laundering, essentially paragraph 8 apply to radicalization. In addition, Art. 6 of the Tunisian Constitution provides that the State *"commits to prohibiting and preventing accusation of apostasy and incitement to hatred and violence and to contain them".*

- In Hungary, the act of radicalization is not as such a penal offence and the principle of legality is strictly applied to criminalization by analogy:

  Radicalization may coincide with the elements of a criminal offence provided by the Criminal Code [e.g. incitement to hatred] (Section 312), violence against a member of a community (Section 216), homicide (Section 160), public denial of the crimes of national socialist or communist regimes (Section 333), libel (Section 226), defamation (Section 227), terrorist act (Section 314).

- In France, the act of radicalization is not as such a penal offence. However, other offences can be used to counter online radicalization.

  - Art. 24 of the Press Law of 1881 criminalizes incitement to racial discrimination, hatred, or violence on the basis of one's origin or membership (or non-membership) in an ethic, national, racial, or religious group.

  - Art. of Law N° 2004-575 of 21 June 2004 on confidence in the digital economy provides for the blocking of websites inciting racial hate and for one-year imprisonment and a 15 000 euro fine for the publisher.

- Art. R 625-7 of the Criminal Code makes it an offense to incite to racial hate via private communication.

- In Tanzania, the act of radicalization is not as such a penal offence, but other offences may be applied to counter radicalization.

  - Art. 6 (1) of the Prevention of Terrorism Act of 2002:
    Where two or more persons associate for the purpose of, or where an organization engages in any act for the purpose of;
    […]
    promoting, encouraging or exhorting others to commit an act of terrorism; or […]

  - Art. 7 (1) of the Prevention of Terrorism Act 2002:
    A person commits an offence who, in any manner or form;
    (a) solicits support for, or tenders support in relation to, an act of terrorism, or
    (b) solicits support for, or tenders support to, a proscribed organization.
    (2) "Support" as used in subsection (1), means and includes;
    (a) instigation to the cause of terrorism;
    (c) offering of or provision of moral assistance, including invitation to adhere to a Proscribed organization; […]

  Moreover, there are relevant provisions in Part II of the Cybercrime Act of 2015:

  - Art. 16 - Publication of false information
    Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or counseling commission of an offence, commits an offence […].

  - Art. 17 - Racist and xenophobic material
    (1) A person shall not, through a computer system -
    (a) Produce racist or xenophobic material for the purposes of distribution;
    (b) Offer or make available racist or xenophobic material; or
    (c) Distribute or transmit racist or xenophobic material.

  - Art. 18 - Racist and xenophobic motivated insult
    (1) A person shall not insult another person through a computer system on the basis of race, color, descent, nationality, ethnic origin or religion.

  - Art. 19 - Genocide and crimes against humanity
    (1) A person shall not unlawfully publish or cause to be published, through a computer system, a material which incites, denies, minimizes or justifies acts constituting genocide or crimes against humanity.

- In the Federation of Russia, the act of radicalization is not as such a penal offence. However, other offences can be used to counter radicalization.

  - Art. 205 of the Criminal Code reads:
  1. Terrorism, that is, the perpetration of an explosion, arson, or any other action endangering the lives of people, causing sizable property damage, or entailing other socially dangerous consequences, if these actions have been committed for the purpose of violating public security, frightening the population, or exerting influence on decision-making by governmental bodies, and also the threat of committing said actions for the same ends, shall be punishable by deprivation of liberty for a term of five to ten years.

  - Art. 205.1. Involvement of a Person in the Commission of Crimes of Terrorist Nature or Otherwise Assisting in their Commission:
  1. Involvement of a person in the commission of the crime stipulated by Articles 205, 206, 208, 211, 277 and 360 of this Code or persuading a person to participate in a terrorist organization, the arming or training of a person with the aim of perpetrating the said crimes as well as the financing of an act of terrorism or a terrorist organization shall be punishable by deprivation of freedom for a term of four to eight years.
  2. The same deeds perpetrated by the person repeatedly or through the use of his official position shall be punishable by deprivation of freedom for a term of seven to fifteen years with confiscation of property, or without such confiscation.

  Hate speech offences can also be used.

  Art. 1 of the Federal Law N° 114-FZ contains a definition of extremist materials. It includes: (1) calling for extremist; (2) supporting the necessity of extremist activity; (3) justifying the necessity of extremist activity; and (4) extremist information by virtue of the law.

- In Belgium, Art. 3(15) of the Law on Intelligence and Security of 1999 (amended, originally in the Ministry Circular GPI 78 of 31 January 2014 of the Ministry of Interior relating to the processing of information in favor of an integrated approach of terrorism and violent radicalization by the police) provides for a definition of radicalization. It defines it as: *"a process influencing an individual or group of individuals in such way that the said individual or group of individuals is mentally prepared or disposed to engage in terrorist acts."*

  Terrorist-related offences can be used to counter radicalization.

  - Art. 140 bis of the Criminal Code prohibits public provocation to commit a terrorist offence
  - Art. 140 quarter punishes the fact of giving instructions on how to create weapons to be used for terrorism.
  - Art. 140 quinquies punished the fact of giving instructions or taking a course on how to commit a terrorist act.
  - The Law of 30 July 1981 prohibits racist or xenophobic acts and incitement to hatred or violence against a person, group, community, on the basis of their race, skin color, national

or ethnic identity, etc. These acts can be punished of 1 month to a 1-year imprisonment and/or from EUR50 to EUR1000 fine.

- In India, currently, the act of radicalization is not as such a penal offence.

  Cases pertaining to the same are sought to be addressed by invoking the incitement of hatred provisions, under existing law.

- In Nigeria, the act of radicalization is a penal offence as such. Furthermore, the Terrorism Act (Amendment) of 2013 can be used to counter radicalization.[29]

  - Section 1:

  (2) A person or a body in or outside Nigeria directly or indirectly willingly
  (a) does, attempts or threatens any act of terrorism,
  (b) commits an act preparatory to or in furtherance of an act of terrorism,
  (c) omits to do anything that is reasonably necessary to prevent an act of terrorism,
  (d) assists or facilitates the activities of persons engaged in an act of terrorism or is an accessory to any offence under this Act,
  (e) participates as an accomplice in or contributes to the commission of any act of terrorism or offences under this Act,
  (f) assists, facilitates, organizes or directs the activities of persons or organizations engaged in any act of terrorism,
  (g) is an accessory to any act of terrorism, or
  (h) incites, promises or induces any other person by any means whatsoever to commit any act of terrorism or any of the offences referred to in this Act,
  commits an offence under this Act and is liable on conviction to maximum of death sentence.

  - Section 5:

  (1) Any person who knowingly, in any manner, directly or indirectly, solicits or renders support -
  (a) for the commission of an act of terrorism, or
  (b) to a terrorist group,
  commits an offence under this Act and is liable on conviction to imprisonment for a term of not less than twenty years.
  (2) For the purposes of subsection (1) of this section, "support" includes -
  (a) incitement to commit a terrorist act through the internet, or any electronic means or through the use of printed materials or through the dissemination of terrorist information […]

- In the United Arab Emirates, the act of radicalization is not as such a penal offence. However, the following offences can be used by analogy:

[29] See also the Nigerian laws *"Administration of Criminal Justice Act"* (2015) and *"Cybercrime (Prohibition and Prevention) Act"* (2015).

- Art. 34 of Federal Law N°7 of 2014 On Combating Terrorism Offences:
  1. Temporary imprisonment for no more than 10 years shall be imposed on whoever knowingly promotes or supports a terrorist organisation, person or offence, whether verbally, in writing or by any other method.
  2. Temporary imprisonment for no more than 10 years shall be imposed on whoever: Knowingly possesses, in person or through someone else, any documents, print or recordings of any kind, that encompass promotion or supporting of any terrorist organization, person or offence if intended for distribution or access by others.
  Knowingly possesses or acquires any printing, recording or publishing mean used or intended to be used, even if temporarily, for the printing, recording, circulating or publishing any of the aforementioned.

- Art. 26 of the Federal Decree-law N°5 of 2012 on Combating Cybercrimes:
  Shall be punished by imprisonment for a period of at least five years and a fine not less than one million dirhams and not in excess of two million dirhams whoever establishes, manages or runs a website or publishes information on the computer network or information technology means for the interest of a terrorist group or any unauthorized group, association, organization, or body with the intent to facilitate communication with their leaders or members or attract new members, or to promote or praise their ideas, finance their activities or provide actual assistance thereof or for the purpose of publishing methods for manufacturing incendiary devices or explosives or any other devices used in terrorism acts.

- Art. 7 of the Federal Decree Law N°2 of 2015 On Combating Discrimination and Hatred criminalizes hate speech and Art. 10 criminalizes the:
  misuse [of] religion to call individuals or groups as infidels by any means aiming to achieve their own interests or illegal purposes […]

- Art. 11 stipulates that:
  Any person who produces, manufactures, promotes, offers for sale or circulates products, goods, publications, recordings, movies, tapes, discs, software, smart applications or information in the field of electronic service or any other industrial materials or other things involving the means of expression, which may incite to commit blasphemy, or provoke discrimination or hate speech, shall be sentenced to imprisonment […]

- Art. 12:
  Any person, who acquires or possesses documents, publications, recordings, movies, tapes, discs, software, smart applications or information in the field of electronic services or any industrial materials or other things involving the means of expression that are intended for distribution or open for public aiming to offend religions, provoke discrimination or hate speech, shall be sentenced to imprisonment […]. Moreover, the same punishment shall apply to any person who acquires or possesses any means of printing, recording, storage, sound or visual recording devices or other means of publication, broadcasting or promotion that are used, with his knowledge, in the commission of any of the crimes set forth in the present Federal Decree.

- Art. 13:

  Any person, who establishes, sets up, organizes or manages an association, center, entity, organization, league or group or any branch thereof or uses any other means aiming to offend religions, or provoke discrimination or hate speech or any act involving encouragement or promotion of the same shall be sentenced to imprisonment for a period not less than ten years.

- In Canada, the Criminal Code of Canada does not have a specific offence of radicalizing someone to commit a terrorism offence or a terrorist activity, but it does have numerous offences that can be used to address the active encouragement of someone to commit a "terrorism offence" or a "terrorist activity".

  The Criminal Code has a comprehensive set of terrorism offences and a definition of "terrorist activity".

  The Criminal Code definition of "terrorist activity" has two parts. First, "terrorist activity" means an act or omission that is committed in or outside Canada and that, if committed in Canada, is an offence referred to in different subsections of Section 7 of the Criminal Code that implement various United Nations counter-terrorism conventions or protocols.

  The second part of the definition of "terrorist activity" reads, as follows:

  An act or omission, in or outside Canada,
  (i) that is committed
  (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and
  (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and
  (ii) that intentionally
  (A) causes death or serious bodily harm to a person by the use of violence,
  (B) endangers a person's life,
  (C) causes a serious risk to the health or safety of the public or any segment of the public,
  (D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or
  (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C) […]

Canada has extensive criminal law provisions that address incitement to terrorism. First, by the operation of Section 22 of the Criminal Code, a person who counsels the commission of any crime is a party to that offence. Subsection 22(3) of the Criminal Code defines "counsel" to include procure, solicit or incite. By Section 464 of the Criminal Code, it is also a crime to counsel the commission of a crime which is not committed.

Secondly, the definition of "terrorism offence", in Section 2 of the Criminal Code, provides, in paragraph (d) of the definition, that "terrorism offence" includes conspiracy or an attempt to commit, or being an accessory after the fact to, or any counselling in relation to a terrorism offence.
Thirdly, the definition of "terrorist activity" in Subsection 83.01(1) of the Criminal Code includes a conspiracy, attempt or threat to commit a terrorist activity, or being an accessory after the fact or counselling in relation to any terrorist activity. Hence, someone who, for example, incites another (inciting being one way to counsel) to commit an act or omission that constitutes "terrorist activity" engages in "terrorist activity". "Terrorist activity" is a key element found in the definitions of many terrorism offences, such as knowingly facilitating a terrorist activity (Section 83.19 of the Criminal Code), knowingly instructing any person to carry out a terrorist activity (Section 83.22 of the Criminal Code), or committing an indictable offence that constitutes a terrorist activity (paragraph 2(c) of the Criminal Code definition of "terrorism offence").

Finally, there is also an offence of knowingly advocating or promoting the commission of terrorism offences in general while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed (Section 83.221 of the Criminal Code).

The Criminal Code contains three hate propaganda offences: advocating and promoting genocide against an identifiable group (Subsection 318(1)), inciting hatred against an identifiable group in a public place that is likely to cause a breach of the peace (Subsection 319(1)), and willfully promoting hatred against an identifiable group other than in a private conversation (Subsection 319(2)). "Identifiable group" is defined as any section of the public distinguished by color, race, religion, national or ethnic origin, age, sex, sexual orientation or mental or physical disability. The offence of advocating or promoting genocide carries a maximum penalty of five years' imprisonment, while the offences of inciting hatred or willfully promoting hatred are punishable by a maximum penalty of two years' imprisonment.

By the application of subsections 22 and 464 of the Criminal Code, counselling the commission of murder is a crime, including whether or not the murder is committed.

- Singapore does not have a specific penal offence against the act of radicalization as such.

The following penal laws in Singapore can and have been used in situations where the criminalized conduct would not amount to the level of radicalization associated with terrorism and extremism leading to terrorism.

Sedition Act, which criminalizes acts with a tendency to "promote feelings of ill-will and hostility between different races or classes of the population of Singapore."

Penal Code, Section 298A, which makes it a criminal offence to knowingly promote or attempt to promote "disharmony or feelings of enmity, hatred or ill-will between different religious or racial groups", or to commit any act that the offender knows is "prejudicial to the maintenance of harmony between different religious or racial groups and which disturbs or is likely to disturb the public tranquility.

Both the Sedition Act and the Penal Code, Section 298A have been applied against material on the Internet.

- The act of radicalization is not as such a penal offence in New Zealand. The Human Rights Act of 1993 provides for prohibitions that may include radicalization.

  - Section 61 - Racial disharmony:
    (1) It shall be unlawful for any person:
    (a) to publish or distribute written matter which is threatening, abusive, or insulting, or to broadcast by means of radio or television or other electronic communication words which are threatening, abusive, or insulting; or
    (b) to use in any public place as defined in section 2(1) of the Summary Offences Act 1981, or within the hearing of persons in any such public place, or at any meeting to which the public are invited or have access, words which are threatening, abusive, or insulting; or
    (c) to use in any place words which are threatening, abusive, or insulting if the person using the words knew or ought to have known that the words were reasonably likely to be published in a newspaper, magazine, or periodical or broadcast by means of radio or television,—being matter or words likely to excite hostility against or bring into contempt any group of persons in or who may be coming to New Zealand on the ground of the colour, race, or ethnic or national origins of that group of persons.

    The Crimes Act of 1991 specifies in its Section 66 that:
    (1) Every one is a party to and guilty of an offence who
    (d) incites, counsels, or procures any person to commit the offence.

- The act of radicalization is not as such a penal offence in China. However, the Counter-Terrorism law of 2015 can be used to counter radicalized content.

  - Art. 2 of the Counter-Terrorism Law (2015):
    The State opposes all kinds of terrorism, bans terrorist organizations according to law, and pursues legal responsibilities of anyone who organizes, plots, prepares to carry out, or carry out terrorist activities; or who advocates terrorism, incites to

commit terrorist activities, organizes, leads, joins terrorist organizations, or aids terrorist activities. and

- Art. 3:
  "Terrorist Activities" as used in this law refers to the following acts of a terrorist nature: […]
  (2) Advocating terrorism, inciting others to commit terrorist activities, unlawfully possessing items that advocate terrorism, or compelling others to wear or bear clothes or symbols that advocate terrorism in a public place […]

  Offences under the Chinese Criminal Code can be used by way of analogy.

- Art. 120-3 of the criminal code:
  Advocating terrorism or extremism through methods such as producing or distributing items such as books or audio-visual materials advocating terrorism; or advocating terrorism or extremism by giving instruction or releasing information; or inciting the perpetration of terrorist activity; […]

- Art. 120-4 of the criminal code:
  Using extremism to incite or coerce the masses to undermine the implementation of legally established systems such as for marriage, justice, education or social management is sentenced to up to three years' imprisonment […]

- The act of radicalization is not as such a penal offence in Argentina.

  Other offences can be used to counter radicalization:

  Art. 41 of the reformed criminal code doubles the penalties for any crime committed with the aim of terrorizing the people or pressuring the national authorities or foreign governments or agents of an international organization to take some action.

  Art.213 the Argentine Criminal Code provides for the offence of advocacy of crime.

- The Norwegian Penal Code criminalizes the following acts as stand-alone crimes. The different offenses can in varying degree apply when a person is in the process of radicalization.

  (1) Participation in military operations against Norway (s. 119)
  (2) Terrorist acts (s. 131)
  (3) Terrorist conspiracy (s. 133)
  (4) Terrorist threats (s. 134)
  (5) Terrorist financing (s. 135)
  (6) Incitement, recruitment and instruction of terrorist acts, including training and being trained for terrorism (s. 136)
  (7) Participation in a terrorist organization (s. 136 a)
  (8) Aiding and abetting to evasion from punishment for terrorist acts (s. 137)
  (9) Hate speech (s. 185)
  (10) Public incitement to committing a criminal act (s. 183)

- In Kenya, pursuant to Art.12 D of the Prevention of Terrorism Act of 2012, N° 19 of 2014, s. 62, radicalization refers to: *"a person who adopts or promotes an extreme belief system for the purpose of facilitating ideologically based violence to advance political, religious or social change […]".*

  Other offences include:

  - Art. 27 of the same Act, incitement defined as acts committed by *"a person who publishes, distributes or otherwise avails information intending to directly or indirectly incite another person or a group of persons to carry out a terrorist act […]"*

  - Art. 13 of the National Cohesion and Integration Act from 2008 provides that:
    (1) A person who—
    uses threatening, abusive or insulting words or behavior, or displays any written material; publishes or distributes written material; presents or directs the performance the public performance of a play; distributes, shows or plays, a recording of visual images; or provides, produces or directs a program, which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behavior commits an offence if such person intends thereby to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up. […]

- Japan:

  The act of radicalization is not as such a penal offence under Japanese law.

  Other offences are however relevant:

  - Japan enacted its first anti-hate speech law in May 2016.

  - Art. 61 of the Criminal Code:
    Any person who induces a crime, directly or through an intermediary, is subject to sentencing as though the inducer had been one of the material executors of the offence.

- Egyptian Law does not have a specific offence relating to the act of radicalization. But has a number of provisions in its Anti-Terrorism Law of 2015 that may apply:

  - Art. 1 of Anti-Terrorism Law of 2015*:*
    In the application of the provisions of this Law, the following expressions and words shall bear the meaning indicated next to them: […]
    (B) Terrorist: Any natural person who commits, attempts to commit, incites, threatens, or plans a terrorist crime domestically or abroad by any means, even if individually, collaborates in such a crime in the context of a joint criminal venture, or commands, leads, manages, founds, or establishes or of any terrorist entity as

stipulated in article (1) of President of the Arab Republic of Egypt Decree by Law N° 8 of 2015 on the designation of terrorists, terrorist entities, or any person who funds such entities or contributes to their activity knowingly.

(C) Terrorist Crime: Any offense stipulated in this Law and any felony or misdemeanor committed by using a means of terrorism or in order to achieve or carry out a terrorist act, call to commit any crime of the above, or threaten to commit such a crime, without prejudice to the provisions of the Criminal Code […].

- Art. 6:
Incitement to commit a terrorist crime shall be punished with the same penalty prescribed for the completed offense, whether the incitement is directed at a specific person or group, in public or private, regardless of the method used, and even if such incitement does not result in any impact. […]

- Art. 28:
Whoever promotes or prepares to promote, directly or indirectly, the perpetration of any terrorist crime, whether verbally, in writing, or by any other means, shall be punished by imprisonment for no less than five years.
Indirect promotion shall include the promotion of ideas and beliefs inciting the use of violence by any of the means set forth in the preceding paragraph of this Article.
[…] Whoever possesses or acquires any public means of printing or recording used or intended for use, even if temporarily, for the purpose of printing, recording, or broadcasting the aforementioned shall be punishable by the same penalty set forth in the first paragraph of this Article.

- Art. 29:
Whoever establishes or uses a communications site, website, or other media for the purpose of promoting ideas or beliefs calling for the perpetration of terrorist acts or broadcasting material intended to mislead security authorities, influence the course of justice in any terrorist crime, exchange messages, issue assignments among terrorist groups or their members, or exchange information relating to the actions or movement of terrorists or terrorist groups domestically and abroad shall be punished by imprisonment with hard labor for no less than five years.

Whoever unduly or illegally accesses websites affiliated with any government agency in order to obtain, access, change, erase, destroy, or falsify the data or information contained therein in order to commit an offense referred to in the first paragraph of this Article or prepare it shall be punishable by imprisonment with hard labor for no less than ten years.

Art. 86 bis of the Criminal Code punished the participation in groups
"the purpose of which is to call by any method, for interrupting the provisions of the constitution or laws, or preventing any of the Slate's institutions or public authorities from exercising its works, or encroaching on the personal freedom of citizens or other freedoms and public rights as guaranteed by the constitution or the law, or impairing the national unity or social peace. […]".

- The act of radicalization is not as such a penal offence in Brazil. However, the Anti-Terrorism law of 2016 prohibits and punishes terrorist-related offences:

  - Promotion of and Preparation for Terrorism:
    Whoever promotes, creates, takes part in, or provides assistance to, in person or through an intermediary, a terrorist organization will be punished (id. Art. 3).

  - Terrorist Recruitment and Training:
    The same punishment of five to eight years' imprisonment and a fine applies to those who, for the purpose of practicing acts of terrorism, recruit, organize, transport, or equip with ammunition individuals traveling to a country other than that of their residence or nationality or who provide or receive training in a country other than that of their residence or nationality. (Id. Art. 5(§1).)

    Brazilian legislation also condemns crimes against public peace, such as incitement to criminal behavior or apology of crime.

- The act of radicalization is not as such a penal offence in Poland. However, a new Anti-Terrorism Law was adopted on 22 June 2016. According to this law acts of a terrorist nature […] include the expression of *"fundamentalist slogans" by representatives of Muslim institutions in Poland; information indicating the intent of a foreign national from a "high risk" country coming to Poland for academic training or to study; details relating to conferences/seminars/meetings of foreigners from "high risk" countries on Polish territory; details of plans to establish Islamic universities in Poland; information regarding the participation of Polish nationals in Internet platforms (chat rooms and forums) on so-called "radical Muslim websites […]".*

  Other offences can be used to counter radicalization.

  - Art. 119 of the Criminal Code:
    § 1. Whoever uses violence or makes unlawful threats towards a group of persons or a particular individual because of their national, ethnic, political or religious affiliation, or because of their lack of religious beliefs, shall be subject to the penalty […]
    § 2. The same punishment shall be imposed on anyone, who incites commission of the offence specified under § 1.

  - Art. 255 of the Criminal Code:
    § 1. Whoever publicly incites to the commission of an offence, shall be subject to a […] penalty […]
    § 3. Whoever publicly praises the commission of an offence, shall be subject to a […] penalty […]

  - Art. 256 of the Criminal Code:

Whoever publicly promotes a fascist or other totalitarian system of state or incites hatred based on national, ethnic, race or religious differences or for reason of lack of any religious denomination shall be subject to a […] penalty […]

- Art. 257 of the Criminal Code:
  Whoever publicly insults a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his lack of any religious denomination or for these reasons breaches the personal inviolability of another individual shall be subject to a penalty [...]

- In the United States the Bill of 23 October 2007 (Act to prevent Homegrown Terrorism), which was however not passed by the Senate, contains the following definition of "radicalization":[30]

"'VIOLENT RADICALIZATION. —The term 'violent radicalization' means the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. […]"

''IDEOLOGICALLY BASED VIOLENCE. —The term 'ideologically based violence' means the use, planned use, or threatened use of force or violence by a group or individual to promote the group or individual's political, religious, or social beliefs."[31]

At the European level a definition of the term "radicalization" would not appear possible from the European Court of Human Rights case-law.

The Court does not use the term (apart from once in a case from 2013, in the - very different - context of a strike).

The Council of Europe Convention on the Prevention of Terrorism of 16 May 2005 does not define radicalization, it contains the following definition of **"public provocation to commit a terrorist offence"** (Art.5): *"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."*

The Convention also defines **"recruitment for terrorism"** (Art. 6) as the act: "*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."*

---

[30] H.R. 1955 (110th): Violent Radicalization and Homegrown Terrorism Prevention Act of 2007. Available at: https://www.govtrack.us/congress/bills/110/hr1955/text. [Accessed 27 September 2016].

[31] H.R.1304 (111th): Free Speech Protection Act of 2009 (Free Speech Protection Act of 2009. Available at: https://www.congress.gov/bill/111th-congress/house-bill/1304/text. [Accessed 27 September 2016]; See also Holmer, I. (2016): "Explaining the appeal of militant Salafism in a Norwegian context", *FLEKS*, Volume 3, No. 1, p. 1: *"When referring to radicalization, I mean the "…change in beliefs, feelings, and behaviors in directions that increasingly justify intergroup violence and demand sacrifice in defense of the in-group (McCauley and Moskalenko, 2008: 416).*

- o -

Most of the definitions currently employed describe radicalization as the process whereby individuals or groups of individuals come to approve of and (ultimately) participate in the use of violence for ideological, political or religious objectives. Some authors refer to "violent radicalization" in order to emphasize the violent outcome and distinguish the process from non-violent forms of "radical" thinking.[32]

Another definition of "online radicalization" as related by RAND[33] reads: *"a process whereby individuals through* […] *their online interactions and exposures to various types of Internet context, come to view violence as a legitimate method of solving social and political conflicts"*.[34]

Jessica Stern and J.M. Berger in their book ISIS: "*The State of Terror"* suggest the following definition:

"Radicalization is a process involving an individual or group whereby they are indoctrinated to a set of beliefs that support acts of terrorism, that can be manifested in one's behaviour and attitudes."[35]

The Royal Canadian Mounted Police defines radicalization "*as the process by which individuals - usually young people - are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs towards extreme views."*[36]

The FBI defines *"violent extremism"* as the act of *"encouraging, conditioning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social or economic goals."*[37]

---

[32] Stevens T; Neumann P. (2009): "Countering Online Radicalization, A Strategy for Action", Policy report published by the International Centre for the Study of Radicalization and Political Violence (ICSR), p.10 Available at: http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalizationReport.pdf [Accessed 27 September 2016].
See also: The Centre for the Prevention of Radicalization leading to violence defines "radicalization" as: "*A process whereby individuals adopt an extremist belief system – including the willingness to use, support, or facilitate violence – in view of achieving the triumph of an ideology, a political project, or a cause as a means to effecting changes in society*." Available at: https://info-radical.org/fr/radicalization/definition/ [Accessed 27 September 2016].

[33] RAND ("Research And Development") is a research organization that develops solutions to public policy challenges. Available at http://invention.si.edu/research-and-development-rand-corporation-videohistory-collection-1987-1990 [Accessed 27 September 2016].

[34] Von Behr, I.; Reding, A.; Edwards, C.; Gribbon L. (2013): "Radicalization in the digital era The use of the internet in 15 cases of terrorism and extremism", RAND. (p. 2-3).

[35] Stern, J. and Berger, J.M. (2015) *Isis: The state of terror*. New York, NY: Ecco Press. p. 302, See also: Directorate-General Justice, Freedom and Security, European Commission (2009), "Manual for trainers", Community Policing Preventing Radicalization & Terrorism. Available at: http://www.coppra.eu/dl%5Cpreview%20trainers%20manual.pdf [Accessed 27 September 2016].
In the handbook "Violent radicalization: recognition of and responses to the phenomenon by professional groups concerned" (2008), the authors use a narrow definition:
Radicalization might be defined as:
• *The growing willingness to support far-reaching changes in society, which may be aimed to the abolition of the established democratic legal order and which may involve the use of Undemocratic methods.*
• *A process that leads an individual or a group to accept, support or encourage the use of violence as a political means."*

[36] Royal Canadian Mounted Police, National Security Criminal Investigations (2009), Radicalization - *A Guide for the Perplexed*. Available at: http://publications.gc.ca/collections/collection_2012/grc-rcmp/PS64-102-2009-eng.pdf [Accessed 27 September 2016].

[37] FBI (2016) Available at: www.cve.fbi.gov; [Accessed 27 September 2016**].**

In light of the above, the concept of radicalization is linked to well defined notions like "terrorism" and "hate speech" (in its various manifestations). It is more abstract however and removed from the actualization of these associated crimes. Radicalization seems to contain an important ingredient of (1) manipulation/conditioning with the (2) intention to incite (3) violent action by the recipient (4) in the name of an ideology or religion (5) without regard to the "innocence" of the victims.

Before turning to a definition the following questions must also be addressed:

1) Does the definition need to include an intentional element ("*mens rea*") or will it suffice to establish the potentiality of causation?

2) Should the definition include a subjective element on the "recipient's" side causing the contextual analysis also to consider whether the content in question is likely to lead to the commission of violent acts on account of the recipient's "vulnerability" or pre-conditioned ("groomed") state?

Caution should be applied against subjective or relative approaches. It would not only lower the threshold, but also largely complexify content examination. Clearly the same message may impact on a recipient in various ways as a result of his/her specific situation and environment.

From a legality point of view content qualification must rely on objective standards.

3) Should the definition include an element of counter factuality?

To a large extent radicalizing content owes its compelling nature to its unconventional interpretation and rendition of history and its vision of societal dynamics. For the purposes of our definition it seems unnecessarily controversial to include an element of counter factuality.

"Radicalization" designates a process. The "radicalizing content" has not - yet - turned into a direct call to commit a specific act of terrorism, recruitment, instruction or training, but rather a precursory inducement (or approval) for such later action. At the same time "radicalizing content" should not be so far removed from the potential act of violence that it encompasses content of a merely shocking, offending or disturbing nature.

The term "radicalization" is not only linked to the concept of "terrorism" [38], but also to concepts such as "incitement to hatred" and "genocide", "crimes against humanity" and notions like apostasy, takfir, negationism, disobedience of "the law of the land", defamation and offences of religious faith or sentiments. All form part of the conceptual panoply of radicalization.[39]

Radicalization is a process as we have seen and furthermore it is indispensable to integrate a reference to its likely effects. The effects may however not necessarily be qualified as "imminent" as opposed to the Brandenburg Doctrine.[40]

The importance of "violence" is exemplified by incitement or encouragement to protest against government policy by non-violent means for instance peaceful demonstrations, calls for civil

[38] The Media Development Foundation (Georgia) expresses the view that "Criminalizing the publication of material is more appropriate than criminalizing incitement and direct, immediate and clear threat should be identified for such restriction" (Annex 1 "Country Questionnaire/Survey").

[39] Stevens T; Neumann P. (2009): "Countering Online Radicalization, A Strategy for Action", Policy report published by the International Centre for the Study of Radicalization and Political Violence (ICSR). Available at: http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalizationReport.pdf [Accessed 27 September 2016]. (p. 10)

[40] *Brandenburg v. Ohio* [1969], 395 U.S. 444 (Supreme Court of the United States): *Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.* […]*."*

disobedience, strikes or not to pay taxes (which in some countries is equivalent to "rebellion"). Such "incitement" is obviously not germane to the definition of "radicalizing content". Encouragement (potentially or of a precursory nature) to commit violent acts against individuals or groups not vested with governmental authority is an essential feature of the illicitness of "radicalizing content".

On the other hand, content that may most likely condition action directed against a government should be excluded owing to the specific and undesirable risk to free speech for repressive purposes.

"Violence" should not be limited to physical violence against individuals and groups of individuals. It should encompass destruction of property, infrastructure and economic violence.

The definition should not include a reference to "terrorism".

Finally, the ideology or belief provoking or conditioning radicalization should not be predicated upon any distinctive features (for instance "fostering hatred"). The performance of content qualification should preclude determination of the characteristics of ideology.

The author suggests the following definition:
"Radicalizing content" designates content which taken in context may likely condition a recipient under normal circumstances to endorse or be mentally disposed to engage in violent acts intentionally causing deaths or bodily harm or a serious danger to health or safety or substantial damage to infrastructure, private property, economic security or enterprise or serious intimidation of the population in whole or in part and directed indiscriminately against an individual, a nation, a people, an ethnic, religious or any other group in the name of or by glorification of an ideology or belief.

Section 3: Freedom of Speech: The challenge

3.a. General Principles of Freedom of Speech

The international community's response to Internet radicalization even in the absence of an agreed definition has been forceful and consequential. Several initiatives have been employed directly targeting dissemination of such content by way of criminalization and calls for coordinated action with civil society and industry stakeholders.

Given the somewhat judgmental features of "radicalizing content" (even if a legally viable definition is eventually agreed) and the universal nature of the Internet this Section outlines the essential qualities and scope of freedom of speech protection and its **general** exceptions as developed in international law and different countries in order to determine how far regulation of content may go without encroaching upon the protection guaranteeing freedom of speech.

In below Section 3.c we shall complete this overview by identifying areas where **specific** restrictions to freedom of speech have achieved consensus.

- o -

International instruments protecting free speech cover most countries around the world.

The central current instrument is the "International Covenant on Civil and Political Rights" (ICCPR) of 16 December 1966:

> **Art.19**
>
> *"*[…]
>
> *2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*
>
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals."*[41]

The protection of freedom of speech on media in general and the Internet in particular (the question of alignment will be developed in Section 3.b *infra*), has been reaffirmed by international treaties, resolutions, national laws and case law around the world:

Freedom of speech protection is recognized by countries and regions all over the world (albeit with varying interpretations and scope).

In Latin America the Inter-American Court of Human Rights has made numerous judgements on the protection of free speech.[42]

---

[41] Art. 19 of the International Covenant on Civil and Political Rights as opposed to the Universal Declaration of Human Rights (10 December 1948) is a legally binding instrument.

[42] *RCTV v. Venezuela* (22 July 2015); *Lopez Lone et al. v. Honduras* (5 October 2015); *Velez Restrepo y Familiares v. Colombia* (3 September 2012); *Uzcategui y Otros v. Venezuela* (3 September 2012); *Manuel Cepeda Vargas v. Colombia* (26 May 2010); *Gomes Lund et al. v. Brazil* (24 November 2010); *Rios (and Perozo) et al. v. Venezuela* (28 January 2009); *Lopez Alvarez v. Honduras* (1 February 2006); *Ricardo Canese v. Paraguay* (31 August 2004); *Ivcher-Bronstein v. Peru* (6 February 2001); *Claude Reyes et al. v. Chile* (19 September 2006); *Olmedo-Bustos et al. v. Chile* (5 February 2001); *Palamara-Iribarne v. Chile* (22 November 2005); *Kimel v. Argentina* (2 May 2008).

The East African Court of Justice has recently applied the same principles[43] and so does the African Court on Human and Peoples' Rights.[44]

The European Court of Human Rights has consistently adopted an unyielding position in support of quint-essential properties of free speech.

Freedom of speech is far-reaching and includes other freedoms like freedom of religion. Thus in the United States religious freedom is protected by the First Amendment which also protects free speech.

As the United States Supreme Court famously said*, "The law knows no heresy, and is committed to the support of no dogma, the establishment of no sect."*[45]

Freedom of speech is not without limits however. Indeed, the preeminent international instruments protecting freedom of speech as a human right explicitly stipulate restrictions:

"The exercise of the rights provided in paragraph 2 of this article carries with it ***special duties and responsibilities*** [...]*"* (International Covenant on Civil and Political Rights Art. 19. 3).

A congruent exception is found in the European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950), Art. 17:

"Prohibition of abuse of rights

Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act ***aimed at the destruction of any of the rights and freedoms*** *set forth herein or at their limitation to a greater extent than is provided for in the Convention*."

Restrictions of Speech can also be found in the American Declaration of the Rights and Duties of Man (2 May 1948):

"Preamble

---

43 *Burundian Journalists Union v. The Attorney General of the Republic of Burundi* [2015], n°07-2013 (East African Court of Justice, First Instance Division). In its first decision on free speech, the East African Court of Justice found Burundi's 2013 Press Law to violate the fundamental principles of the rule of law: *"[…] the principles of democracy must of necessity include adherence to press freedom. In our view, citizens of any democratic State should be entitled to information that informs their choices in matter of governance […] a government should not determine what ideas or information should be placed in the market place of information and we dare add, if it restricts that right, the restriction must be proportionate and reasonable. We have grave doubts about some of the aspects of the Press Law in applying that test. In that regard the following restrictions, in our view, cannot face the test of reasonability, rationality or proportionality i.e. the restriction not to disseminate information on the stability of the currency, offensives articles or reports regarding public or private persons, information that may harm the credit of the State and national economy, diplomacy, scientific research and reports of Commission of Inquiry by the State […]."*

44 *Lohé Issa Konaté v. Burkina Faso* [2014], n°004/2013 (African Court on Human and Peoples' Rights).

45 The so-called "Establishment clause". Rascoff S. (2012): "Establishing Official Islam? *The Law and Strategy of Counter-Radicalization*", *Stanford Law Review*, Volume 64, Issue 1, p. 125. Available at: http://poseidon01.ssrn.com/delivery.php?ID=811029101084126106086103102019091027053076059068029030090096090099024083089119003075018124107061016122018113085103122001121095117071001040021126014117001078002092124055058043103123096122088071102009121001075127090119067102013124091073115064011024002118&EXT=pdf [Accessed 27 September 2016].
See also: Article 19 (2013), "Internet intermediaries: Dilemma of Liability". Available at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf [Accessed 27 September 2016]. In the case Epperson v. Arkansas, 393, U.S. 97, 103-104 (1969) the judge summarized as follows: *"Government in our democracy, state and national, must be neutral in matters of religious theory, doctrine, and practice. It may not be hostile to any religion or to the advocacy of no-religion; and it may not aid, foster, or promote one religion or religious theory against another or even against the militant opposite."*

[…] *While rights exalt liberty, duties express the dignity of that liberty* […]

Article I. Every human being has the right to life […]

Article XXVIII. The rights of man are limited by the rights of others, by the security of all and by the just demands of the general welfare and the advancement of democracy."

The same principle is enshrined in the Arab Charter on Human Rights, Art. 30 (League of Arab States, 22 May 2004); in the African Charter on Human and People's Rights, Art. 9 (African Union, 27 June 1981) and in the Cairo Declaration on Human Rights in Islam (1990).

The concepts of "Special Duties and Responsibilities" and "Abuse of Rights" have been recognized in numerous cases worldwide.

An example from the European Court of Human Rights illustrates their application in a case involving incitement to religiously motivated violence:

Kasymakhunov and Saybatalov v. Russia (14 March 2013):

"[…] T*he experts noted that Hizb ut-Tahrir's literature advocated and glorified warfare in the form of jihad, a term which was mainly used in its meaning of "holy war", to establish the domination of Islam* […]. *The Court finds that the dissemination of the political ideas of Hizb ut-Tahrir by the applicants clearly constitutes an activity falling within the scope of Article 17 of the Convention. The applicants are essentially seeking to use Articles 9, 10 and 11 to provide a basis Under the Convention for a right to engage in activities contrary to the text and spirit of the Convention."*[46]

Another example where the European Court of Human Rights rejected free speech protection to speech inciting violence by reference to the above general limitations on free speech is the case *Pavel Ivanov v. Russia* (20 February 2007):

"[…] *that a general and vehement attack on an ethnic group contradicts the underlying values of the European Convention on Human Rights ("ECHR"), most notably tolerance, social peace, and non-discrimination. Such an attack would remove such groups from the protection of Article 10 of the ECHR. Consequently, on the basis of Article 17 of the Convention* […]*."*[47]

The Abuse of Rights principle in Art. 17 is also applied by national courts. An example is *Norwood v. The United Kingdom* (16 November 2004):

"The general purpose of Article 17 is to prevent individuals or groups with totalitarian aims from exploiting in their own interests the principles enunciated by the Convention. The Court, and previously, the European Commission of Human Rights, has found in particular that the freedom of expression guaranteed under Article 10 of the Convention may not be invoked in a sense contrary to Article 17."[48]

Abuse of Rights restrictions often call for a difficult and delicate balancing act between conflicting human rights.

An example from Canadian case law illustrates the application of the theory when freedom of speech negates other human rights: *Saskatchewan human Rights Commission v. Whatcott* (27 February

---

46 *Kasymakhunov and Saybatalov v Russia* [2013], Case No. 26261/05 and 26377/06 (European court of Human Rights).

47 *Pavel Ivanov v. Russia* [2007], Case No. 35222/04 (European court of Human Rights).

48 *Norwood v. the United Kingdom* [2004], Case No. 23131/03 (European court of Human Rights).

2013): *"Freedom of expression is central to our democracy. Nonetheless, this Court has consistently found that the right to freedom of expression is not absolute and limitations of freedom of expression may be justified* […] *Section 1 both "guarantees and limits Charter rights and freedoms by reference to principles fundamental in a free and democratic society* […] *The limitation imposed on freedom of expression* […] *when properly defined and understood, is demonstrably justified in a free and democratic society."*[49]

Case law on the reconciliation of the conflicting imperatives is abundant. It includes cases from the European Court of Human Rights, the European Court of Justice, the Inter American Court of Human Rights, The East African Court as well as national courts, ref. the following examples:

From the Inter American Court of Human Rights:

Case Fontevecchia and D'Amico v. Argentina, Judgment of 29 November 2011:

"[…] *The media, as essential instruments of freedom of thought and expression, are required to discharge their social function responsibly.*
[…] *equity must regulate the flow of information…*
[…] *the Court must find a balance between private life and freedom of expression that, not being absolute, are two fundamental rights guaranteed by the American Convention and of great importance in a democratic society. The Court recalls that every fundamental right is to be exercised with regard for other fundamental rights* […]*"*[50]

From the European Court of Justice:

Case *Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen and Others*, Judgment of 3 September 2014, (C-201/13):

"[…] *the Court notes that the application of the exception for parody, established by the directive (2001/29/CE), must strike a fair balance between, on the one hand, the interests and rights of authors and other rights holders and, on the other, the freedom of expression of the person who wishes to rely on that exception."*[51]

In the United States First Amendment case law applying limitations to freedom of speech is extremely rare[52], but certain elements of "striking the balance" may be detected in some cases.

An example is *Planned Parenthood v. American Coalition of Life Activists* (16 May 2002):

---

[49] *Saskatchewan Human Rights Commission v. Whatcott* [2013], 2013 SCC 11 (Supreme Court of Canada); Available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12876/index.do. [Accessed 30 September 2016]. In Canada, Section 1 of the Canadian Charter of Rights and Freedoms states that it *"guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstratively justified in a free and democratic society."* This wording embodies the idea that constitutional rights are not absolute.

[50] *Fontevecchia and D'Amico v. Argentina* [2011], (Inter-American Court of Human Rights).

[51] *Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen and Others* [2014], Case C-201/13, Court of Justice of the European Union, Grand Chamber. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=157281&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1446412 [Accessed 30 September 2016].

[52] *Brandenburg v. Ohio* [1969], 395 U.S. 444 (Supreme Court of the United States). See also: *Snyder v. Phelps* [2011], 562 U.S. 443 (Supreme Court of the United States): Fred Phelps maintained that God punishes the United States for its tolerance of homosexuality, which they openly advocated at a funeral service with signs like "God Hates the USA/Thank God for 9/11," and "Thank God for Dead Soldiers". The Supreme Court held that the Phelps and his followers were "speaking" on matters of public concern and were entitled to protection Under the First Amendment.

"*Violence is not a protected value. Nor is a true threat of violence with intent to intimidate. By replicating the poster pattern that preceded the elimination of Gunn, Patterson and Britton, and by putting Crist, Hern, and the Newhalls in an abortionists' File that scores fatalities, ACLA was not staking out a position of debate but of threatened demise. This turns the First Amendment on its head. Like "fighting words," true threats are proscribing. We therefore conclude that the judgment of liability in physicians' favour is constitutionally permissible."*[53]

Freedom of speech is recognized as a human right, but it is not the only human right.
Other rights include the right to life (International Covenant on Civil and Political Rights, Art. 6 and European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 2). Each of those rights deserves protection - indeed equal protection. Limiting freedom of speech protection to the perimeter imposed by the co-existence of these other rights does not amount to a violation of free speech protection.

The MacBride report which was commissioned by UNESCO in 1980 acknowledges the importance of freedom of speech while at the same time balancing it against other human rights including specific country based traditions and values: "*It is widely recognized that freedom must be reconciled with an obligation to obey the law and must not be exploited to injure the freedom of others; also that the exercise of freedom has a counterpart which is the need to exercise it with responsibility, which in the field of communication means primarily a concern for truth and the legitimate use of the power it conveys."*[54]

3.b. Internet and Free Speech

It has been established through diverse resolutions and decisions that the rights and obligations that apply to the "offline world" also apply online.[55]

The right to free speech furthermore embraces a right to information and a right to access with the advent of the Internet.[56]

---

53 *Planned Parenthood v. American Coalition of Life Activists* [2002], 290 F. 3d 1058 (U.S. Ct. App. 9th Cir.). Available at: http://www.tumca.org/2011%20Cases/Planned%20Parenthood%20v.%20ACLA%20_%20290%20F.3d%201058_%202002.pdf. [Accessed 30 September 2013]. Opinion of Judge Rymer.

54 ICCP (1980), International Commission for the Study of Communication Problems, chaired by Sean MacBride, Communication and Society Today and Tomorrow: Many Voices One World: Towards a new more just and more efficient world information and communication order, Paris: UNESCO. (p. 18).

55 An example is the International Telecommunication Union (ITU) declared that the right to freedom of opinion and expression "is an essential foundation of the Information Society" (2003).

56 United Nations (1996), The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, E/CN.4/1996/39. Available at: http://hrlibrary.umn.edu/instree/johannesburg.html [Accessed 27 September 2016] have been regularly endorsed by the United Nations Special Rapporteur on Freedom of Opinion and Expression, and by the United Nations Commission on Human Rights and Human Rights Council. In 2012 the General Assembly, Human Rights Council (29 June 2012) declared the extension of "offline rights" to the online sphere:
The Human Rights Council […]
Noting that the exercise of human rights, in particular the right to freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies,

Protection of Free Speech on the Internet has become so pervasive that it may even be protected by international trade agreements. Thus it has been argued that China's censorship of the Internet constitutes a barrier to international trade and may amount to a violation of the World Trade Organization's treaties in so far it restricts online commerce.[57]

In the EU, specific protection of freedom of speech on the Internet has been reiterated in directives, regulations and case law and explicitly extended to cover rights to access information[58] and net neutrality.

UNESCO at its General Conference (10 August 2015), in accordance with the R.O.A.M Principles reaffirmed: [59]

> "[…] *that freedom of expression applies, and should be respected, online and offline in accordance with Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights* […]
>
> *3.4 Noting the relevance to the Internet and digital communications of the international Convention on the Rights of Persons with Disabilities (CRPD), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the work of the*

---

1. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression […] The Special Rapporteur (Frank La Rue) confirms this principle:
By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur Underscores that article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet.
Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as an interactive medium. La Rue, F. (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, United Nations, A/HRC/17/27. Available at:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [Accessed 27 September 2016].

[57] Whether the Internet is covered by the GATT and GATS agreements has not been addressed by the World Trade Organization, Source: King & Spalding LLP (2007): "Free Speech Group Petitions U.S. Trade Representative to File WTO Complaint to End Chinese Internet Censorship, Reports", *Business Wire*. Available at: http://www.businesswire.com/news/home/20071210005945/en/Free-Speech-Group-Petitions-U.S.-Trade-Representative [Accessed 27 September 2016].

[58] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031 [Accessed 27 September 2016].
Article 3
"Internal market
[…]
Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.
Freedom to provide (and not just receive) information is professed as a key feature of the Internet:
Regulation (EU) 2015/2120 (November 2015) laying down measures concerning open Internet access:
'End-users should have the right to access and distribute information and content, and to use and provide applications and services without discrimination, via their Internet access service. The exercise of this right should be without prejudice to Union law, or national law that complies with Union law, regarding the lawfulness of content, applications or services. […].
The Council of Europe at its meeting (30 March 2016) on Internet Governance (Council of Europe Strategy 2016-2019) confirmed that:
3. The Council of Europe is recognized for its work on protecting the Internet's Universality, integrity and openness. It has reasserted the need to protect and empower citizens without hindering their freedom to use the Internet for everyday activities."

[59] R.O.A.M. refers to the Outcome Document on Connecting the Dots.

Office of the High Commissioner on Human Rights, concerning the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Rabat Plan of Action 2012), promote educational and social mechanisms for combating online hate speech, without using this to restrict freedom of expression."[60]

An interesting case before the Inter-American Court of Human Rights illustrates enhanced protection of free speech on the Internet:

Case of *Norín Catriman et al. (leaders, members and activists of the Mapuche Indigenous People) v. Chile*, Judgment of May 29, 2014.

In its ruling, the Court examined whether prohibiting members of the Mapuche Indigenous People from using social media was compatible with the American Convention on Human Rights Treaty Art. 13.[61]

The Court found that this prohibition imposed undue restrictions on the right to freedom of expression.[62]

- o -

Specific Media Rights were already enacted in the 1970s, but as it will be seen free speech on the Internet has developed into a concept unencumbered by the restrictions inherent in these early Media Rights.

UNESCO adopted the "Declaration on Fundamental Principles concerning the Contribution of the Mass Media to Strengthening Peace and International Understanding, to the Promotion of Human Rights and to Countering Racialism, apartheid and incitement to war" on 28 November 1978.

This Declaration included restrictions on certain forms of content (interestingly it appears that over time these early policies on media content restrictions are being reintroduced after an initial Internet driven libertarian ideology):

"Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated;

---

60 The Riga Guidelines on Ethics in the Information Society (16-17 October 2013) state a commitment:
"[…] to the full implementation in cyberspace of the human rights and fundamental freedoms proclaimed in the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, the resolution "The promotion, protection and enjoyment of human rights on the Internet" adopted by United Nations Human Rights Council A/HRC/20/8, and other Universally recognized legal instruments", UNESCO (2013), Riga Guidelines on Ethics in the Information Society. Available at:http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/ifap/ifap_riga_guidelines_ethics_in_information_society_en.pdf [Accessed 27 September 2016]. See also: The African Declaration on Internet Rights and Freedoms (Project) expresses the following objectives: Article 3: Freedom of Expression: "*Everyone has the right to hold opinions without interference. Everyone has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through the Internet and digital technologies and regardless of frontiers* […]."

Article 4: Right to Information*: "Everyone has the right to access information on the Internet. All information, including scientific and social research, produced with the support of public funds, should be freely available to all, including on the Internet*.". Source: The African Declaration on Internet Rights and Freedoms. Available at: http://africaninternetrights.org/articles/ [Accessed 27 September 2016].

61 *"Article 13. Freedom of Thought and Expression*
1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice."

62 *Norín Catriman et al. (leaders, members and activists of the Mapuche Indigenous People) v. Chile* [2014] Inter-American Court of Human Rights. Available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_279_ing.pdf. [Accessed 30 September 2016].

[…] *Freedom of information requires as an indispensable element the willingness and capacity to employ its privileges* ***without abuse****. It requires as a* ***basic discipline the moral obligation*** *to seek the facts without prejudice and to spread knowledge without malicious intent;"* [the author's emphasis]

"Recalling Resolution llO(I1) of the General Assembly of the United Nations, adopted in 1947, condemning all forms of propaganda which are designed or likely to provoke or encourage any threat to the peace, breach of the peace, or act of aggression, Recalling resolution 127(11), also adopted by the General Assembly in 1947, which invites Member States to take measures, within the limits of constitutional procedures, to combat the diffusion of false or distorted reports likely to injure friendly relations between States, as well as the other resolutions of the General Assembly concerning the mass media and their contribution to strengthening peace, trust and friendly relations among States."

- o -

It is interesting in the light of the above that the restrictions on abuse, incitement and the promotion of *"friendly relations"* and tolerance which were anchored in the early media related instruments have been partially eclipsed by free speech protection (except UNESCO 10.8.2015).

Since human rights protection in the online and offline world is considered aligned the balancing act that we have seen *supra* under 3.b must also be performed with regard to content regulation online.

The Special Rapporteur to the United Nations (Frank La Rue) summarized the challenge as follows:

"[…] *like all technological inventions, the Internet can be misused to cause harm to others. As with offline content, when a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights , namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other Unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application (p. 19)."*[63]

Notwithstanding the dominance of free speech advocacy, it may safely be affirmed that not only freedom of speech but also other human rights recognized by the international community are preserved in the online world and that this alignment includes the rights as well as their limitations as enunciated in the

63 La Rue, F. (2011): Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council Seventeenth Session Agenda item 3.

International Covenant on Civil and Political Rights Art. 19.3 and the European Convention for the Protection of Human Rights and Fundamental Freedoms Art. 17.

3.c. Specific Restrictions on Freedom of Speech

Given that the protection of human rights offline and online are aligned and that their enjoyment is subject to the restrictions imposed by their necessary co-existence, this section covers specific restrictions to free speech as they apply to distinct activities/domains as articulated in treaties, regional and national laws, regulations and case law. These restrictions are specific and complementary to the general theories of "Abuse of Rights" and "Special Duties and Obligations" as enunciated by Art. 19.3 of the International Covenant on Civil and Political Rights and Art. 17 pf the European Convention for the Protection of Human Rights and Fundamental Freedoms.

The International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965 provides an example of such particular restrictions or limits to free speech. Its Art. 2 mandates the State Parties to *"prohibit and bring to an end, by all appropriate means, including legislation as required by circumstances, racial discrimination by any persons, group or organization."*

The International Covenant on Civil and Political Rights imposes a specific obligation upon States to prohibit speech conceived as *"any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."* (Art. 20 (2)).

Category or domain based limitations cover a wide range of activities (commercial as well as non-commercial). Many examples of such limitations apply explicitly to the Internet and it is even often considered an aggravating circumstance if violations of these restrictions (*i.e.* illicit speech) occur online.

Such restrictions include online advertising of goods and services deemed illegitimate owing to their dangerous/harmful nature or the perception that unregulated commercialization/distribution may lead to overconsumption or abuse. In the interest of public health, consumer protection, protection of minors and individuals in a vulnerable state, safety, the environment and even morals many such restrictions have developed over the years and enjoy worldwide consensus.[64]

[64] Below, a list (non-exhaustive) of directives in The European Union imposing specific restrictions:
Directive 93/13/EEC of 5 April 1993 on Unfair terms in consumer contracts, Directive 97/7/EC […] of 20 May 1997 on the protection of consumers in respect of distance contracts […], Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising, Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit, Directive 93/22/EEC of 10 May 1993 on investment services in the securities field, Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours, Directive 98/6/EC […] of 16 February 1998 on consumer production in the indication of prices of products offered to consumers, Directive 92/59/EEC of 29 June 1992 on general product safety, Directive 94/47/EC […] of 26 October 1994 on the protection of purchasers in respect of certain aspects on contracts relating to the purchase of the right to use immovable properties on a timeshare basis, Directive 98/27/EC […] of 19 May 1998 on injunctions for the protection of consumers' interests, Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions concerning liability for defective products, Directive 1999/44/EC of the European Parliament and of the Council of

The Unlawful Internet Gambling Enforcement Act (13 October 2006) in the United States provides an example of such targeted restrictions.[65]

Another example is the Council of Europe Convention on the Counterfeiting of Medical Products and Similar Crimes Involving Threats to Public Health (Moscow, 28.X.2011):

> *Article 6 –Supplying, offering to supply, and trafficking in counterfeits*
>
> *1. Each Party shall take the necessary legislative and other measures to establish as offences under its domestic law, when committed intentionally, the supplying or the offering to supply, including brokering, the trafficking, including keeping in stock, importing and exporting of counterfeit medical products, active substances, excipients, parts, materials and accessories.*
>
> *Article 13 –Aggravating circumstances*
>
> *d) the offences of supplying and offering to supply were committed having resort to means of large scale distribution, such as information systems, including the Internet."*[66]

Free speech does not protect false advertising. Indeed, it is not a foundational value of freedom of speech to protect harmful speech.

Further examples of specific restrictions in the Interest of *"human health protection"* are provided by the European Court of Justice (judgments of 2015 and 2016):

The *Neptune Distribution* case of 17 December 2015, in which the Court held:

"[…] *it must be held that the EU legislature were legitimately entitled to consider that limitations and restrictions, such as those at issue […], as regards the use of claims or indications referring to the low sodium content of natural mineral waters were appropriate and necessary to ensure the protection of human health in the European Union."*[67]

and

the *Philip Morris Brands* case of 4 May 2016 in which the Court ruled:

"[…] *it must be held that, in prohibiting the placing, on the labelling of unit packets and on the outside packaging, as well as on the tobacco product itself, of the elements and features referred to in Article 13(1) of Directive 2014/40, even when they include factually accurate information, the EU legislature*

25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services and Council Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products; […] of 6 July 1998 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products adopted within the framework of the internal market.

65 Unlawful Internet Gambling Enforcement Act of 2006, 31 USC 5361-5366. Available at: https://www.fdic.gov/news/news/financial/2010/fil10035a.pdf. [Accessed 30 September 2016].

66 Several initiatives are taken at different levels to enforce such restrictions. One such example is Operation Pangea which is coordinated by INTERPOL. More than 2,410 websites have been taken offline as a result of these activities. In the United States the FDA seized and shut down 1.677 fake pharmacy websites.

67 *Société Neptune Distribution v. Ministre de l'Économie et des Finances* [2015], Case No. C-157/14 (European Court of Justice, Fourth Chamber).

did not fail to strike a fair balance between the requirements of the protection of the freedom of expression and information and those of human health protection." [68]

We also find restrictions applying to whistle blowers (despite the enhanced protection in some countries of individuals who in the interest of public health, safety, security or public policy and transparency publicize information which for various reasons may be considered privileged or classified). [69]

A recent case from Luxembourg (29 June 2016) on bank secrecy (known as the "LuxLeaks-case") and the Snowden case serve as examples of such "prohibited speech."[70]

Specific speech restrictions require **explicit** legislative stipulations.

An example of this requirement is the decision 6 September 2016 of the *Cour de Cassation* in France[71] regarding exchange of information on the location of police officers controlling traffic regulations:

Whereas it appears from the judgment under appeal and the pleadings, that *"*[…] *a discussion group created on* […] *Facebook, called "the group that tells you where the police is in Aveyron",* [...] *gave the location of roadside checks, the prosecutor summoned some members of the group before the criminal court,* [...] *on the basis of Article R 413- 15 I and III of the Traffic Code, prohibiting the use of devices, instruments or products allowing to avoid the recording of traffic offenses,* [...]. *Since Article R. 413-15 I of the Traffic Code do not prohibit* ***provision of information*** *regarding the location of devices, instruments or systems used for the recording of offenses to traffic or regulation, but only prohibits the* ***possession****, transport and use of devices to detect the presence or disrupt the operation of devices, instruments and systems used for the recording of offenses to traffic regulations or allowing to avoid interception, the court of appeal justified its decision without breaching the invoked provision."* [the author's translation].

Specific speech regulation cannot be grounded in analogy.

---

68 *Philip Morris Brands SARL e.a. v. Secretary of State for Health* [2016], Case No. C-547/14 (European Court of Justice, Second Chamber).

69 In *Houchins v. KQED*, the Supreme Court rejected the principle that freedom of governmental information is implicit in First Amendment guarantees. In a plurality opinion, Justice Burger held that there was "(n)o First Amendment guarantee of a right of access to all sources of information within government control". Source: *Houchins v. KQED, Inc*. [1978], 438 U.S. 1, 98 S.CR. 2588 (Supreme Court of the United States).

70 *Deltour, Perrin, Halet v. Ministère Public* [2016]. Tribunal d'arrondissement du Luxembourg, douzième chambre. Available at: http://www.justice.public.lu/fr/actualites/2016/06/jugement-affaire-luxleaks/index.html. [Accessed 30 September 2016]. See also: Edward Snowden, against whom criminal charges have been filed. Finn, P.; Horwitz, S. (2013): "U.S. charges Snowden with espionage". Available at: https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html. [Accessed 30 September 2013]. Letter from the Attorney General of the United States to the Russian Minister of Justice (2013). Available at: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/26_07_13_attorney_general_letter_to_russian_justice_minister.pdf [Accessed 30 September 2016].
Another example is false alarm. False alarms involving for instance bomb threats have become increasingly frequent. In Paris 2 teenagers were arrested for such acts on 17 September 2016. The French penal code imposes severe penalties (art. 322-14: "*communication of false information with the intention to cause people to believe that a destruction posing a danger will be committed is punished by up to 2 years' imprisonment and 30 000 €"* [the author's translation]. Source ; Breteau, P. (2016) : "Que risquent les auteurs d'une fausse alerte terroriste ?", *Le Monde*. Available at: http://www.lemonde.fr/les-decodeurs/article/2016/09/19/que-risquent-les-auteurs-d-une-fausse-alerte-terroriste_4999873_4355770.html#kSbtxsGtc5VuuLot.99 [Accessed 27 September 2016].

71 *Parquet général près la cour d'appel de Montpellier v. Cindy A. et a.* [2016], 15-86412 (Cass. Crim.)

Free speech is subject to important restrictions as a consequence of cultural policy. Thus the "Proposal for a Directive of the European Parliament and of the Council" (25 May 2016) on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities mandates that:

"Member States shall ensure that providers of on-demand audiovisual media services under their jurisdiction secure at least a 20% share of European works in their catalogue and ensure prominence of these works."[72]

The European Commission supplements:

"[…] *The EU and its Member States are fully free to discriminate against foreign providers of audiovisual services* […] *The EU also wants… to stress the right of the parties to take measures necessary to achieve legitimate public policy objectives for promoting cultural diversity as laid down in the UNESCO Convention."*

Restrictions justified by child protection policy are especially firm:

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 25.10.2007) provides an example hereof.

The Convention outlaws offences related to child pornography (art. 20) including "*c) distributing or transmitting child pornography* […] *f) knowingly obtaining access, through information and communication technologies, to child pornography."*[73]

Content restrictions also apply to racism, glorification of genocide or crimes against humanity. An example hereof is the "Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems" (Strasbourg, 28. January 2013)[74] :

> *"Article 3 – Dissemination of racist and xenophobic material through computer systems*
>
> *1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*
>
> *Article 4 – Racist and xenophobic motivated threat* […]
>
> *threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, color, descent or national or ethnic origin, as well as religion, if*

---

72 The proposal has been updated on May 25, 2016. It is still a proposal, as discussions are ongoing within the Council or its preparatory bodies. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN; http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2016:287:FIN.

73 The same is the case for the Council of Europe (2001), Convention on Cybercrime, 23.XI.2011. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 27 September 2016].
"*Article 9 – Offences related to child pornography*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
C. *distributing or transmitting child pornography through a computer system;".*

74 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (2003), Council of Europe, Treaty No.189.

used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult […]

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

Article 6 – Denial, gross minimization, approval or justification of genocide or crimes against humanity

[…] *distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity* […]."[75]

Similar restrictions are found in the Convention on the Prevention and Punishment of the Crime of Genocide (1951), the International Convention on the Elimination of All Forms of Racial Discrimination (1965) and, although to a lesser extent, the Convention on the Elimination of All Forms of Discrimination against Women - CEDAW (1981).[76]

Hate Speech is a category where specific regulations remain subject to conflicting views and interpretations. For the purpose of regulating radicalizing content, legal containment of hate speech is however of prime importance due to the somewhat coinciding manifestations of these concepts.

The Human Rights Committee explains the concerns as follows:

"There is a pattern in international law which emphasizes the mutuality between freedom of expression and protection against hate speech. Recent documents such as the Human

[75] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008F0913 [Accessed 27 September 2016]. The text establishes that the following intentional conduct will be punishable in all EU Member States:
- Publicly inciting to violence or hatred, even by dissemination or distribution of tracts, pictures or other material, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.
- Publicly condoning, denying or grossly trivializing
- crimes of genocide, crimes against humanity and war crimes as defined in the Statute of the International Criminal Court (Articles 6, 7 and 8) directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin, and
- crimes defined by the Tribunal of Nuremberg (Article 6 of the Charter of the International Military Tribunal, London Agreement of 1945) directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.

[76] Restrictions aimed at eliminating violence against women are "encouraged" by the Council of Europe, Source: Council of Europe (2011), Convention on preventing and combating violence against women and domestic violence, Istanbul, 11.V.2011. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008482e [Accessed 27 September 2016]:
Article 17 –Participation of the private sector and the media
1. Parties shall encourage the private sector, the information and communication technology sector and the media, with due respect for freedom of expression and their independence, to participate in the elaboration and implementation of policies and to set guidelines and self-regulatory standards to prevent violence against women and to enhance respect for their dignity.

Rights Committee General Comment and the Rabat Plan of Action have repeatedly done this. The latter gives an overview:

Under international human rights standards, which are to guide legislation at the national level, expression labelled as "hate speech" can be restricted under articles 18 and 19 of the ICCPR on different grounds, including respect for the rights of others, public order, or even sometimes national security. States are also obliged to "prohibit" expression that amounts to "incitement" to discrimination, hostility or violence (under article 20.2 of the ICCPR and, under some different conditions, also under article 4 of the ICERD"[77]

In Europe the Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law includes a definition and prohibition of hate speech:

"Certain forms of conduct as outlined below, are punishable as criminal offences:

- *public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, color, descent, religion or belief, or national or ethnic origin;*
- *publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes as defined in the Statute of the International Criminal Court (Articles 6, 7 and 8) and crimes defined in Article 6 of the Charter of the International Military Tribunal, when the conduct is carried out in a manner likely to incite violence or hatred against such a group or a member of such a group."*

In addition to the limits to freedom of speech imposed by the above treaties and directives we find restrictions covering: defamation, glorification of suicide and euthanasia, cyberbullying, harassment, negationism, infringement of the presumption of innocence in penal proceedings (this often includes an obligation not to disclose the identity of civil parties in penal cases), disclosure of privileged information by doctors, lawyers, priests and civil servants.[78]

---

[77] Gagliardone, I.; Gal, D.; Alves, T.; Martinez, G. (2015), *Countering Online Hate Speech*, UNESCO Publishing. Available at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf [Accessed 27 September 2016].

[78] In some countries re-publishing of such information may be a penal offence. The ICCPR explicitly reaffirms the principle of presumption of innocence as a human right (Art. 14) and stipulated that "*the press and public may be excluded from all or part of a trial for reasons of morals, public order, national security in a democratic society or when the internet of the private lies of the parties so requires […]"*
In France (and a number of other countries) there are speech restrictions covering "negationism" (loi Gayssot) concerning the holocaust and genocide. The aforementioned "loi Gayssot" was deemed compatible with the International Covenant on Civil and Political Rights art. 19 by the United Nations Commission of Human Rights in the case Robert Faurisson against France (19 July 1995). In the words of Justice Prafullachandra Bhagwati: *"[…] I firmly believe that in a free democratic society, freedom of speech and expression is one of the most prized freedoms which must be defended and upheld at any cost and this should be particularly so in the land of Voltaire. It is indeed unfortunate that in the world of today, when science and technology have advanced the frontiers of knowledge and mankind is beginning to realize that human happiness can be realized only through inter-dependence and cooperation, the threshold of tolerance should be going down. It is high time man should realize his spiritual dimension and replace bitterness and hatred by love and compassion, tolerance and forgiveness."*

Protection of privacy also establishes boundaries as stipulated in Art. 7 and 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01)[79] and in many countries with the notable exception of the United States which applies a *sui generis* approach to privacy protection.

We find specific restrictions to freedom of speech on media already from the time of the League of Nations.

The International Convention Concerning the Use of Broadcasting in the Cause of Peace from 1936 prohibits broadcasting of propaganda and "*false news*" (Art. 3 and Art. 4).

According to Art. 1 of the Convention the signatory States must proscribe any broadcast originating within their jurisdiction if it is "*of such a character as to incite the population of any territory to acts incompatible with the internal order or the security of a territory."*

Art. 2 prohibits content *"inciting to war against another high contracting party."*[80]

Free speech is also restricted by certain trade agreements for instance the **"**Transatlantic Trade and Investment Partnership (TTIP)" (which will most probably however not be adopted, but for reasons unrelated to the subject covered by this Report). The European Union Position Paper (20 March 2015) states that the TTIP should include:

> *"a. Compliance with international IP treaties:*
>
> *Rome Convention; Berne Convention; WIPO Copyright Treaty; WIPO Performances and Phonograms Treaty; WIPO Beijing Treaty and Marrakesh Treaty (if ratified in the meantime); Trademark Law Treaty; Singapore Treaty on the Law of Trademarks; Protocol Relating to the Madrid Agreement; The Hague Agreement on Designs* […] *and the so-called "Geographical Indications."*

All of the above treaties and geographical indications impose speech restrictions by enforcing intellectual property right protection. Restrictions of free speech in the field of intellectual property rights is well established and violations carry substantial civil and penal sanctions.[81]

The recent judgment (8 September 2016) in the case *GS Media v. Sanoma et al*. from the European Court of Justice on hyperlinks is an example of online enforcement of intellectual property rights:

---

79 Art. 7 refers to respect for private and family life and Art. 8 refers to protection of personal data; (Art. 11 protects freedom of expression and information); Source: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

80 The International Convention Concerning the Use of Broadcasting in the Cause of Peace (1936). Available at: http://treaties.fco.gov.uk/docs/fullnames/pdf/1938/TS0029%20(1938)%20CMD-5714%201936%2023%20SEP,%20GENEVA%3B%20INTL%20CONVENTION%20CONCERNING%20USE%20OF%20BROADCASTING%20IN%20CAUSE%20OF%20PEACE.pdf). [Accessed 30 September 2016].

81 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001L0029 [Accessed 27 September 2016]:
"(16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks […]"
Article 7
Obligations concerning rights-management information
Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:
[…]
If such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC."

> *"Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society must be interpreted as meaning that, in order to establish whether the fact of posting, on a website, hyperlinks to protected works, which are freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public' within the meaning of that provision, it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature."*[82]

An example of specific restrictions in the shape of "forced speech" is the Audio Visual Media Service Directive (2010/13 of 10 March 2010) of the European Union which imposes an obligation on sponsored "Audio Visual Media Services" to ensure that *"[…] viewers shall be clearly informed of the existence of a sponsorship agreement"* (Art. 10, 1 (c)).[83]

The combination of the general exclusion of free speech protection covered in section 3.a. based on the Abuse of Rights and Duty and Obligations Theories (or balancing act) and the specific restrictions developed in this section 3.c support the conclusion that prohibiting or regulating "radicalizing content" as tentatively defined above will not per se violate freedom of speech protection.[84]

Section 4: Online Law Enforcement and Liability

We have seen above in Section 3.b that the protection of human rights in the online and offline world are aligned.

The appropriate legal mechanisms ensuring the efficient protection of these rights online - and the enforcement of their symmetrical obligations must however be determined. Such determination is the subject of this Section 4.

Prior to the analysis of enforcement and the identification of entities that may be held liable for online content we need to address the following question:

---

82 *GS Media BV v. Sanoma Media Netherlands BV and Others* [2016], Case C-160/15, Court of Justice of the European Union, Second Chamber.

83 The Directive also contains prohibitions on product placement of tobacco and specific medicinal products (Art. 11,4 (a). Advertisements for "alcoholic beverages" are subject to strict regulations (Art. 22).

84 Monroe E. Price (2009): "Satellite Transponders and Free Expression". (p. 35). Available at http://www.cardozoaelj.com/wp-content/uploads/Journal%20Issues/Volume%2027/Issue%201/Price.pdf [Accessed 30 September 2016]: *"Terrorism is the trope that has succeeded in breaking the rule of flows of information where cultural exception, fear of pornography, sweeping concerns about cultural imperialism, and fears for national identity failed. Terrorism has brought the deacons of free expression to the table of regulation, even of clumsy intervention."*

4.a. Can/Should the Internet be Regulated?

A debate as to the legal nature of the Internet or Cyberspace and its "regulability" emerged already in the 90s and led to different theories like Universalism, Exceptionalism, Libertarianism, Territorialism and the Bordered Internet.[85]

At the outset many authors claimed that Cyberspace was beyond regulation both at State and international level. The debate between the extremes claiming on the one hand that the Internet neither could nor should be regulated and on the other hand those that maintained that there is no legally relevant difference between offline and online jurisdiction seems to have been overtaken by events and replaced by a *de facto* "Bordered Internet" approach based on the Westphalien Sovereign State Concept according to which each State retains jurisdiction (legislative, adjudicatory and enforcement prerogatives) within its own territorial boundaries.

"*To assert the supremacy of law over technological determinism"* seems to be the current thinking.[86]

We shall see in Section 4.b. how the issue of Internet jurisdiction is however facing increasing challenges.

In his book "*World Order*", Dr. Henry Kissinger describes the problem inherent in the theories that confer upon the Internet a dimension elevating it beyond legislative authority in the following terms:

> *"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* […]

---

[85] Dyson, E.; Gilder, G.; Keyworth, G.; Toffler, A. (1994): "Cyberlaw and the American Dream: A Magna Carta for the Knowledge Age". Progress & Freedom Foundation.
See also: Spinello, R.A.; Tavani H.T. (2002) *Readings in Cyberethics*. Boston, United States. Jones and Bartlett Publishers.

[86] Watt, H.M. (2003): "Yahoo! Cyber-Collision of Cultures: Who Regulates?". University of Michigan Law School. Referred in: Segura-Serrano, A. (2006): "Internet Regulation and the Role of International Law", Max Planck UNYB, p. 206. Available at: http://www.mpil.de/files/pdf3/06_antoniov1.pdf [Accessed 30 September 2016].

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?"[87]

Due to the very nature of the Internet, jurisdiction will tend to become increasingly extraterritorial unless global standards are agreed which will replace veritable chaos by some measure of law.

The Internet is *de facto* subject to both international and State law. Given the differences in definitions, cultural traditions and regulatory approaches to "radicalizing content" clashes over jurisdiction are bound to increase as a consequence of the growing impact of online radicalization.

4.b. Jurisdiction and Extraterritoriality

In this section we shall analyze specific problems and suggested solutions to jurisdiction[88] and extraterritoriality issues posed by the Internet.

As far as international jurisdiction is concerned, the Internet raises significant and complicated problems due to its very nature as a universal medium.

Indeed "Universal Jurisdiction" has been proposed as the appropriate "regulator" of the Internet.[89]

The question of jurisdiction on the Internet and extraterritoriality in terms of legislative/adjudicatory authority and enforcement has given rise to considerable debate in jurisprudence and a substantial number of important judicial decisions.

When considering regulatory conflicts on the Internet, *"there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it. Analysis of such a claim has shown that I reverse the proper relationship between law and technology. Technology being purely man made, and thus subject to ideological choice, should not dictate the way in which law manages conflicting interests arising through its medium."*[90]

---

87 Kissinger, H. (2014), *World Order: Reflections on the Character of Nations and the Course of History*, Penguin Press.

88 Failure to establish jurisdiction is exemplified by the case *Bankovic and Others v. Belgium and 16 Other States* [2001], Decision as to the admissibility of Application No. 52207/99, European Court of Human Rights, Grand Chamber, 12 December 2001.
This application was brought by six people living in Belgrade (Serbia) against 17 NATO Member States which were also Contracting States to the European Convention on Human Rights. The applicants complained in particular about the bombing by NATO, as part of its campaign of air strikes against during the Kosovo conflict, of the Serbian Radio-Television headquarters in Belgrade which caused damage to the building and several deaths.
The Court was satisfied that, while international law did not exclude a State's exercise of jurisdiction extra-territorially, jurisdiction was, as a general rule, defined and limited by the sovereign territorial rights of the other relevant States. It found that other bases of jurisdiction were exceptional and required special justification in the particular circumstances of each case. The Court further observed that the Convention was a multi-lateral treaty operating in an essentially regional context and notably in the legal space of the Contracting States. The then Federal Republic of Yugoslavia clearly did not fall within that legal space. The Court was therefore not persuaded that there was any jurisdictional link between the victims and the respondent States and declared the application inadmissible.

89 The term "Universal Jurisdiction" as used in this context is not to be confused with the jurisdiction created for the prosecution of certain crimes against humanity for instance genocide.

90 Segura-Serrano, A. (2006): "Internet Regulation and the Role of International Law", Max Planck UNYB, p. 206. Available at: http://www.mpil.de/files/pdf3/06_antoniov1.pdf [Accessed 30 September 2016].

Clashes between values entertained by different cultures and traditions raise some of the most difficult regulatory challenges facing the enforcement of the rule of law on the Internet. Unilateral State intervention will lead to increased conflict and potentially to a carving up of the Internet thereby negating its contribution to universalism.
This "battle of online jurisdiction" is far from resolved. Its origins may be traced back to the *CompuServe* case (*Felix Somm*) in Germany (15 July 1998) which held that access to content conferred jurisdiction on the local Court in Munich (See *infra* on the French Yahoo cases 2000-2004) and that CompuServe Inc was liable for the acts of CompuServe GmbH and its General Manager.[91]

A second much later case (October 2005) highlights the complexity involved in extraterritorial enforcement. The plaintiff, the French company Louis Feraud, sought to enforce a judgement obtained before the Courts in France awarding damages for design violations against a company based in New York.[92]

The New York court rejected enforcement arguing that the design violations were "committed" (published) in the United States where they enjoyed protection under the First Amendment.

The court's view amounted to an application of the so-called *"subjective territorial principle"* according to which a State's authority under International Law is restricted to regulation of acts originating within its territory (the French court had applied an effects theory as opposed to "origination").

If this approach was followed globally, the result would be that content be governed exclusively by the laws of the "Country of Origin". Actually this is the rule we find in the e-Commerce Directive and the Audiovisual Media Services Directive in the European Union,[93] but its accommodation hinges upon the fact that as a result of harmonization of the substantive laws in the European Union, on the subject matters covered by those directives it does not impact on the final legal assessment whether "domicile law", "effects law" or "country of origin law" applies.

Another approach is that of **accessibility** according to which the country from whose territory a user may access the content in question has jurisdiction. This is the principle applied by the Court in Paris and to a certain extent in the United States in the *Yahoo* cases from 2000-2004[94] as well as the *CompuServe* case in Germany (*supra* p. 55).

The problem with this position may be summarized in the words of the U.S Court of Appeal, Fourth Circuit in the case *Als Scan, Inc. v. Digital Service Consultants, Inc*. (14 June 2002):

> *"If we were to conclude as a general principle that a person's act of placing information on the Internet subjects that person to personal jurisdiction in each State in which the*

---

91 *The People v. Felix Somm* [1999], File no. 20 Ns 465 Js 173158/95 (Munich Regional Court)

92 *Sarl Louis Feraud Intern. v. Viewfinder Inc.* [2005], 406 F. Supp. 2d 274 (S.D.N.Y.). Available at: https://www.courtlistener.com/opinion/2323660/sarl-louis-feraud-intern-v-viewfinder-inc/ [Accessed 30 September 2016].

93 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031 [Accessed 27 September 2016].

94 *Ligue contre le racisme et l'antisémitisme and Union des étudiants juifs de France v. Yahoo! Inc. and Société Yahoo! France* [2000], 00/0538 (Tribunal de Grande Instance de Paris). See also: *Ligue contre le racisme et l'antisémitisme and Union des étudiants juifs de France v. Yahoo! Inc. and Société Yahoo! France* [2004], 01-17424 (Ct. App. 9th Cir.). Available at: http://openjurist.org/379/f3d/1120/yahoo-inc-v-la-ligue-contre-le-racisme-et-lantisemitisme. [Accessed 30 September 2016].

information is accessed, then the defense of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist."[95]

In the case *PSINET, Inc. v. Chapman*, the Fourth Circuit put the matter in these terms:

"The content of the Internet is analogous to the content of the night sky. One state simply cannot block a constellation from the view of its own citizens without blocking or affecting the view of the citizens of other states. Unlike sexually explicit materials disseminated in brick and mortar space, electronic materials are not distributed piecemeal. The Internet uniformly and simultaneously distributes its content worldwide."[96]

A different approach is illustrated by another leading case on Internet jurisdiction. This approach is based on **"focused"** or **"targeted" accessibility** if the content is targeted at an audience in a specific jurisdiction the author, the publisher, the editor or the ISP must accept to comply with the laws of that jurisdiction.

Gutnick v. Dow Jones (10 December 2002)[97] is an example of such "focused accessibility": A website based in the United States had sold subscriptions to Australian users. The High Court of Australia concluded that this established a territorial attachment in favor of Australian jurisdiction.

A more recent example of jurisdiction based on a targeted approach which allows the "target country" to regulate the content "received" on its territory (and not only block it, but also impose a takedown order on the ISP through whose infrastructure the content is disseminated) is the *Rilley v. MoneyMutual* case (24 August 2016)[98]:

---

95 *Als Scan, Inc. v. Digital Service Consultants, Inc.* [2002], 01-1812 (Ct App. 4th Cir.). Available at: http://caselaw.findlaw.com/us-4th-circuit/1372742.html. [Accessed 30 September 2016].

96 *PSINET Incorporated v. Chapman III* [2004], Case No. 01-2352 (United States Court of Appeals, Fourth Circuit).
King, K. (2011), "Personal jurisdiction, Internet commerce, and privacy: The pervasive legal consequences of modern geolocation technologies", *ALB. L.J. SCI. & TECH*, Volume 21.1, p. 61.
The European Court of Human Rights develops the theory of "origin" further in terms of violations of human rights in other countries as a consequence of "origins" within its territorial jurisdiction:
Ben El Mahi and Others v. Denmark [2006], Application No. 5853/06 (European Court of Human Rights, Fifth Section).
The applicants were a Moroccan national living in Morocco and two Moroccan associations operating in that country. In September 2005, a privately owned Danish newspaper published twelve cartoon caricatures of Prophet Muhammad, the most controversial of which showed him with a bomb in his turban. Several Muslim organisations in Denmark subsequently complained to the Danish police that the cartoons invoked blasphemy and religious insult. Following the prosecutor's refusal to initiate criminal proceedings against the newspaper, the applicants complained that Denmark had permitted that publication. The Court recalled in particular that only *"in exceptional circumstances may the acts of Contracting States performed outside their territory or which produce effects there amount to an exercise by them of their jurisdiction within the meaning of Article 1 (obligation to respect human rights) of the Convention. Accountability in such situations stems from the fact that Article 1 cannot be interpreted so as to allow a State Party to perpetrate violations of the Convention on the territory of another State which it would not be permitted to perpetrate on its own territory."*

97 *Gutnick v. Dow Jones* [2002] HCA 56. Available at: http://www.5rb.com/wp-content/uploads/2013/10/Gutnick-v-Dow-Jones-HCA-10-Dec-2002.pdf [Accessed 30 September 2016].

98 *Scott Rilley v. MoneyMutual* [2016], Case No. A14-1307 (Supreme Court of Minnesota).
A consumer based in Minnesota sought personal jurisdiction over the company MoneyMutual in that state and argued that MoneyMutual had bought the keyword "payday loans Minnesota". The Minnesota Supreme Court judged that:
"[…] *if MoneyMutual paid for AdWords directed at other states, such as "payday loan New York," it would not diminish the conclusion that MoneyMutual targeted Minnesota with its AdWords campaign. Rather, it would tend to establish contacts with both Minnesota and New York.*
[…] *MoneyMutual's use of Google AdWords advertising that was specifically designed to target Minnesota residents is a relevant contact with the Minnesota forum* […]"
As far as the United States is concerned the challenge has been twofold: defining the perimeter of jurisdiction domestically and internationally and delimitating "extraterritorial effects" within the United States as such (by virtue principally of the so-called

AdWords containing country specific keywords expose the user to personal jurisdiction in each of the countries "targeted" by those keywords.[99]

In the *Cartier International AG, Montblanc Simplo, Richemont etc.* case (13 November 2014) the judge in the London Court of Appeals summarized as follows:

> *"I turn then to consider* (the) *second submission, namely that there was no evidence* […] *that the services of each of the ISPs were actually used to transmit any offers or advertisements from each of the target websites to any actual or potential customers in the United Kingdom.*
>
> *I reject this submission. Each of the target websites was directed to consumers in the United Kingdom and the operators of those sites were advertising and offering for sale counterfeits of the goods of one of the named claimants.* […] *If and in so far as the target websites had not yet been accessed by consumers in the United Kingdom using the services of each of the ISPs there was plainly a real risk that they would be in the future. The judge was entitled to make an order to try to prevent this happening* […]*"*

Some countries have enacted **specific jurisdiction laws** typically limiting the effects of foreign laws and judgements on their territory. This is the case for the United States where the "Free Speech Protection Act (2009)" allows "*any U.S. person against whom a lawsuit for defamation is brought in a foreign country that does not provide the full extent of free speech protection awarded by the First Amendment to bring an action in a U.S. district court against the plaintiff in the foreign suit, if the speech at issue in the foreign lawsuit does not constitute defamation under U.S. law."*[100]

In the European Union a set of specific procedural rules apply to Internet jurisdiction with regard to *"attacks against information systems"* as stipulated in Art. 12 on Jurisdiction of the Directive 2013/40/EU (August 12th 2013):

> *"3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where:*
> *(a) the offender has his or her habitual residence in its territory; or*

"Dormant Commerce Clause" in Amendment 14 which prohibits enacting laws in one state to the extent they could have a discriminatory effect on another).

[99] Goldman, E. (2016): "AdWords Buys Using Geographic Terms Support Personal Jurisdiction–Rilley v. MoneyMutual", *Technology & Marketing Law Blog*. Available at: http://blog.ericgoldman.org/archives/2016/08/adwords-buys-using-geographic-terms-supports-personal-jurisdiction-rilley-v-moneymutual.htm [Accessed 27 September 2016].

[100] *The United States respects the sovereign right of other countries to enact their own laws regarding speech, and seeks only to protect the First Amendment rights of Americans in connection with speech that occurs, in whole or in part, in the United States. (Free Speech Protection Act of 2009, 111th Congress, 1st Session. H.R. 1304)*
In addition, a number of states have passed so-called "Anti-Slapp Acts" *i.e.* laws that restrict enforcement of foreign judgements to the extent they are deemed to infringe the First Amendment. An example is the "Code of Civil Procedure" of California: "*(a) The Legislature finds and declares that there has been a disturbing increase in lawsuits brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances. The Legislature finds and declares that it is in the public interest to encourage continued participation in matters of public significance, and that this participation should not be chilled through abuse of the judicial process* […]. *(b) (1) A cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech Under the United States Constitution or the California Constitution in connection with a public issue shall be subject to a special motion to strike, Unless the court determines that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim.* […]*."*

(b) the offence is committed for the benefit of a legal person established in its territory."

In the European Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (28 November 2008) we find the following criteria:

"Article 9-– Jurisdiction […]

2. When establishing jurisdiction […] *each Member State shall take the necessary measures to ensure that its jurisdiction extends to cases where the conduct is committed through an information system and:*

(a) the offender commits the conduct when physically present in its territory, whether or not the conduct involves material hosted on an information system in its territory; […]*"*

A further jurisdictional criterion was developed in the "Right to be Forgotten" judgment of 13 May 2014 (Court of Justice of the European Union).[101] The Court stressed the importance of local presence; the theory being that a Member State has jurisdiction over an ISP based in a different country (the particular case dealt with jurisdiction over Google Inc. for content disseminated in the European Union), to the extent that the ISP sets up or controls a business entity in that Member State (typically through a subsidiary, branch or rep. office) and said local presence may be deemed **"inextricably linked"** to the "parent".

The criterion of the "inextricably linked" relationship was also used by the French Court in its decision of 16 September 2014. In that particular case, the dereferencing obligations were enforced by imposing daily penalties against the local subsidiary (Google France).[102]

The most recent development in the European Union on Internet jurisdiction is found in the Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (27 April 2016):[103]

"(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. […]
(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the

101 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González* [2014], Case C-131/12 (Court of Justice of the European Union, Grand Chamber).

102 Légipresse (2014) : "Google condamné en référé à déréférencer des liens renvoyant vers des articles diffamatoires", N°320, pp. 522-523.

103 Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016.

controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

the monitoring of their behavior as far as their behavior takes place within the Union."

As it will be seen the above Regulation consecrates a "focused accessibility" approach while at the same time extending protection and jurisdiction to persons "in the Union" irrespective of the geographic location of the ISP in question.

In addition to current Internet Jurisdiction Law (which approximates a mosaic of different and competing approaches rather than an agreed set of rules) the possibilities offered by **geolocalization capability** on resolving jurisdictional conflict and delimitation of territorial scope of court orders have not been fully developed.

Geolocalization technology may secure both prescriptive, adjudicatory and enforcement jurisdiction with regard to content regulation. Such laws will typically not violate International Jurisdiction Law.

It may be argued that in case an ISP decides not to implement geolocalization features enabling it to accommodate content disseminated through its services to country based content regulation, it knowingly exposes itself to coexistent and often contradictory substantive laws in all jurisdictions where the content in question may be accessed.[104]

According to this theory, country jurisdiction and even extraterritorial enforcement over "radicalizing content" apply to the host and other ISPs which "expose themselves" to jurisdiction by not filtering on

[104] King, K. (2011), "Personal jurisdiction, Internet commerce, and privacy: The pervasive legal consequences of modern geolocation technologies", *ALB. L.J. SCI. & TECH*, Volume 21.1.

the basis of geolocalization (this theory may however run afoul of the Digital Agenda of the European Union which limits the use of geolocalization and "comportamentalization").[105]

As it will be seen competing theories of jurisdiction and extraterritorial reach directly impact content regulation.

In the interest of legal certainty as well as the efficacy of a policy directed at the suppression of radicalizing content it is imperative that a treaty solution be adopted.

UNESCO is well placed to initiate this process.

Finally, the question of ISP liability will be dealt with separately under Section 4. d. *infra*. Jurisdiction may however be taken to imply liability.

4.c. Internet Specific Law/Media Law

In addition to the above questions on the regulability of Cyperspace, the applicability of Human Rights and obligations to the Internet, on jurisdiction, enforcement and the exercise of sovereign State Power in conflict with other States, one of the classic questions dealt with in jurisprudence has been the appropriateness of applying Media Law ("Broadcasting Law") to the Internet.

This question attracts particular interest due to the content liability regime developed over the years in the field of Media Law. Radicalizing content would most probably in the vast majority of cases engage liability under Media Law.[106]

The debate is still ongoing and actually also impacts on jurisdiction.

The argument against applying Media Law to the Internet may be summarized as follows:

According to the United Nations' Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (16 May 2011):

> *"Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as an interactive medium. Indeed, with the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information.*
>
> *27. In addition, the Special Rapporteur emphasizes that due to the unique characteristics of the Internet, regulations or restrictions which may be deemed legitimate and proportionate for traditional media are often not so with regard to the Internet."*

105 Brussels, 25.5.2016 COM (2016) 289 final 2016/0152 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC.

106 Derieux, E. (2015), *Droit des Médias, Droit français, européen et* international, 7th ed., LGDJ, pp. 397-597.

And in the words of the Supreme Court of the United States:

> *"The special factors recognized in some of the Court's cases as justifying regulation of the broadcast media-the history of extensive government regulation of broadcasting*, […] *and its "invasive" nature,* […] *are not present in cyberspace. Thus, these cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to the Internet."*[107]

One of the principles of Broadcasting Law is emphasized in The International Convention Concerning the Use of Broadcasting in the Cause of Peace from 1936, Art. 1 which provides that: "*The High Contracting Parties mutually undertake to prohibit and, if occasion arises, to stop without delay the broadcasting within their respective territories of any transmission which to the detriment of good international understanding is of such a character as to incite the population of any territory to acts incompatible with the internal order or the security of a territory of a High Contracting Party."*[108]

The United Nations Committee on the Peaceful Uses of Outer Space ("COPUOS") established in 1959 argued for *"a prohibition on broadcasts beamed from satellites by one State to others without the explicit prior consent of the Government concerned through bilateral or multilateral agreements."*[109]

The United Nations General Assembly Resolution 37/92 on the Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting did not finally implement the principle of "prior consent" from the receiving countries, but it stated that *"States should bear international responsibility for activities in the field of international direct television broadcasting by satellite carried out by them or under their jurisdiction."* This was consistent with the principle adopted by the United Nations and UNESCO whereby the country from whose territory the broadcast ("content") originated was responsible for monitoring and policing that such "content" did not *"[…] incite the population […]to acts incompatible with internal order or the security of the territory of the receiving State."*[110]

---

107 *Reno v. American Civil Liberties Union* [1997], 521 U.S. 844 (Supreme Court of the United States).

108 The International Convention Concerning the Use of Broadcasting in the Cause of Peace (1936). Available at: http://treaties.fco.gov.uk/docs/fullnames/pdf/1938/TS0029%20(1938)%20CMD-5714%201936%2023%20SEP,%20GENEVA%3B%20INTL%20CONVENTION%20CONCERNING%20USE%20OF%20BROADCASTING%20IN%20CAUSE%20OF%20PEACE.pdf. [Accessed 30 September 2016].

109 Price, M. E. (2009): "Satellite Transponders and Free Expression" (p. 9) Available at http://www.cardozoaelj.com/wp-content/uploads/Journal%20Issues/Volume%2027/Issue%201/Price.pdf [Accessed 30 September 2016];

110 *"[…]to incite the population [...] to acts incompatible with the internal order or the security of the territory of the receiving State* (Article 1 of The International Convention Concerning the Use of Broadcasting in the Cause of Peace from 1936).

In the European Union satellite broadcasting has always been governed by the principle that broadcasts originating in the European Union are subject to regulation by the Member State *"of origin*".[111]

The analogous principle is embodied in the e-Commerce and the Audiovisual Media Services Directives[112]:

"Art. 2.1. Each Member State shall ensure that all audiovisual media services transmitted by media service providers under its jurisdiction comply with the rules of the system of law applicable to audiovisual media services intended for the public in that Member State."[113]

The importance of the application of Media Law is however not restricted to such country of origin responsibility, but includes the prescription of a general accountability doctrine covering "publishers".

Media laws in most countries contain strict liability rules on content. The dynamics of the Internet as it has converged with classic media functionality increasingly causes the principles of content liability as developed under Media Law to be advocated in litigation around the world and stresses the importance of defining "the editor" and "the publisher" of content online.

In a recent Australian case (*Duffy v Google Inc.* [2015] SASC 170) this question (who is the publisher on the Internet?) was submitted to the Supreme Court of South Australia.[114] In its judgement of 27 October 2015 Justice Blue concluded that: "*Google published to a substantial number of persons searching for* […] *imputations defamatory of* […]." A search engine may thus be liable as a "secondary publisher". The specific case included the autocomplete function. Failure to delete defamatory content after notice was qualified as a "*direct result of human action or inaction*" even though the autocomplete function and search algorithm were machine generated. The same logic applies to snippets and hyperlinks.

Furthermore, Media Law includes a range of jurisdiction and applicable law provisions which are not only of general importance to Internet regulation, but also to that of fighting online radicalization.

From a common sense and value standpoint there is some difficulty in not applying some of the basic concepts in "conventional" Media Law to the Internet (with the necessary adaptations).[115]

---

111 Price, M. E. (2010): "Orbiting Hate? Satellite Transponders and Free Expression", *Derecho Comparado de la Informacion*, p. 164.

112 Article 19 (2013): "Defending freedom of expression and information: Internet intermediaries: Dilemma of Liability".

113 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (Directive on electronic commerce) and Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 (Audiovisual Media Services Directive).

114 Fewster, S. (2016): "Dr Janice Duffy preparing second Google defamation claim, less than a year after $115,000 victory", *The Advertiser*. Available at*:* http://www.adelaidenow.com.au/news/south-australia/dr-janice-duffy-preparing-second-google-defamation-claim-less-than-a-year-after-115000-victory/news-story/bfaec391c4b7c02b1676b90a2e860658 [Accessed 27 September 2016] and http://www.abc.net.au/news/2015-12-23/google-ordered-to-pay-researcher-more-than-$100k-for-defamation/7051450 [Accessed 27 September 2016]

115 As we have seen, the arguments against applying Media Law are not only that licensing is no longer necessary (no scarcity), but also that the Internet is highly interactive and decentralized and that a substantial portion - possibly the major portion - is user generated. The arguments do not relate to values.

It is troubling that dissemination of radicalizing content should not give rise to liability on the Internet while the opposite is the case if the same content were published in a newspaper or on the radio/TV.[116]

Our analysis on the applicability of Media Law to the Internet brings us to the key issue of ISP liability based on Internet specific principles in recognition of the inherent difficulties of direct transposition of the liability structure of Media Law to the Internet.

Traditionally companies like Google, Twitter, Facebook etc. are viewed as *"*mere conduits" of content, hence privileged under the Safe Harbor Rules (which exclude accountability for content) as codified by the Communications Decency Act of the United States (1996)[117], the e-Commerce Directive[118] in the European Union as well as a number of national laws.
These Safe Harbor Rules largely came about as a consequence of the dilemma illustrated by the following cases in the United States: *Stratton, Oakmont v. Prodigy Services* (1995) and *Cubby v. CompuServe* (1991). In the *Prodigy* case the court ruled that Prodigy's screening of content caused it to be treated as an editor or a publisher thereby incurring Media Law liability.[119]

In the *CompuServe* case[120] the court ruled that even if the ISP only performed the services of a "distributor" with no editing function it could be liable simply for making the content available.[121]

As a consequence, ISPs would expose themselves to liability potentially just for "distributing" content and most assuredly if they engaged in any monitoring or editing activity.

---

116 "Countering Online Radicalization: A Strategy for Action" published by the International Centre for the Study of Radicalization and Political Violence (ICSR) (2009).

117 The Communications Decency Act enacted by the U.S. Congress on 1 February 1996 reads at Section 203 "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*."

118 Directive 2000/31 on electronic commerce (June 8th 2000):
"(40) […]*; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities;* […].
(43) A service provider can benefit from the exemptions for 'mere conduit' and for 'caching' when he is in no way involved with the information transmitted. […].
(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be Undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level;
(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities. […].
Article 14 - Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. […]"

119 *Stratton Oakmont, Inc. v. Prodigy Services Co.* [1995], WL 323710 (N.Y. Sup. Ct.).

120 *Cubby, Inc. v. CompuServe Inc*. [1991], 776 F.Supp. 135 (S.D.N.Y.).

121 Sableman, M., Thomson Coburn LLP (2013): "ISPs and content liability: The original Internet law twist". Available at: http://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2013-07-09/isps-and-content-liability-the-original-internet-law-twist [Accessed 27 September 2016].

This is one of the reasons why Section 230 C of the Communications Decency Act not only introduced a Safe Harbor Provision but also immunity for "Good Samaritan" attempts to filter content.[122]

The principle of content immunity has been credited for its substantial contribution to the growth and penetration of the Internet. Indeed, as we have seen, it replaced a regime of quasi-Media Law application with its inherent liability standard by a regime of impunity.
Without challenging the principle of content immunity as such we must however raise the question of ISP accountability in certain specific areas and in particular that of radicalizing content given its lethal consequences and the important gatekeeper function already performed by ISPs.

Given that freedom of speech is a human right and must co-exist with other human rights under International Law the question must be raised whether ISPs are subject to human rights obligations and liabilities under International law and to what extent Safe Harbor Rules should accommodate violations of such human rights.

The following additional questions must also be raised: To what extent do existing laws and regulations impose obligations on private enterprises to perform duties of a law enforcement or quasi-law enforcement nature and to what extent may such private sector entities encounter liability (penal and/or civil) for non-compliance with such duties? The answers to these questions are essential to the effectiveness of a ban on radicalizing content given the critical role of ISPs in content dissemination.

This brings us to the following section 4.d. on Private Sector Enforcement and Liability.

4.d. Private Sector Enforcement and Liability

[122] Below follow leading cases pursuant to the introduction in 1996 of CDA Section 230 C:

- *Federal Trade Commission v. LeadClick Media,* [2016] WL 5338081 (2d Cir. Sept. 23, 2016)

This suit deals with a company selling weight loss products, and its alleged violation of the FTCA due to it coordinating with affiliates to promote its products, when some of those affiliates used fake "news" sites for promotional purposes. The court found that LeadClick was not a provider of an Interactive Computer Service under Section 230 because its use of affiliates for advertising did not benefit customers and was not the type of service contemplated by Congress when it enacted Section 230. The court also found that LeadClick "developed" the content on the fake news sites because it chose affiliates who created such sites and purchased ads on the sites.

- *Enigma Software Grp. USA, LLC v. Bleeping Computer LLC,* [2016] U.S. Dist. LEXIS 89160 (S.D.N.Y. July 8, 2016)

This case dealt with a plaintiff suing an online message board for the contents of posts authored by one of the message board's unpaid moderators. The court found that the moderator was an agent of the message board because he had defined duties and authority and was described as part of the message board's "staff."

- *Barrett v. Rosenthal* [2006], 146 P.3d 510 (Cal. S.C.).

It is a 2006 California Supreme Court case concerning online defamation. The case resolved a defamation claim brought by Stephen Barrett, Terry Polevoy, and attorney Christopher Grell against Ilena Rosenthal and several others. Barrett and others alleged that the defendants had republished libelous information about them on the Internet.
The California Supreme Court interpreted Section 230 as providing immunity to an individual Internet "user" who is not a provider […] the originator of the content […].

- *Barnes v. Yahoo!, Inc*. [2005], 570 F. 3d 1096 (D. Or.).

It is a United States Court of Appeals for the Ninth Circuit case in which the Ninth Circuit held that Section 230 ruled that Yahoo!, Inc., as an Internet service provider cannot be held responsible for failure to remove objectionable content posted to their website by a third party.
The court even stated that Barnes' argument that Yahoo! did not keep its promise of removing the defamatory content online did not dismiss the immunity provided to Internet service providers by Section 230 C of the CDA.

Given the accelerating concentration of information and economic power wielded by some private sector entities today, the question of their obligations under International Human Rights Law is increasingly critical.

Over the years several proposals have been formulated extending human rights obligations to private entities.

Among such initiatives is the Global Online Freedom Bill (The American Congress) of 2 April 2013 which provides that companies must perform a "*HUMAN RIGHTS DUE DILIGENCE"* and define "*Company policies applicable to the company's internal operations that address human rights due diligence through a statement of policy that is consistent with applicable provisions of the Guidelines for Multinational Enterprises issued by the Organization for Economic Co-operation and Development."*[123]

At the United Nations level the "Guiding Principles on Business and Human Rights" adopted in 2011 provide[124]:

> *"The United Nations Guiding Principles on Business and Human Rights (UNGPs) are a global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity. On June 16, 2011, the United Nations Human Rights Council unanimously endorsed the Guiding Principles for Business and Human Rights, making the framework the first corporate human rights responsibility initiative to be endorsed by the United Nations.*
> *These Guiding Principles are grounded in recognition of:*
> *(a) States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms;*
> *(b) The role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights;*
> *These Guiding Principles apply to all States and to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure.*
> *2. States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.*
> *11. Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved* […].
> *The corporate responsibility to respect human rights indicates that businesses must act with due diligence to avoid infringing on the rights of others and to address negative impacts with which they are involved* […]. *The UNGPs hold that companies have the power*

123 H.R.491 (113th Congress) Global Online Freedom Act of 2013 referred in 2013 to the Subcommittee on Africa, Global Health, Global Human Rights and International Organizations. See also: OECD (2011), Guidelines for Multinational Enterprises.

124 Office of the High Commissioner (2011), Guiding Principles on Business and Human Rights, Implementing the United Nations "Protect, Respect and Remedy" Framework. Available at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf [Accessed 27 September 2016].

> *to affect virtually all of the internationally recognized rights.* ***Therefore, there is a responsibility of both the state and the private sector to acknowledge their role in upholding and protecting human rights*** […]*."* [the author's emphasis]

The Compact's policies[125], for example, Principles 1 and 2 provide that *"businesses should support and respect the protection of internationally proclaimed human rights"* and *"make sure that they are not complicit in human rights abuses*."[126]

Another example is provided by the "Globalization Declaration of Responsibilities and Human Duties adopted by a high-level group" (2002):

> *"Conscious of the increasing power and influence exercised by private and public corporations in the global order,* […]
> *Recognizing the changes that new technologies, scientific development and the process of globalisation have brought about, and aware of the need to address their impact upon and potential consequences for human rights and fundamental freedoms,* […]
>
> *Article 2* […]
> *6 Public and private corporations, especially transnational corporations, have a duty to respect, promote and implement human rights and fundamental freedoms in all spheres of their activities.*
>
> *Article 17*
> *2 The media and journalists have a duty to report honestly and accurately and to avoid incitement of racial, ethnic or religious violence or hatred* […].
>
> *Article 18 - Duties and Responsibilities Concerning Information and Communications Technologies*
> *4 States have a duty to prevent any misuse of these communications technologies and systems, especially as regards the propagation of hate and of material compromising the well-being of children."*[127]

The requirement to respect human rights, pursuant to Global Compact Principle 2 and the United Nations Guiding Principles on Business and Human Rights, includes avoiding **complicity** of violations in the course of conducting private business activities.[128]

---

125 The United Nations Global Compact is a United Nations initiative to call companies to align strategies and operations with universal principles on human rights, labour, environment and anti-corruption, and take actions that advance societal goals. The aim is to create a sustainable and inclusive global economy that delivers lasting benefits to people, communities and markets. This initiative is based on ten principles. Source: https://www.unglobalcompact.org/what-is-gc/mission/principles; https://www.unglobalcompact.org/ [Accessed 30 September 2016].

126 Bauml, J. (2011): "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship," *Federal Communications Law Journal*, Volume 63, issue 3, Article 6, p. 697. Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1600&context=fclj [Accessed 27 September 2016].

127 Globalization (2002) Declaration of Responsibility and Human Duties, adopted by a high-level group chaired by Richard J. Goldstone under the auspices of the city of Valencia and UNESCO initiated and organized by the Valencia third millennium foundation. Available at: https://fr.scribd.com/document/69837465/Declaration-of-Responsibilities-and-Human-Duties [Accessed 27 September 2016].

128 *On Principle 2 - Businesses should make sure that they are not complicit in human rights abuses:*

In the United States it had been suggested that the Alien Tort Statute (ATS) from 1789, the relevant section of which reads as follows: *"The district courts shall have original jurisdiction of any civil action by an alien for a tort only committed in violation of the law of nations* […]*"*[129] could be applied to corporate responsibility.[130]

To what extent legal liability may be imposed upon ISPs for failure to take action against radicalizing content which violates International Human Rights Law and in particular the right to life and to what extent such liability may be covered by the above complicity standard and how these "Internet Law Principles" interplay with domestic immunity are questions that must necessarily be addressed by the international community.

In addition to accountability standards under **International Law** we shall now turn to State laws that impose obligations and liability on the private sector by **delegation** of government duties and responsibilities to such private actors.

Historically delegation of government's core prerogatives and duties to the private sector is a well-established tradition. We need only think of States having recourse over the centuries to mercenaries and privateers fulfilling essential roles of government (based on a Hobbesian view).[131]

---

*"**Complicity is generally made up of 2 elements:***

- *An act or omission (failure to act) by a company, or individual representing a company, that "helps" (facilitates, legitimizes, assists, encourages, etc.) another, in some way, to carry out a human rights abuse, and*
- *The knowledge by the company that its act or omission could provide such help."*

"Accusations of complicity can arise in a number of contexts:

- *Direct complicity — when a company provides goods or services that it knows will be used to carry out the abuse*
- *Beneficial complicity — when a company benefits from human rights abuses even if it did not positively assist or cause them*
- *Silent complicity — when the company is silent or inactive in the face of systematic or continuous human rights abuse. (This is the most controversial type of complicity and is least likely to result in legal liability)."*

129 28 U.S. Code §1350.

130 This seems not to be the case however after the judgement in *Kiobel v. Royal Dutch Petroleum* (17. September 2010). Kiobel dealt with claims by residents in Nigeria against Shell Transport and Trading Company PLC for aiding and abetting the Nigerian government in human rights violations.The court held that corporations could not be held liable under the ATS (while individuals can). *Kiobel v. Royal Dutch Petroleum Co*. [2013], 133 S.Ct. 1659 (Supreme Court of the United states of America).

131 Wittes, B.; Blum, G: (2015) *The future of violence: Robots and germs, hackers and drones - Confronting the new age of threat*. Gloucestershire, United Kingdom: Amberley Publishing: The role of privateers played in the American Revolution actually led the Framers to write into the Constitution the authority to "grant Letters of Marque and Reprisal. The Torpedo Act, which put on all British warships a bounty worth half their value to any civilian who managed to destroy one is another such example. See also: Eastman, Famous Privateers of New England p. 1 (citing Edward I 1295 reprisal commission). See also: Francis R. Stark, "The Abolition of Privateering and the Declaration of Paris," in Studies in History, Economics and Public Law 221, 270–72 (Faculty of Political Sci. of Columbia Univ. eds., Columbia University, 1897): King Henry III of England first issued what later became known as privateering commissions in 1243.These early licenses were granted to private individuals and allowed them to seize assets of enemies of the realm in return for splitting the proceeds.
See also : Code de la Marine Ordonnance Colbert Ordonnance de Louis XIV Roy de France et de Navarre données à Fontainebleu au mois d'Août 1681 touchant la marine (abrogée par l'article 7 de l'ordonnance no 2006-460 du 21 avril 2006 relative à la partie législative du code général de la propriété des personnes publiques), LIVRE TROISIEME. Des Contrats Maritimes, X. Des Lettres de Marque, ou de Représailles.
See also: Article I, section 8 of the Constitution of the US: *"The Congress shall have Power To lay and collect Taxes, Duties, Imposts and Excises, to pay the Debts and provide for the common Defence and general Welfare of the United States; but all Duties, Imposts and Excises shall be uniform throughout the United States; […]"*
To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water;"
See also : Déclaration du Congrès de Paris sur le droit maritime : "*Les Plénipotentiaires qui ont signé le Traité de Paris du 30 mars 1856, réunis en conférence, […] Dûment autorisés, les susdits Plénipotentiaires sont convenus de se concerter sur les moyens d'atteindre ce but, et, étant tombés d'accord, ont arrêté la Déclaration solennelle ci-après :*
1° La course est et demeure abolie ;
2° Le pavillon neutre couvre la marchandise ennemie, à l'exception de la contrebande de guerre ;

In the United States more recently a bill was presented before the House of Representatives (10 October 2001) according to which:

> *"(4) The President of the United States is authorized and requested to commission, under officially issued letters of marque and reprisal, so many of* ***privately armed and equipped persons and entities*** *as, in his judgment, the service may require, with suitable instructions to the leaders thereof, to employ all means reasonably necessary to seize outside the geographic boundaries of the United States and its territories the person and property of Osama bin Laden, of any al Qaeda co-conspirator, and of any conspirator with Osama bin Laden and al Qaeda who are responsible for the air piratical aggressions and depredations perpetrated upon the United States of America on September 11, 2001, and for any planned future air piratical aggressions and depredations or other acts of war upon the United States of America and her people."*[132] [The author's emphasis].

Delegation is sometimes referred to as "cooperation" or "out-sourcing" or "privatization".

In the United Kingdom the government has undertaken partial privatization of services of the Royal Fleet Auxiliary.

Training of sailors and coastguards have been outsourced to private entities in several countries.

Oil platforms which are easy targets for pirates and terrorists and Private Military Companies (PMCs) often ensure armed escorts between ports and platforms.

The deployment of private soldiers in Iraq is another example. It was approved by the Coalition Provisional Authority (CPA) in June 2004.

Since 2005, a comprehensive reform has profoundly changed the provision of security services to French airports. Airport management is now entrusted to private companies by means of a Public Service Delegation.

Private companies are increasingly commissioned with security services to the United Nations. Specific United Nations Guidelines have been published on the use of such private security services.[133]

In some instances, delegation is complete in the sense that it imposes duties on private enterprises which are backed by legal sanctions.

3° La marchandise neutre, à l'exception de la contrebande de guerre, n'est pas saisissable sous pavillon ennemi ;
4° Les blocus, pour être obligatoires, doivent être effectifs, c'est-à-dire maintenus par une force suffisante pour interdire réellement l'accès du littoral de l'ennemi. […] Fait à Paris, le 16 avril 1856."
In May 2007, the company SECopEX (a private military company based in Carcassonne, France) signed a training contract with the Somali government for coastguards Ageis Defense Services in Yemen and Djibouti. Coastal surveillance. The British company VT Group provides ships to the Royal Navy and thereby participates to coastal surveillance; including partnerships with the US Coast Guard, the US Navy and the Royal New Zealand Navy to which it provides ships and detection and monitoring equipment. Escorts performed by armed ship like those of Background Asia Risk Solutions (BARS), or Blackwater have also been outsourced.

132 H.R. 3076, September 11 Marque and Reprisal Act of 2001. Available at https://www.gpo.gov/fdsys/pkg/BILLS-107hr3076ih/pdf/BILLS-107hr3076ih.pdf [Accessed 27 September 2016].

133 Wittes, B.; Blum, G. (2015) The future of violence: Robots and germs, hackers and drones - Confronting the new age of threat. Gloucestershire: Amberley Publishing.
See also: United Nations Department of Safety and Security (2012), Guidelines on the Use of Armed Security Services from Private Security Companies.

An example of such **Complete Delegation** is the "outsourcing" of the efforts against "money laundering".

In the European Union the Directive 2015/849 (20 May 2015) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing imposes substantial and detailed obligations on the private sector:

> Recital (18): "*This Directive should also apply to activities of obliged entities which are performed on the Internet.* […] *obliged entities."* [are defined as follows in Art. 2]:
>
> *"(1) credit institutions;*
>
> *(2) financial institutions;*
>
> *(3) the following natural or legal persons acting in the exercise of their professional activities:*
>
> *(a) auditors, external accountants and tax advisors;*
> *(b) notaries and other independent legal professionals,* […]
> *(c) trust or company service providers not already covered under point (a) or (b);*
> *(d) estate agents;*
> *(e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;*
> *(f) providers of gambling services.*[134]"

"Obliged entities" are both private individuals and corporations and their duties and obligations are clearly of a law enforcement nature. Violations of these duties and obligations carry severe sanctions.

The United Nations' Security Council had already adopted Resolution 1373 on 28 September 2001. The resolution imposes obligations on financial institutions:

> *"[…] All states shall:*
>
> *(d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned*

---

134 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC:
- Article 8:
"1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing […].
3. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing […]."
- Article 11:
"Member States shall ensure that obliged entities apply customer due diligence measures […]."
- Article 18:
"2. Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex and Unusually large transactions, and all Unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious".
- Article 58:
"1. Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive […]. Any resulting sanction or measure shall be effective, proportionate and dissuasive."

or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;"[135]

The Convention on Cybercrime imposes strict obligations on ISPs as a consequence of *de facto* delegation of government duties (Budapest, 23. November 2001):

"Article 18 – Production order
1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: […]
b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
Article 20 – Real-time collection of traffic data
1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: […]
B. compel a service provider, within its existing technical capability:
I to collect or record through the application of technical means on the territory of that Party; or
II to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. […]

Article 21 – Interception of content data
1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: […]
b. compel a service provider, within its existing technical capability:
I to collect or record through the application of technical means on the territory of that Party, or
II to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system."[136]

---

135 United Nations Security Council (2001), Resolution 1373 Adopted on 28 September 2001. Available at: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf [Accessed 27 September 2016] and the General Assembly (1999), United Nations Convention for the Suppression of the Financing of Terrorism: Resolution 54/109. Available at: http://www.un.org/law/cod/finterr.htm [Accessed 30 September 2016]:
"Article 18
(b) Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity. For this purpose, States Parties shall consider:
(ii) With respect to the identification of legal entities, requiring financial institutions, when necessary, to take measures to verify the legal existence and the structure of the customer by obtaining, either from a public register or from the customer or both, proof of incorporation, including information concerning the customer=s name, legal form, address, directors and provisions regulating the power to bind the entity;
(iii) Adopting regulations imposing on financial institutions the obligation to report promptly to the competent authorities all complex, unusual large transactions […]
(iv) Requiring financial institutions to maintain, for at least five years, all necessary records on transactions, both domestic or international […]"

136 Convention on Cybercrime (2001), Council of Europe, Treaty No. 185.

The Arab Convention on Combating Information Technology Offences (21 December 2010) contains similar obligations:

> *"Article 25: Order to Submit Information*
> *Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:*
> *1- Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information.*
> *2- Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or Under his control.*
>
> *Article 28: Expeditious Gathering of Users Tracking Information*
> *1- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to:*
> *a- gather or register using technical means in the territory of this State Party.*
> *b- require the service provider, within his technical competence, to:*
> *- gather or register using technical means in the territory of this State Party, or*
> *- cooperate with and help the competent authorities to expeditiously gather and register users tracking information with the relevant communications and which are transmitted by means of the information technology."*[137]

The General Data Protection Regulation of the European Union (27 April 2016) is another example of Complete Delegation:

> *"Article 24 - Responsibility of the controller*
> *1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.* […]
>
> *Article 25 - Data protection by design and by default*
> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
> *2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed* […]*."*

[137] Arab Convention on Combating Information Technology Offences (2010), League of Arab States.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. […]. *"*[138]

An interesting example of Complete Delegation (even involving strict liability) is provided by the Convention on Third Party Liability in the Field of Nuclear Energy of 29th July 1960, as amended by the Additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982 whereby the Signatory States agreed as follows:

"Article 1

a. For the purposes of this Convention:

i. "Operator" in relation to a nuclear installation means the person designated or recognised by the competent public authority as the operator of that installation."

"Article 3

a. The operator of a nuclear installation shall be liable, in accordance with this Convention, for:

i. damage to or loss of life of any person; and

ii. damage to or loss of any property other than

1. the nuclear installation itself and any other nuclear installation, including a nuclear installation under construction, on the site where that installation is located; and

2. *any property on that same site which is used or to be used in connection with any such installation,*

upon proof that such damage or loss (hereinafter referred to as "damage") was caused by a nuclear incident in such installation or involving nuclear substances coming from such installation, except as otherwise provided for in Article 4."[139]

Obligations have also been imposed on financial institutions to stop illegal Internet gambling and processing of payments.

---

138 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG [Accessed 30 September 2016].

139 Convention on Third Party Liability in the Field of Nuclear Energy of 29th July 1960, as amended by the Additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982. Available at: https://www.oecd-nea.org/law/nlparis_conv.html [Accessed 27 September 2016].

In the United States the unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) [140] has made financial institutions liable for payment processing and[141] the Communications Assistance for Law Enforcement Act (CALEA) of 1994 imposes a duty to cooperate with Law Enforcement Agencies.[142]

The "Communication from the Commission to the European Parliament and the Council concerning Terrorist recruitment: addressing the factors contributing to violent radicalization" (29 September 2005) is another example of such "Complete Delegation" of government prerogatives and obligations to the private sector:

> *"2.2. The Internet* […]
>
> *Article 3(4) – (6) covers the possibility to take appropriate measures against violent radicalization and terrorist recruitment occurring via the Internet.* […] *Therefore, measures may be adopted against services provided illegally in the context of terrorism. Article 15(2) of the Directive allows Member States to establish obligations for information society service providers to immediately inform competent public authorities of specific alleged illegal activities undertaken or information provided by recipients of their service* […]. *"*[143]

Another example is the Proposal for a Directive of the European Parliament and of the Council concerning the provision of audiovisual media services in view of changing market realities:

---

140 Unlawful Internet Gambling Enforcement Act of 2006, 31 USC 5361-5366.

141 Visa and each of the other traditional payment networks maintain separate monitoring campaigns to identify and eliminate transactions emanating from child pornography merchants. Visa's program, for example, began in 2002. It has retained the services of an outside firm to search the Internet for child pornography websites that appear to be accepting Visa payment cards. This firm uses advanced web crawling and filtering technology to detect these websites. It looks for websites that display the Visa logo, and that satisfy one or more indicators that they are engaged in the sale of child pornography or are marketing themselves as engaged in that business. The sweeps are ongoing; they are conducted daily and search hundreds of millions of web pages each month. Source: MacCarthy, M. (2009) *What Internet Intermediaries Are Doing About Liability and Why It Matters*, Washington, United States: ExpressO, Georgetown University

142 Communications Assistance for Law Enforcement Act of 1994, 47 USC 1001-1010; Wittes, B.; Blum, G. (2015) *The future of violence: Robots and germs, hackers and drones - Confronting the new age of threat*. Gloucestershire: Amberley Publishing, where the Copyright Alert System in the United States and ICANN delegation are also mentioned. See also Van Eeten, M.; Mueller, M. and Van Eijk, N. (2014) *The Internet and the State: A Survey of Key Developments*. Den Haag, Netherlands: Raad voor Maatschappelijke Ontwikkeling.

143 Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment: addressing the factors contributing to violent radicalization [COM (2005) 313 final].
"Option 2: Forbidding Internet services providers to give access to material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism
This option implies the introduction of a new legislative instrument specifically addressed to Internet service providers or the amendment of the existing provisions. It intends that Internet service providers based in Europe apply systematically blocking techniques in order to prevent Internet users from accessing material aiming at public provocation to commit terrorist offences, recruitment or training for terrorism. This material should be kept outside EU cyber-space."

"An important share of the content stored on video-sharing platforms is not under the editorial responsibility of the video-sharing platform provider. However, those providers typically determine the organization of the content, namely programmers or user-generated videos, including by automatic means or algorithms. Therefore, those providers should be required to take appropriate measures to protect minors from content that may impair their physical, mental or moral development and protect all citizens from incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, color, religion, descent or national or ethnic origin."[144]

As far as the legitimacy of outsourcing the above duties to private sector is concerned it seems reasonable to assert that the same reasoning applies to content regulation and particularly by analogy from anti-money laundering obligations. ISPs are most favorably placed to monitor their own infrastructure and technology. Given ISP control over that infrastructure it may additionally be argued that delegating duties in the field of content regulation is even more legitimate than delegating money laundering duties to financial institutions in view of the capability of government through financial regulators to act independently.

Apart from the notion of government formally delegating specific obligations to the private sector which as we have seen is a well-established method of satisfying government's duties we also see an expanding use of **voluntary schemes** or **"Cooperation Undertakings"** and in particular with regard to Internet content regulation. An example hereof is the *"Safer Social Networking Principles for the EU"* which were adopted, by the main Internet actors (Dailymotion, Google, Facebook, Yahoo etc.)[145]:

"Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

SNS providers should, during the normal course of developing and managing SNSs, assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports of images, videos and text that may contain illegal and inappropriate/Unacceptable/prohibited content and/or conduct.

There is a range of procedures which can be used to promote compliance with the Terms of Service, Acceptable Use Policy and/or House Rules. These may include for example: human and/or automated forms of moderation; technical tools (e.g. filters) to flag potentially illegal or prohibited content; community alerts; user-generated reports.

Some providers employ human moderators who interact in real-time with children or young people. Such providers should take reasonable steps (working within good practice frameworks where possible or legal frameworks as applicable), to minimize the risk of employing candidates who may be unsuitable for work which involves real-time contact with children or young people."

Some ISPs have adopted Codes of Practices on a voluntary basis.

144 Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities [COM/2016/0287 final - 2016/0151 (COD)].

145 Safer Social Networking Principles for the European Union (2009).

This is the case for The Internet Service Providers Association (ISPA) in the UK (25 January 1999/03 July 2007):[146]

> "*2.1 Legality**:***
> *Members shall use their reasonable endeavors to ensure the following:* […]
> *2.2.2 Members, their Services (excluding Third Party Content) and Promotional Material do not encourage anything which is in any way unlawful.*
> *5.2 ISPA co-operates with the IWF in its efforts to remove illegal material from Internet web-sites and newsgroups. Members are therefore required to adhere to the following procedures in dealing with the IWF.*
> *5.4 Where the IWF has notified them that Internet sites they host and/or use net news groups contain material which the IWF considers to be illegal child abuse images, members shall remove the specific web pages and/or use net articles. If it is not technically possible for them to remove the material, Members shall notify the IWF of the reasons as soon as reasonably practical."*[147]

The Internet Watch Foundation (IWF) in the United Kingdom is an example of delegation of services, but without liability and the INHOPE system works according to the same methodology.[148]

Sometimes an appeal for **cooperation** is chosen.

An example of **cooperation** is the European Union Directive 2013/40/EU on attacks against information systems (August 12th 2013):

"It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes."[149]

---

146 ISPA UK Code of Practice (1999, as amended in 2007).

147 The European Commission and IT Companies Announce an agreed Code of Conduct on illegal online hate speech (31 May 2016)
"By signing this code of conduct, the IT companies commit to continuing their efforts to tackle illegal hate speech online. This will include the continued development of internal procedures and staff training to guarantee that they review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.
The code of conduct includes the following public commitments […]
Upon receipt of a valid removal notification, the IT Companies to review such requests against their rules and community guidelines and where necessary national laws […], with dedicated teams reviewing requests."

148 Internet Watch Foundation, Available at: https://www.iwf.org.uk/ [Accessed 29 September 2016]; INHOPE - International Association of Internet Hotlines, Available at: http://www.inhope.org/gns/home.aspx [Accessed 29 September 2016]

149 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

The United Nations General Assembly Plan of Action to Prevent Violent Extremism reads:

> Recital 58:
> […] "*(k) Invite relevant private actors, including communications and social media companies, to support the prevention of violent extremism initiatives and generate creative ideas to help the international community effectively address the spread of violent extremism through the Internet;"*
>
> *"**V. An appeal for concerted action.**"*[150]

Outsourced liability may also be construed on the basis of a **concession model**:

Directive 1999/93/EC on a Community framework for electronic signatures December 13th 1999:

> "*Article 6 - Liability*
> *1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:* […]"[151]

In addition to liability based on delegation ("outsourcing" or "privatization") or voluntary schemes ISP liability might conceivably be based on a product liability theory:

> "[ISPs] *are in a unique position to address the problems presented by malicious content on hosted websites, created either by the customer running the site or by third parties who have infected* [a] *site owned by a customer*." (Stop BadWare)[152]

---

150 United Nations Plan of Action to Prevent Violent Extremism (2015), Seventieth session Agenda items 16 and 117.

151 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Article 19: Security requirements applicable to trust service providers:
"1. Qualified and non-qualified trust service providers shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."
See also: Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, Article 1: *"This Directive establishes the rights of end-users and the corresponding obligations on Undertakings providing publicly available electronic communications networks and services."*
See also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Recital (20): [...]"*The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, Unforeseen security risks and restore the normal security level of the service*.";
Article 4 - Security: "1. *The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented*."

152 StopBadWare is a non-profit organisation "that maked the Web safer by fighting BadWare" (www.stopbadware.org) Quote cited from the webarticle *Web Hosting Provider Liability for Malicious content. (*p. 2.) Available at: https://www.nist.gov/sites/default/files/documents/itl/StopBadware_Web-Hosting-Provider-Liability-for-Malicious-Content.pdf [Accessed on 27 September 2016].

Does this "unique position" cause ISP liability for malware diffused through their infrastructure and if so inadvertently or after acquiring knowledge of the malicious content placed by a third party?

This question is of course pertinent also to the inadvertent or continued dissemination of radicalizing content.

It is undecided whether the Communication Decency Act's immunity regime covers damage caused by malware. In the case *Green v. America Online*[153] the court held that "information" included computer machine language and that an ISP was not liable for the consequences of third party generated "signals" as per the immunity provisions of the Communication Decency Act. It is not decided yet however to what extent such immunity also covers **continued** dissemination of malware (*i.e.* after the ISP acquires knowledge about its presence on its infrastructure). In the United States current case law would not directly support such liability.[154]

Google's development contract for third parties does however recognize potential product liability linked to distribution of applications developed by such third parties.[155]
Thus Google has contractually discharged any liability it might have for prejudice caused by applications developed by third parties and downloaded from its platform (of course the end user not being party to the developer agreement may forcefully argue not to be bound by it).

In recognition of this potential exposure Google announced that Android applications would be analyzed for malicious functionality before being allowed onto the Android Market (this is the so-called "Bouncer-system").[156]

On 17 March 2016 Google announced moving to human review of applications replacing machine vetting.

---

153 *Green v. America Online* [2003], 318 F.3d 465 (Ct. App. 3rd Cir.).

154 StopBadWare (2016) *Web Hosting Provider Liability for Malicious content.* (p. 3) Available at: https://www.nist.gov/sites/default/files/documents/itl/StopBadware_Web-Hosting-Provider-Liability-for-Malicious-Content.pdf. [Accessed on 27 September 2016].
The *Zeran* case (*Zeran v. America Online, Inc*. [1997], 129 F.3d 327 (4th Cir.) releases ISPs from an obligation to remove harmful content.

155 Google Play Developer Distribution Agreement (02 July 2016). Available at: https://play.google.com/about/developer-distribution-agreement.html [Accessed 30 September 2016]:
"*4.4* ***Prohibited Actions.*** *You agree that you will not engage in any activity with the Store, including the development or distribution of Products, that interferes with, disrupts, damages, or accesses in an Unauthorized manner the devices, servers, networks, or other properties or services of any third party including, but not limited to, Android users, Google or any mobile network operator. You may not use customer information obtained from the Store to sell or distribute Products outside of the Store.*
7.2 ***Google Takedowns.*** *While Google does not Undertake an obligation to monitor the Products or their content, if Google is notified by you or otherwise becomes aware and determines in its sole discretion that a Product or any portion thereof or your Brand Features; (a) violates the intellectual property rights or any other rights of any third party; (b) violates any applicable law or is subject to an injunction; (c) is pornographic, obscene or otherwise violates Google's hosting policies or other terms of service as may be updated by Google from time to time in its sole discretion; (d) is being distributed by you improperly; (e) may create liability for Google or Authorized Carriers; (f) is deemed by Google to have a virus or is deemed to be malware, spyware or have an adverse impact on Google's or an Authorized Carrier's network; […] Google may remove the Product from the Store or reclassify the Product at its sole discretion. Google reserves the right to suspend and/or bar any Developer from the Store at its sole discretion. If your Product contains elements that could cause serious harm to user devices or data* […]"

156 Whitman, R. (2012): "Circumventing Google's Bouncer, Android's anti-malware system", *Extreme Tech*. Available at:http://www.extremetech.com/computing/130424-circumventing-googles-bouncer-androids-anti-malware-system. [Accessed on 27 September 2016].

An interesting example involving product liability (and negligence) is offered by the lawsuit filed against Google by Susan Harvey alleging that she lost thousands of dollars over 16 months due to her Google Play store account being hacked. Unfortunately, the questions raised by the case were not addressed since the claims were time barred being subject to a one-year-statute of limitations.[157]

The distinction between "online" and "offline" products (and thus arguably their liability standards) was upheld by the United States Court of Appeal for the Federal Circuit in a recent case (10 November 2015) where it was decided that the United States International Trade Commission (USITC) cannot order the blocking of websites allowing online patent or copyright infringement.

The case involved the company ClearCorrect which scans and forwards information on dental patients to its affiliate based in Pakistan. ClearCorrect Pakistan develops diagrams which are returned – still online – to ClearCorrect in the United States where the "physical" product is created (dental aligners).

The Company Align Technology also based in the United States complained against those practices before the United States International Trade Commission claiming patient infringement. The Court of Appeals found that the Trade Commission did not have the authority to regulate digital goods (even if such "digital infringements" could facilitate "physical infringement").[158]

---

157 *Susan Harvey v. Google Inc. and Does 1-20*, 15-cv-03590 (United States District Court Eastern District of California San Jose Division 2015):
"***1. Violation of Electronic Funds, Transfer Act and the California Unfair Competition Law Negligence (i.a)***
On or about March 20, 2013, Plaintiff activated her new Smartphone supported by an Android software operating system. After powering on her phone, Plaintiff was asked to provide a Google e-mail address or sign on using a Google e-mail address; she signed on using her prior Google e-mail address. Subsequently, the Android operating system prompted Plaintiff to provide payment information in order for her to receive updates regarding her phone. Plaintiff complied by providing the debit/banking information for her checking account with Bank of America.
In or around August of 2014, upon attempting to recover another application she had purchased in 2013, for downloading onto a second phone, Plaintiff logged on to her Google account through her computer, and was notified through her Google dashboard that there were one-hundred and nine (109) transactions on her account. Upon clicking on the appropriate tab on Google's website, Plaintiff was shocked to find approximately six-hundred and fifty (650) listed transactions, the majority of which were Unrecognizable to Plaintiff, and certainly not transactions conducted by Plaintiff.
The plaintiff argued that: […]
19.Google failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised […]
26.Identity thieves can use personal information such as that pertaining to Plaintiff, which Google failed to keep secure, to perpetrate a variety of crimes that do not cause financial loss but nonetheless harm the victims. […]
46.Google, through its actions and/or omissions, unlawfully breached its duty to
timely disclose to Plaintiff that her Information had been compromised. […]
63.Plaintiff was and continues to be damaged as a direct and/or proximate result of Google's invasion of their privacy by publicly disclosing the Information, in the form of, inter alia, actual monetary losses, expenses for credit-monitoring and identity-theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they are entitled to compensation."
See also: CBS News (4 July 2016): "Beware downloading some apps or risk "being spied on". Available at: http://www.cbsnews.com/news/mobile-phone-apps-malware-risks-how-to-prevent-hacking-breach/ [Accessed 30 September 2016]: "*Popular apps on your smartphone can be convenient and fun, but some also carry malicious software known as malware, which gives hackers easy access to your personal information.*
A security firm found that between 75 and 80 percent of the top free apps on Android phones or iPhones were breached. The number jumps as high as 97 percent among the top paid apps on those devices. Whether these apps help advertisers target you or help hackers rip you off, you'll want to do your homework before downloading apps, reports CBS News correspondent Anna Werner."

158 *Clearcorrect Operating Llc and Clearcorrect Pakistan Ltd., v. International Trade Commission and Align Technology Inc.*, 2014-1527 (United States Court of Appeals for the Federal Circuit 2015): The judgement of November 2015 could potentially have been submitted to the Supreme Court, but Align and ITC did not take further steps by the 26 August 2016 deadline.

Thus the law continues to distinguish between "digital" and "physical goods" in terms of agency remit and liabilities, but it may very well only be a question of time before some sort of Product Liability Standard is applied to "online goods".[159]

Liability based on complicity

It has been argued that ISPs may be held liable on the basis of a Theory of Complicity for content dissemination, such liability ultimately being of a penal nature (associated with punitive damages). This theory caused the Council of Europe in its Explanatory Report to the Convention on the Prevention of Terrorism (16. May 2005)[160] to express a limitative view on such liability:

> *"Paragraph 1 requires Parties to establish as a criminal offence the participation as an accomplice in the commission of any of the offences under Articles 5 to 7. Liability for such complicity arises where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. For example, although public provocation to commit a terrorist offence through the Internet requires the assistance of service providers as a conduit, a service provider that does not have criminal intent cannot incur liability under this provision."*[161]

In the United States the two federal statutes that criminalize **material support** for terrorism and foreign terrorist organizations, 18 U.S.C. §§ 2339A and 2339B have been invoked in recent cases dealing with terrorist or radicalizing content.[162] Material support provided in the form of certain kinds of speech under the direction or in coordination with foreign terrorist organizations in violation of section 2339B may be punished and such punishment is deemed consistent with the First Amendment.[163]

---

159 McEvoy, C. (2013): "Google Dodges Class Action over Vulnerable Android Aps", *Law 360*. Available at: http://www.law360.com/articles/414105/google-dodges-class-action-over-vulnerable-android-apps [Accessed on 27 September 2016]: "*A California judge on Friday dismissed a putative class action brought by Android cellphone users who said Google Inc. reaped commissions on faulty applications that were vulnerable to malicious software, ruling that the state's Song-Beverly Consumer Warranty Act is limited to tangible items that can be physically repaired. At a Friday hearing in Los Angeles County Superior Court, Judge Jane L. Johnson granted Google's request to dismiss the lawsuit, but gave the plaintiffs 30 days to amend their complaint as to a portion of the state's."*

160 Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism (2005), Council of Europe, Treaty No.196

161 According to the "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems" (28. January 2013):
"*Article 7 – Aiding and abetting*
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences Under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed."

162 See below: *Tamara Fields v. Twitter.*
18 U.S.C. § 2339A - Providing material support to terrorists prohibits:
"*2. (a) providing material support or resources*
3. knowing or intending that they be used
(a) in preparation for,
(b) in carrying out, […]
4. an offense identified as a federal crime of terrorism, […]*."*

163 *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010), 130 S.Ct. 2705 (Supreme Court of the United States).

Under Section 2339B[164], intention (which is a condition for complicity) relates to "*knowledge that the organization has been "designated terrorist organization"* or *"has engaged in terrorism or terrorist activity"*. The scope of knowledge ("intention") is broader than under Section 2339 A.[165]

A number of cases against ISPs have been introduced by reference to the above "material support theory".

The families of Israeli and American victims argue in a lawsuit filed in New York against Facebook on 10 July 2016 that the company "*knowingly provided material support and resources to terrorist group Hamas*".

The United States Court of Appeals for the district of Columbia Circuit (14 June 2014), decided in a similar case (*Larry Elliott Klayman v. Mark Zuckerberg and Facebook*)[166] that the Communications Decency Act mandates dismissal if (i) Facebook is a "provider or user of an interactive computer service," (ii) the information for which Klayman seeks to hold Facebook liable was "information provided by another information content provider," and (iii) the complaint seeks to hold Facebook liable as the "publisher or speaker" of that *information […].. "We hold that, on the face of this complaint, all three prongs of that test are satisfied […]. Klayman does not seriously dispute that Facebook meets the statutory definition of an interactive computer service […]. He argues, instead, that Facebook should not qualify because it "can control the contents posted on [its] website […]. The short answer is that Congress did not write that additional limitation into the Act, and it is this court's obligation to enforce statutes as Congress wrote them. […]."*

A related "complicity" action was recently dismissed by the United States District Court Northern District of California (10 august 2016), *Tamara Fields v. Twitter*.[167]

In November 2015, Lloyd "Carl" Fields, Jr. and James Damon Creach were shot and killed while working as United States government contractors at a law enforcement training center in Amman, Jordan. In subsequent statements, the Islamic State of Iraq and Syria ("ISIS") claimed responsibility for the attack. Plaintiffs, the wife of Fields and the wife and children of Creach, thought hold Twitter liable under 18 U.S.C. § 2333(a), of the Anti-Terrorism Act, on the theory that Twitter provided material support to ISIS by allowing ISIS to sign up for and use Twitter accounts and that that Twitter *"has knowingly permitted […] ISIS to use its social network as a tool for spreading extremist propaganda, raising funds and attracting new recruits,"* and that *"[t]his material support has been instrumental to the rise of ISIS and has enabled it to carry out numerous terrorist attacks".* Plaintiff further argued that: *"[…] potential recruits and ISIS recruiters often communicate via Twitter's Direct Messaging capabilities"* and "*that their claims are not based on "the contents of tweets, the issuing of tweets, or the failure to remove tweets," but rather on Twitter's "provision of Twitter accounts to ISIS in the first place […]."*

---

164 Section 2339B prohibits providing material support or resources to a foreign terrorist organization knowing that the organization (a) has been designated a foreign terrorist organization, or (b) engages, or has engaged in "terrorism" or "terrorist activity."

165 This is illustrated by the case *United States of America v. Tarek Mehanna* [2013], 12-1461 (Ct. App. 1st Cir.) involving translations of Al Qaeda material.

166 *Larry Elliott Klayman v. Mark Zuckerberg and Facebook Inc*. [2014], 13-7017 (United States Court of Appeals for The District of Columbia Circuit).

167 *Fields v. Twitter Inc*. [2016], 16-cv-00213-WHO (United States District Court Northern District of California). Available at: https://casetext.com/case/fields-v-twitter-inc [Accessed 28/09/2016].

Twitter moved to dismiss on several grounds, including that plaintiffs' claims are barred by the Communications Decency Act since Twitter cannot be treated as a publisher or speaker of ISIS's hateful rhetoric and is not liable under the facts alleged.
Plaintiff's claims were dismissed by the judge (together with a theory of Direct Messaging Capability not being protected by the Communications Decency Act).
Plaintiff has since filed an amended complaint on 30 August 2016 demanding a jury trial.

The fact that social media companies increasingly cooperate in removing radicalising content may however amount to a recognition of terrorist use of their services and it may be expected that case law will evolve on the standards of "complicity", "intention", "knowledge" and "diligence". Thus cases against Facebook are pending in other countries including France, Germany, Israel and Brazil.[168]

ISP liability may also arguably be based on failure to warn or to act:

The case *Doe #14 v. ModelMayhem*[169] illustrates the reasoning:

ModelMayhem is a website for models. The plaintiff was a victim of rape committed by a user of the site. She claimed that ModelMayhem had been instrumental in identifying her as a potential victim and had failed to issue a warning about this "known" risk use of its services.

The plaintiff lost the case since the website had no duty to issue warnings of a generally known risk, but arguably the case would have been different had the risk not been generally known.

As we have seen above liability may also derive from **Media Law principles** in case the ISP is deemed to be **"the publisher"** of the content (sometimes qualified as the "secondary publisher").
The Supreme Court of South Australia found that Google Inc. may be qualified as the "publisher of" defamatory content published in search result "snippets", auto-complete suggestions and even third party websites to which it provides hyperlinked search results.[170]

Google's liability in defamation under English law for material posted on Blogger.com after notice[171] was tested the case *Payam Tamiz v Google Inc*.[172] (14 February 2013). The Court of Appeal of England, while dismissing the case held that Google could be qualified as the publisher. [173]

168 Reuters (2016): "$1 Billion Lawsuit Accuses Facebook of Enabling Palestinian Attacks". Available at: http://fortune.com/2016/07/11/facebook-lawsuit-hamas-attacks/ [Accessed 28/09/2016].

169 *Jane Doe No. 14 v. Internet Brands, Inc., DBA Modelmayhem.com* [2014], No. 12-56638 (9th Cir.). See also: http://blog.ericgoldman.org/ [Accessed 30 September 2016].

170 *Duffy v Google Inc* [2015] SASC 170 (Supreme Court of South Australia) (*supra* p. 67).

171 Greer, D. (2013): "Google Inc's liability in defamation under English law for material posted on Blogger.com". Available at: http://www.lexology.com/library/detail.aspx?g=27427989-9bfa-4f74-b569-aad7645a0afb [Accessed 28/09/2016].

172 *Tamiz v. Google Inc.* [2013] EWCA Civ 68.

173 Blogger.com was acquired by Google in 2003 and is one of the web's most widely used host service providers.

"Google's role in operating Blogger was deemed not purely passive as they provide design tools, a URL, advertisements, service on terms of their choice and have the ability to remove or block access to any blog. Google is arguably a publisher and thus can be liable after notification. The provision of a blog is analogous to the Golf Club notice board in the case of Byrne v Deane [1937] 1 KB 818. In that case, defamatory material was left up on a notice board post notification."

The Court said that in such a case it could be inferred that the provider has participated in or has made itself responsible for its continued publication, unless action is taken within a reasonable time period.[174]

Liability based on prior notice

In the Google BlogSpot decision of 25 October 2011[175] the German Federal Supreme Court developed the principles governing host provider liability after notice.

The Court made obligations and liability under German Law contingent upon the specificity of the notice and the ability of the ISP to conclude on the basis of a superficial verification of the claim that the content is illicit.

In Italy the Court of Milan convicted 3 Google executives of privacy violations. The case dealt with a video uploaded on Google Video that showed a group of students bullying an autistic schoolmate.
In February 2010, the Court of Milan found all three Google executives guilty since they had failed to take down the video upon notice.[176]

Google appealed and the Court of Appeals overturned the judgment on 21 December 2012.[177]

The European Parliament and Council Directive 2000/31/EC of 8 June 2000 ("the e-Commerce Directive") addresses, inter alia, responsibilities of ISPs pursuant to notice.[178]

The European Court of Human Rights (ECHR) passed a landmark judgment (16 June 2015) in the *Delfi AS v. Estonia* case.[179]

---

174 *Davison v. Habeeb*, EWHC 3031 (QB) HHJ Parties QC (25 November 2011); *Byrne v Deane* [1937] 1 KB 818.

175 *Google Blogspot*, VI ZR 93/10 (BGH 2011).

176 *Google v. Vividown*, 1972 (Milan Court of First Instance 2010).

177 *Google v. Vividown* (Milan Court of Appeals 2012). This decision was confirmed by the Italian Supreme Court (*Google v. Vividown*, 5107/2014).

178 *"(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.*
(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.
(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

179 *Delfi AS v. Estonia* [2015], Case No. 64569/09 (European Court of Human Rights Grand Chamber).

It was the first case in which the ECHR was called upon to examine a complaint concerning the liability of an Internet news portal for comments posted by third parties.
The Court held "*that because of the particular nature of the Internet, the "duties and responsibilities" that are to be conferred on an Internet news portal for the purposes of Article 10* [Freedom of Expression under the European Convention for the Protection of Human Rights and Fundamental Freedoms] *may differ to some degree from those of a traditional publisher, as regards third-party content*."

The Court defined four criteria that should be taken into account when determining whether a host/platform was liable for comments posted by third parties had violated Article 10:

- the extreme nature of the comments in question (violation of "human dignity" and "clearly unlawful" nature);
- the fact that the comments were posted in reaction to an article published by the applicant company on its professionally managed news portal run on a commercial basis (readers being invited to post their comments without registering their names or providing any means of identification);
- the inadequate reaction by the platform when put on notice as to the illicit character of the statements to remove the offending comments without delay after publication;
- the moderate sanction imposed by the domestic court in question (Estonia).

The decision of the Estonian courts to hold Delfi AS accountable was upheld by the ECHR. It was deemed justified and did not constitute a disproportionate restriction on the company's right to freedom of expression. Thus, for the first time the European Court of Human Rights acknowledged that the liability of the operator of a commercial news portal had been engaged as a result of offensive comments posted by third parties.

ISP liability is frequently employed for the protection of **Intellectual Property**.

Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (may 22nd 2001) Art. 8 (3) reads:

> *"In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network."*

The judge in the Court of Appeals (London) decided a case on 6 July 2016 related to five English ISPs who appealed against judicial orders against certain websites which were advertising and selling counterfeit copies of Cartier, Montblanc and Richemont goods. The judge applied analogous protection to trademarks and copyrights.[180]

[180] *Cartier International AG, Montblanc-Simplo GMBH, Richemont International SA v. British Sky Broadcasting Limited, British Telecommunications plc and others* [2016] EWCA Civ 658 (Court of Appeal Civil Division):
The judge concluded that he had jurisdiction to make the order sought by Richemont and that it was appropriate to do so. He also held that the ISPs should bear the costs of its implementation. Following further argument, he awarded the costs of the

In the same vein, the European Parliament and Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights ("the Enforcement Directive") guarantees that:

> *"Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right."*[181]

The Comprehensive Economic and Trade Agreement between the EU and Canada[182] in Art. 20.11 reads:

> *"Liability of intermediary service providers*
> *1. Subject to the other paragraphs of this Article, each Party shall provide limitations or exceptions in its law regarding the liability of service providers, when acting as intermediaries, for infringements of copyright or related rights that take place on or through communication networks, in relation to the provision or use of their services.*

The Digital Millennium Copyright Act of 1998[183] in the United States offers a safe harbor from complicity provided the ISP is acting as a pure conduit and abides by a notice-take-down-procedure.

Online platforms may be subject to liability for the sale of counterfeit goods. In the *Tiffany v eBay* case, the Court ruled that eBay may be accountable for infringement of trademark law if it continues to provide its platform to sellers known to violate trademarks (a reason to believe standard is furthermore suggested).[184]

A **general monitoring obligation** is however not allowed:
Art. 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society provides:

---

substantive hearing to Richemont and he also settled the detailed terms of the order. The services of the ISPs allowed consumers in the United Kingdom to access the target websites.
The Court ruled: "95. *The advertisements and offers for sale of the counterfeit goods were communicated to consumers in the United Kingdom using the services of the ISPs, and the agreements to sell and supply counterfeit goods to consumers in the United Kingdom were made using the services of the ISPs*." "*Further, it matters not that there was no contractual relationship between the ISPs and the operators of the websites, or that the ISPs did not exercise any control over the particular services of which those consumers made use. The ISPs were essential actors in all of the communications between the consumers and the operators of the target websites."*
"161. In that regard the judge said this at [251]: "251. Before expressing a conclusion on the question of costs, it is necessary to consider the economic dimension of the problem. […] the economic logic of granting injunctions against intermediaries such as ISPs is that they are the "lowest cost avoiders" of infringement."
"18. An important feature of all of the orders made pursuant to s.97A has been that they have included a provision for the rightholders to notify additional IP addresses or URLs to the ISPs in respect of the websites which have been ordered to be blocked. This has allowed the rightholders to respond to efforts made by the website operators to circumvent the orders by changing their IP addresses or URLs. Responsibility has fallen on the rightholders to identify IP addresses and URLs which are to be notified to ISPs in this way. For this purpose, the film studios have engaged a business called Incopro to monitor the server locations and domain names used by the target websites. The judge found that this service and the costs of collating, checking and sending notifications to the ISPs amounted to around £3,600 per website per year."

181 The Charter of Fundamental Rights of the European Union Art. 17 states: "*Intellectual property shall be protected."*

182 Comprehensive Economic and Trade Agreement between Canada of the one part, and the European Union and its Member States, of the other part.

183 Digital Millennium Copyright Act of 1998, 17 USC. §§ 101, 104, 104A, 108, 112, 114, 117, 512, 701, 1201–1205, 1301–1332; 28 USC. § 4001.

184 *Tiffany Inc. v. eBay Inc*., 600 F.3d 93 (2d Cir. 2010). See also: Mark MacCarthy (2009): "What Internet Intermediaries Are Doing About Liability and Why It Matters". Washington, United States: ExpressO, Georgetown University

"In that regard, the Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as a hosting service provider, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights. […]*."*

On the prohibition of a general monitoring obligation, the Judgment of the European Court of Justice of 16 February 2012 in the case *Sabam v. Netlog*[185] is clear:

Under recitals 47 in the preamble to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market:

"Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature;"

- o -

Against the above initiatives to delegate, duties and obligations to ISPs and impose liability by reference to the above legal theories, a number of resolutions have been passed:

Manila Principles on Intermediary Liability, Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation (Version 1.0, March 24, 2015) provide that:

"a) Any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible.

b) Intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.

d) Intermediaries must never be made strictly liable for hosting unlawful third-party content, nor should they ever be required to monitor content proactively as part of an intermediary liability regime."

In the Report of the Special Rapporteur for the United Nations on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (16 May 2011) imposition of intermediary liability is restricted in the following terms:

185 *SABAM v. Netlog* [2012], Case C-360/10, Court of Justice of the European Union, Third Chamber

The Special Rapporteur emphasizes that censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals' human rights. Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences.

The countries surveyed for the Report apply different levels of ISP liability. In most cases such liability is grounded on general rules of complicity or secondary infringement theories[186]:

- According to Tunisia, liability can be held by analogy with the Law on countering terrorism: notably Art. 5 and 7.

- According to Art. 12 of the Criminal Code in Hungary the perpetrator of a crime "the indirect offender" and the "co-actor" as well as the "instigator" and the "abettor" (who intentionally assists another person in committing a criminal offence) are liable.

- Currently, India does not extend criminal penalty on Internet radicalization for intermediaries. However, India recognizes intermediaries as distinct legal entities. Further, Under Section 79 of the Indian Information Technology Act, 2000, intermediaries are mandated to exercise due diligence while discharging their obligations. Intermediaries are mandated to inform their users that they shall not use intermediaries' platform for violating any laws or public order or for incitement to the commission of any cognizable offence. Further, such intermediaries are required to inform their users that they shall not host, display, modify, publish, transmit, update or share any information on the intermediaries' computer resources that is grossly harmful, harassing, blasphemous, defamatory, libelous, hateful, racially or ethnically objectionable or otherwise unlawful in any manner whatsoever.

- In Australia, pursuant to section 11.2 of the Criminal Code, it is an offence for a person to aid, abet, counsels or procure the commission of another offence ('complicity and common purpose').

- The German criminal law does not explicitly extend the penal liability for Internet radicalization. Unless the law expressly provides for criminal liability based on negligence only intentional conduct attracts criminal liability. Thus intermediaries cannot usually be considered to have committed the offences themselves. However, depending on the individual case, intermediaries could be liable in accordance with the provisions for abetting or for aiding. According to Section 26 of the Criminal Code any person who intentionally induces another to intentionally commit an Unlawful act (abettor) is liable to be sentenced as if he were a principal. According to Section 27 of the Criminal Code any person who intentionally assists another in the intentional commission of an unlawful act shall be convicted and sentenced as an aider.

186 For complete answers, see Annex 1 "Country Questionnaire"

- In Denmark it follows from section 23 of the Criminal Code that the penalty provided for an offence also applies to those who are intermediaries.

- In the United Kingdom Specified Authorities have a duty to prevent extremism. According to Schedule 6 of the Counter Terrorism Act of 2015 this includes primarily schools, law enforcement and similar institutions. The Private sector at such is not included on the list

- In the Seychelles complicity liability could arise, but there is no specific law that addresses ISP liability.

- In Israel the Penal Law allows extending liability to intermediaries on the basis of an awareness standard

- In Slovakia it is assumed that ISPs could be liable for internet radicalization, but they need to meet the element of intention

- In Spain knowledge of disseminating illegal content may lead to liability on the basis of complicity (Criminal Code Law 34/2002)

- In Sweden when a crime is committed on the internet it is protected by the Fundamental Law on Freedom of Expression and in such cases the principle of sole liability applies. This means that only the publisher (typically) may be held criminally liable

- In Iraq any crime that may be extended to "partners or cooperators or persuaders" based on Art. 47, Art. 48 and Art. 49 of the Penal Law 111 of 196

- In Canada the concepts applied to intermediary liability is derived from English common law and appears in structured form in the Criminal Code they allow to extend criminal liability to counseling, attempting or being an accessory after the fact

- In Singapore an intermediary may engage his criminal liability under the Sedition Act and the Penal Code as well as the Broadcasting Act

- In Norway the general rule of complicity in the Penal code s. 15 would apply

- In Belgium, liability (not necessarily criminal) of intermediaries is dealt with by Articles XII.17 (mere conduit activity) to XII.20 (monitoring obligation) of the Code of Economy.

  Art. XII.19. § 1- Hosting activity

  §3 When the provider has knowledge of an illicit activity or data it communicates it immediately to the King's Attorney General who takes the useful measures in accordance with Article 39 bis of the Criminal Code. […]

Refusal to cooperate is a penal offence under XII.20, § 1er, 2 or de Art. XII.20, § 2
In addition, Art 66 -69 of the Penal code provides for a general principle of complicity.

- In Kenya Art. 62 of the National Cohesion and Integration Act from 2008, stipulates that:

  "*(2) A newspaper, radio station or media enterprise that publishes the utterances referred to in subsection (1) [hate speech and discrimination] commits an offense and shall be liable on conviction to a fine […]"*

- In Japan the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders Act No. 37 of 2001 limits the extension of liability to ISPs.

- In Egypt media law governs the liability of intermediaries.

  Art. 195 of the Criminal Code:
  "Subject to the criminal liability, in relation to the author of the text or the designer of the drawing, or such other representation methods, the chief editor of the paper or the editor in charge of the section wherein the, publication took place, if there is not chief editor in his quality of original doer of the crimes that were committed by his paper.
  However, he shall be exempted from the criminal liability:
  1. If he establishes that the publication took place without his knowledge, and from the beginning of the investigation he submits all the information and papers he has, in order to assist in knowing the person responsible for publication.
  2. Or if during the investigation he directs about the perpetrator of the crime, and submits all information and papers he has in order to establish his responsibility, and proves in addition that if he had not published he would have exposed himself to losing his position in the newspaper, or to another serious damage."

- Art. 196 of the Criminal Code:
  "In the cases where the inscription, drawing, pictures, photos, symbols, or other methods of representation that were used in committing the crime, have been published abroad, and in all cases where it is not possible to know and recognized the perpetrator of the crime, the printer importers shall be punished in their quality of original perpetrators."

- Art. 197 of the Criminal Code:
  "No one, in order to evade the criminal responsibility from what is prescribed in the previous Articles, shall be accepted to give a justification or provide an excuse that the inscriptions, drawings, pictures, photos, symbols, or other methods of representation have been communicated or translated from publications issued in Egypt or abroad, or that they are no more than a repetition of rumors or stories flow third parties."

- The "Brazilian Internet Bill of Rights," Federal Law no. 12.965 of 23 April 2014 introduces a liability exemption for Internet connection providers (Art. 18) and the application of a safe harbor doctrine for other Internet application providers (Art. 19).

- In Poland according to Art. 12 of the Act of 18 July 2002 on Providing Services by Electronic Means:

According to Art. 14:
"1. The responsibility for the stored data shall not be borne by the person, who, making the resources of a teleinformation system available for the purpose of the data storage by a service recipient, is not aware of unlawful nature of the data or the activity related to them, and in case of having been informed or having received a message on unlawful nature of the data or the activity related to them, makes immediately the access to the data impossible."

- In New Zealand, Section 124 of the Films, Videos, and Publications Classification Act of 1993 and amended in 2005 reads:

  "(1) Every person commits an offence against this Act who does any act mentioned in section 123 (1), knowing or having reasonable cause to believe that the publication is objectionable.

  Furthermore, offenses under the Human Rights Act may also engage.

  However, it must be noted that Section 21 of the Defamation Act 1992 provides for a legal exemption for ISPs in case of innocent dissemination:

  "In any proceedings for defamation against any person who has published the matter that is the subject of the proceedings solely in the capacity of, or as the employee or agent of, a processor or a distributor, it is a defense if that person alleges and proves—
  a) That that person did not know that the matter contained the material that is alleged to be defamatory; and
  b) That that person did not know that the matter was of a character likely to contain material of a defamatory nature; and
  c) That that person's lack of knowledge was not due to any negligence on that person's part."

- In China according to Art. 286-1 of the criminal code (9th amendment, 2015):

  "In any of the following circumstances where network service providers do not perform information network security management duties as provided by law or administrative regulations, and upon being ordered by the oversight and management department to adopt rectification measures but refusing to make corrections, the sentence is up to three years imprisonment, short-term detention or controlled release, and/or a fine:
  (1) Where it results in the transmission of a large volume of unlawful information;
  (2) Where it results in disclosure or user information causing serious consequences;
  (3) Where it results in the destruction of evidence in a criminal case and the circumstances are serious;
  (4) There are other serious circumstances.

  In addition, Art. 84 of the Counter-Terrorism Law (2015) provides that: *"In any of the following circumstances, the competent departments shall fine telecommunications operators or internet service providers (...)"*

- According to Art. 1.109 of the Argentine Civil Code, *"Any person performing an act, which through his fault or* ***negligence*** *causes damage to another, is obliged to repair the damage. This obligation is governed by the same provisions to which the offenses of the civil law are subject."* [the author's emphasis].

- Nigeria provides for a limited liability with regard to intermediaries. Art. 11 of the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission pursuant to Section 70(2) of the Nigerian Communications Act of 2003 provides for different scenarios:

  "(a) Acting as Mere Conduit

  ISPs shall not be liable for the content of any Internet service transmission by a user of the service or for providing access to such content by other users (…).

  (v) acts without delay to remove or disable access to the information on receipt of any takedown notice."

- In the United Arab Emirates, Art. 39 of the Federal Decree-law no. (5) of 2012 on Combating Cybercrimes reads:

  "Shall be punished by imprisonment and a fine or any of these two penalties any owner or operator of a website or computer network who deliberately and knowingly saves or makes available any illicit content or if he fails to remove or blocks access to this illicit content within the period determined in the written notice addressed by the competent authorities indicating the illegal content and being available on the website or the computer network."

- In France, a liability regime applies to ISPs. According to Art. 6.I of Law No. 2004-575 for the Confidence in the Digital economy, ISPs can be held liable if, once they are aware of the illegal nature of content, they do not remove it promptly. The Cybercrime Act contains provisions on intermediary liability:

  Article 39 - Monitoring obligation:

  "(1) When providing services in accordance with the provisions of this Part, a service provider shall not
  (a) Monitor the data which the service provider transmits or stores; or
  (b) Actively seek facts or circumstances indicating an unlawful activity.
  (2) The Minister may prescribe procedures for service providers to-
  (a) Inform the competent authority of alleged illegal Activities undertaken or information provided by Recipients of their service; and
  (b) Avail competent authorities, at their request, with information enabling the identification of recipients of their service.
  (3) A service provider shall not be liable for disclosure, by a third party, of data lawfully made available to the third party upon proving that-
  (a) The third party acted without the knowledge of the service provider; or
  (b) The service provider exercised due care and skill to prevent the disclosure of such data.

  (4) Where a service provider has knowledge of illegal information, or activity he shall -
  (a) Remove the information in the computer system within the service providers control;
  (b) Suspend or terminate services in respect of that information or activity; and(c) Notify appropriate law enforcement authority of the illegal activity or information, relevant facts and the identity of the person for whom the service provider is supplying services in respect of the information.

Article 43 - Hyperlink provider:

"A hyperlink provider is not liable for the information linked provided that the hyperlink provider:
(a) Immediately removes or disables access to the information after receiving an order to do so from the relevant authority; and
(b) Upon becoming aware of the specific illegal information stored by other ways than an order from a public authority, immediately informs relevant authority.

- In the Russian Federation the Federal Law No. 126-FZ of 7 July 2003 on Communications provides in its Chapter 11. Responsibility for Violating the Legislation of the Russian Federation in the Sphere of Communications, Article 68.

- o -

In addition to the legal assessment of ISP liability for radicalizing content a growing number of policy statements have been made around the world.

A call for the introduction of a general accountability standard for content has been gathering increasing traction in the wake of terrorist use of the net. An example is the Minister of Justice of Israel[187]: *"We need to acknowledge the fact that some very severe crimes are being conducted and incited through those platforms — such that there should be some measure of accountability"*.

The United Kingdom Home Affairs Committee House of Commons[188] and the Home Affairs Select Committee have accused Internet giants such as Google of "passing the buck" and allowing websites to become "recruiting platforms for terrorism":

Committee chair Keith VA MP described online forums, message boards, and social media platforms as "the lifeblood of Daech," also known as Islamic State (IS, formerly ISIS/ISIL).

The parliamentary inquiry into tackling radicalization said that social media platforms have become the "vehicle of choice in spreading propaganda."

Vaz said: "Huge corporations like Google, Facebook and Twitter, with their billion-dollar incomes, are consciously failing to tackle this threat and passing the buck by hiding behind

187 Large Internet companies and content providers such as Facebook, Google and Twitter should be held accountable for criminal activity on their platforms, Justice Minister Ayelet Shaked said at a conference in Tel Aviv.
"*We need to acknowledge the fact that some very severe crimes are being conducted and incited through those platforms - such that there should be some measure of accountability*" regarding the illegal activities and content that is published through their services, declared Shaked, who said these large Internet companies were an "area of focus" for her ministry. Source: Solomon, S. (2016): "Google, Facebook must be held accountable for criminal content – justice minister", *The Times of Israel*.

188 "*Social media companies are consciously failing to combat the use of their sites to promote terrorism and killings. Networks like Facebook, Twitter and YouTube are the vehicle of choice in spreading propaganda and they have become the recruiting platforms for terrorism. They must accept that the hundreds of millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of responsibility and ownership for the impact that extremist material on their sites is having. […] Manuals for terrorists and extremists should be removed from the Internet. It is therefore alarming that these companies have teams of only a few hundred employees to monitor networks of billions of accounts and that Twitter does not even proactively report extremist content to law enforcement agencies. These companies are hiding behind their supranational legal status to pass the parcel of responsibility and refusing to act responsibly in case they damage their brands. If they continue to fail to tackle this issue and allow their platforms to become the 'Wild West' of the Internet, then it will erode their reputation as responsible operators."*

their supranational legal status, despite knowing that their sites are being used by the instigators of terror."

The Labour MP added: "The company's' failure to tackle this threat has left some parts of the Internet Ungoverned, Unregulated and lawless."

MPs want the government to introduce measures that would force web providers to cooperate with the UK authorities by promptly investigating reported hate speech sites and closing them down, or provide an explanation for why they are still online. [189]

In France, the judge who ensures oversight over administrative blocking orders condenses his findings as follows in his report "Removal of content, blocking and dereferencing related to terrorism" from march 11, 2015 to February 29, 2016:

"2. Passive operators facing the threat

The mission interviewed representatives from Facebook, Twitter, Google and Dailymotion. In February 2016, Twitter has publicly revealed that since the middle of 2015, the company had suspended 125,000 terrorists accounts or affiliates relating mainly to Daech.

Beyond this initiative, however, it became very clear to the rapporteur that the major social web platforms are not sufficiently proactive in the fight against Daech propaganda.

Although social networks are defending themselves to have "a religion of the First Amendment of the US Constitution", they interpret extensively the freedom of expression or the right to information, which can lead them to not delete Internet content advocating terrorism".[190] [the author's translation]

From a legal point of view the main question seems to be whether ISPs have developed into something more and different than simple Service Providers in the sense of "Access Providers" or "Mere Conduits".

Indeed, the Right to Forgotten Judgment of the European Court of Justice of May 13th 2014 provided a detailed and extensive analysis of the Data Privacy Directive 1995/46 for the purposes of determining

---

189 RT (2016): "Facebook, Twitter & YouTube 'consciously failing' to tackle online extremism – MPs". Available at: https://www.rt.com/uk/357148-online-extremism-social-media/ [Accessed 28/09/2016]:
Twitter said it has suspended 235,000 accounts for promoting terrorism in the six months since February, while Facebook insisted it has dealt "swiftly and robustly" with reports of terrorist-related content.
Google told the committee it had removed more than 14 million videos from across the world in 2014 connected to all types of abuse.
Facebook director of policy Simon Milner said: *"As I made clear in my evidence session, terrorists and the support of terrorist activity are not allowed on Facebook and we deal swiftly and robustly with reports of terrorism-related content."*
"In the rare instances that we identify accounts or material as terrorist, we'll also look for and remove relevant associated accounts and content. Online extremism can only be tackled with a strong partnership between policymakers, civil society, academia and companies."
A YouTube spokesman said: *"We remove content that incites violence, terminate accounts run by terrorist organizations and respond to legal requests to remove content that breaks UK law. We'll continue to work with government and law enforcement authorities to explore what more can be done to tackle radicalization."*

190 Linden, A. (2016), Qualified Person's report on measures to withdraw, block and declassify unlawful websites through administrative channels. Paris, France: CNIL.

whether a search engine activity should be viewed as "data processing" as opposed to a mere conduit activity.[191]

The decision of the Court was affirmative in this regard and it may indeed be argued that the services provided by such companies (as opposed to telecoms or quasi-telecoms) can no longer be qualified as "mere conduits". They catalogue, process and organize information in a way which may cause them to forfeit their status as "mere conduits". Indeed, the European Union Commission's investigation into Google's competition practices including its prioritizing of search results arguably in its own economic interest may be taken as further evidence of a selection or "processing" function performed by search engines.[192]

The same may be said for Facebook which performs an organizes third party content.

It may actually be useful henceforth to distinguish between "Internet Access Providers" ("IAP"), "Internet Service Providers "("ISP") and "Internet Content Providers" ("ICP").

ISPs are engaged in activities that are increasingly moving towards the middle of the spectrum where their transmission and communication services converge with processing and "editing functions", (irrespective of the above suggested redefinition of "ISPs" we shall continue to employ the term throughout this Report in accordance with the definition applied supra in footnote 4 on page 6.

Specific content related problems may be solved in the future on the basis of the concrete facts surrounding the case leaving out the somewhat outdated reference to a particular category or status which would determine accountability.

By way of preliminary conclusion international treaty regulations, case law from Human Rights Courts and Tribunals and national law allow for (1) delegation of public services including those forming part of the state's core prerogatives (*i.e.* defence and protection of its citizens) and (2) a certain imposition of private sector liability for violations of duties incumbent upon government, but delegated to those private entities. Liability may also conceivably be grounded in media law or derivates ("publisher"), product liability, complicity, diligence obligations, knowledge (notice based, actual or construed awareness) or disqualification of "mere conduit" status. Such liability would arguably apply to radicalizing content.

4.e. State Responsibility for Private Actors

Having analyzed the basis and extent of ISP liability we must now turn to state responsibility. To what extent may a state be liable under Public International Law for radicalizing content originating from its territory?

By "originating" is meant either authored or originally posted or disseminated via the services of an ISP subject to the jurisdiction and regulatory authority of that State (see above under responsibility of State of Origin).

---

191 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González* [2014], Case C-131/12, Court of Justice of the European Union, Grand Chamber

192 European Commission Press release (2016): "Antitrust: Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules". Available at: http://europa.eu/rapid/press-release_IP-16-2532_en.htm [Accessed on 27 September 2016].

One of the solutions to jurisdictional conflicts may be increased state accountability for the acts of private individuals and corporations under their control. This would cause private acts indirectly to be subject to international law and state accountability.

The accepted theory under international law is that state responsibility for private actors is conditioned upon the state's failure to exercise sufficient control over acts that originate from or transit its territory.[193]

An example of State responsibility is the case involving the US diplomatic and consular staff in Tehran. According to the International Court of Justice (judgement of 24 May 1980)[194] Iran had violated its obligations under International Law notwithstanding the fact that the hostage taking had not been executed by agents of the government, but because of the government's failure to expedite efficient and adequate control:

The Court is therefore led to conclude that on 4 November 1979 the Iranian authorities were fully aware of their obligations Under the conventions in force, and also of the urgent need for action on their part, that they had the means at their disposal to perform their obligations, but that they completely failed to do so.

This theory of State Responsibility for private actors may under certain circumstances be extended to cover a State's failure to take adequate steps to efficiently meet its obligations under International Law to fight terrorism and prosecute authors and it could also eventually apply to a state's failure to suppress radicalising content originating from its territory.

Foreign states are generally immune from being sued in other jurisdictions. Limitations on such immunity have however been imposed in several countries relative to State support of terrorism. An example is the Canadian State Immunity Act (1985), Art. 6.1.[195] This Act combined with the Justice for Victims of Terrorism Act of 2012 makes it possible for foreign judgments against such a State to be enforced in Canada.[196]

The United Nations Guiding Principles on Business and Human Rights reconfirm the tenet of State responsibility.[197]:

> *"While states are not responsible for human rights abuse by private actors, they may be in breach of their international human rights law obligations when they fail to take proper steps to prevent or punish abuses by the private sector."*

---

193 Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001), International Law Commission, Supplement No. 10 (A/56/10), chp.IV.E.1.

194 *United States of America v. Iran* [1980], Case Concerning United States Diplomate and Consular Staff in Tehran (ICJ).

195 State Immunity Act, R.S.C., 1985, c. S-18: *"A foreign State that is set out on the list referred to in subsection 2 is not immune from the jurisdiction of a court in proceedings against it for support to terrorism…"*

196 Justice for Victims of Terrorism Act, S.C. 2012, c. 1, s. 2. Available at: http://laws-lois.justice.gc.ca/eng/acts/j-2.5/page-1.html. [Accessed 30 September 2016].

197 Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (2011), Human Rights Council (A/HRC/17/31). Available at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf [Accessed 30 September 2016].

The United Nations General Assembly points out that States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies (Resolution 55/63, 4 December 2000).[198]

In the United States the "Justice Against Sponsors of Terrorism Act" (JASTA)[199] was passed by both the House and the Senate, but was vetoed by the President given its impact on foreign policy (on 23 September 2016). The latest development has however been Congress voting to override the President's veto insisting that States that sponsor terrorism should be brought to justice (even though "sponsoring" does not equate to the commission of the terrorist act by non-government agents).[200]

The Tallinn Manual also imposes such duties on States in the field of Cyber Warfare: *"Rule 15. A State should not knowingly allow cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States".* [201]

It may be argued that states have a responsibility under international law to ensure that violations (by non-state actors subject to their jurisdiction) of human rights in other states be brought to an end. This obligation may place the "Country of Origin" theory in a new light as far as radicalizing content is concerned.

---

198 General Assembly Resolution, Combating the criminal misuse of information technologies (A/RES/55/63).
See also: The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict (17 September 2008):
"6. Although entering into contractual relations does not in itself engage the responsibility of Contracting States, the latter are responsible for violations of international humanitarian law, human rights law, or other rules of international law committed by PMSCs or their personnel where such violations are attributable to the Contracting State, *[…]"*
"Obligation to protect human rights
[…] States have an obligation to take measures to prevent misconduct by PMSCs and to assist persons harmed by such misconduct. This also includes misconduct by PMSCs against their own employees.
It would be unrealistic, however, to expect States to prevent all and any possible harm caused by private companies. Instead, States are expected to exercise due diligence, that is, to do what can reasonably be expected to prevent or minimize harm."

199 S.2040 - Justice Against Sponsors of Terrorism Act, 114th Congress (2015-2016).
RESPONSIBILITY OF FOREIGN STATES - A foreign state shall not be immune from the jurisdiction of the courts of the United States in any case in which money damages are sought against a foreign state for physical injury to person or property or death occurring in the United States and caused by—
"(1) an act of international terrorism in the United States; and
"(2) a tortious act or acts of the foreign state, or of any official, employee, or agent of that foreign state while acting within the scope of his or her office, employment, or agency, regardless where the tortious act or acts of the foreign state occurred.

SEC. 4. AIDING AND ABETTING LIABILITY FOR CIVIL ACTIONS REGARDING TERRORIST ACTS.
"(2) LIABILITY.—In an action under subsection (a) for an injury arising from an act of international terrorism committed, planned, or authorized by an organization that had been designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189), as of the date on which such act of international terrorism was committed, planned, or authorized, liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism.".

200 Steinhauer J.; Mazzetti M.; Hirschfeld Davis J. (2016): "Congress Votes to Override Obama Veto on 9/11 Victims Bill. Available at: http://www.nytimes.com/2016/09/29/us/politics/senate-votes-to-override-obama-veto-on-9-11-victims-bill.html?_r=0 [Accessed 30 September 2016].

201 Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Cambridge University Press, is the product of international law scholars and practitioners. *"It addresses topics including sovereignty and State responsibility"*. The Manuel with later extensions was prepared at the invitation of the NATO Cooperative Cyber Defence Center of Excellence.

Section 5: Filtering, Blocking, Encryption and Counter-Narrative

Ensuring the legality of orders to block, filter or take down content in terms of procedure, enforcement, judicial oversight and appeal is critical to any regulation of content and arguably in particular with regard to radicalizing content given the risks of abuse/repression.

Regulation of radicalizing content is currently actively pursued in several countries and often as a result of concerted action:

Europol's EU Internet Referral Unit has disclosed below statistics covering the period of 1 July 2015 – 1 July 2016:

Total content assessed: 11 050
Proposals for referral: 9787
Content removed by online service providers: 8949
Success rate: 91.40%
Platforms identified: 70
Platforms referred to: 31[202]

In the United Kingdom, the government's Counter Terrorism Internet Referral Unit (CTIRU) [203], set up in 2010, has removed more than 49,000 pieces of content that "encourages or glorifies acts of terrorism", 30,000 of which were removed since December 2013. [204]

London police take down over 1,000 extremist web pages every week. According to London's police chief 300,000 pages have been removed in the past 18 months. Now most of that is to do with terrorist type posting but it's not only that. It's also extremes on both sides. There are also right wing sites.

In Germany, the State media supervisory authorities examined ca. 30,250 websites in 2015. Of those, 935 were considered illegal incitements to hatred or illicit use of symbols of "Unconstitutional Organizations" (*e.g.* swastika). Given that almost all content was hosted on servers outside Germany the method of choice was that of notifying the ISPs in question (*e.g.* Facebook) through privileged communication channels.

In 2014, jugendschutz.net achieved removal of 58% of all hate speech offences. 95% of the successful cases were obtained by notifying the provider. [205]

---

202 EU Internet Referral Unit - Year One Report Highlights (2016), Europol.
The EU Internet Referral Unit (EU IRU) made over 500 referrals in the first 16 weeks after it was established in July 2015, of which 90% were successfully removed.

203 In 2010 the Counter Terrorism Internet Referral Unit (CTIRU) was launched within the Association of Chief Police Officers (ACPO) in the UK. It proactively scans the web for radicalizing content that promotes or glorifies terrorism, as well as acting on referrals from citizens and public bodies. Flagged sites' content is reviewed by specialists and where material is deemed to breach UK law, CTIRU seeks to remove the site from the Internet in collaboration with Internet service providers.

204 Source: Country answers to The Questionnaire - Annex 1.

205 Source: Country answers to The Questionnaire - Annex 1. Jugendschutz.net is a platform on which any individual can report violations of youth protection laws (http://www.jugendschutz.net/en/hotline/).

At the request of the French government, Facebook erased 32,000 posts linked to the carnage of November 13th 2015.[206]

- o -

Blocking access to content is a very sensitive issue. It may border on censorship (or even cross the line).

The risk involved in blocking, filtering and other content restricting technologies is often referred to as "Collateral Filtering".[207]

Collateral filtering may block entire websites, IP addresses, or domains as opposed to the specific radicalizing content identified.

Before turning to the conditions that must be met in order to ensure the legality of blocking orders we need to understand the basic functioning of blocking/filtering technologies:

There are essentially three methods used for website blocking: IP blocking, DNS blocking, and URL blocking.[208]

IP Blocking

ISPs can modify their network settings so that users are blocked from access to certain IP addresses.

IP addresses can however easily be changed and furthermore IP blocking can include perfectly uncontentious websites hosted at the same IP address.

DNS Blocking

The Domain Name System is often described as the telephone directory of the Internet.

Just like IP blocking DNS blocking may cause over-blocking as a single domain may host many websites through website extensions.[209]

URL Blocking

URL blocking involves examining both "metadata" (the source and destination IP addresses) and the contents. This is done through Deep Packet Inspection (DPI). URL blocking is content targeted and generally considered least critical with regard to its collateral scope. At the same time Deep Packet Inspection raises privacy concerns.

---

206 Breindl, Y. (2013): "Internet content regulation in liberal democracies". A literature review. *Institute of Political Science*, Georg-August-Universität Göttingen: "It was the largest amount of "restricted content" by country in Facebook's twice-yearly report on government requests for access, ahead of India — which had 14,971 posts restricted over legal requests in July-December 2015 "as alleged anti-religious and hate speech that could cause unrest and disharmony within India" — and Turkey, which had 2,078 posts removed during that same period for "a range of offenses including personal rights violations, personal privacy, and defamation of Ataturk," the first president of modern Turkey.

207 Take downs of illicit content entails less of a risk of "collateral effects" than blocking. Source: Comparative Study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe (2015), 14-067. Lausanne, Switzerland: Swiss Institute of Comparative Law, Excerpt pp. 773-800.

208 Cory, N. (2016): "How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet"", *Information Technology & Innovation Foundation*.

209 However, this risk can be addressed by implementing DNS blocking at the subdomain level.

Content filtering / Dynamic filtering

This method runs content automatically against a list of keywords (possibly provided by government black lists), content filtering demands important resources since its data streams will have to be reconfigured if the keywords on the list are split into isolated Packets.

Proxy filtering

This method involves proxy servers which will allow accurate blocking of URLs with little risk of collateral blocking. Proxy filtering is however considered economically excessive which brings us to **hybrid filtering.**

Hybrid Filtering combines the features of proxy filtering and IP filtering. It works as a 2-step approach: first it screens against address for those that match the list a second verification takes place time at the webpages as such.

More refined technology and decentralized architecture will must probably allow further cost reduction and accuracy.

Hiding

In addition to blocking in its various forms radicalizing content may also be "removed" by a technique known as "Hiding". This technique causes search engines to refer radicalizing content to the bottom of search results (or even completely filter out the URLs from its lists).

On the legality of blocking or similar access restricting orders:

The most efficient method of implementing any of the above mechanisms would be by adopting a general monitoring program

In the *SABAM* case the European Court of Justice[210] held however that ISPs could not be required to filter access to websites that contain copyright infringing material by way of such a broad and indiscriminate monitoring approach. Such obligations must be specifically targeted against the illicit content in question (see supra p.86).

The European Court of Justice in its judgment in the case *UPC Telekabel v. Constantin Film*[211] describes the general conditions that must be met by injunctions:

> *The fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an Internet service provider from allowing its customers access to a website placing protected subject-matter online without the agreement of the rightholders when that injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive Internet users of the possibility of lawfully accessing the information available and*

---

210 *SABAM v. Netlog* [2012], Case C-360/10, Court of Justice of the European Union, Third Chamber.

211 *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH* [2014], Case C-314/12, Court of Justice of the European Union Fourth Chamber.

(ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging Internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish.

The overarching conditions of legality are summarized as follows by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (16 May 2011):

States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression, […] *Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an Unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body.*

The Yildirim-case[212] before the European Court of Human Rights reaffirmed those principles and stated that restrictions to information must be grounded in law and must allow for effective appeal mechanisms: "*a restriction on access to a source of information was only compatible with the Convention if a strict legal framework was in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses*."[213]

The European Union support these views and warns against "collateral effects":

"[…] incorrect blocking of legitimate material represents an economic impact. Collateral blocking may have serious legal and economic implications.

---

212 *Ahmet Yıldırım v. Turkey,* 3111/10 (European Court of Human Rights 2012).
Wholesale blocking of access, without a legal basis, to the entire YouTube website, of which the applicants were active users, because of ten pages infringing the prohibition on insulting the memory of Atatürk: violation of Article 10.
Interim court order incidentally blocking access to host and third-party websites (all Google Sites) in addition to the website concerned by proceedings (blocked because of its illegal content): violation of Article 10.

213 Brown, I. (2010): "Internet Self-Regulation and Fundamental Rights", University of Oxford - Oxford Internet Institute, Index on Censorship Vol. 1.
"The Council of Europe has belatedly recommended that blocking should only take place if it "concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body" […] the European Parliament, the new EU Telecoms Package includes specific protection for users' rights, stating:
"Measures taken by Member States regarding end-users access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons… these measures…may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards… including effective judicial protection and due process."

Human rights impact: "Collateral blocking, referred to above, may not only cause serious economic losses but necessarily involves a violation of the freedom of speech.
First of all, dynamic filtering clearly limits freedom of speech and access to information because it automates censorship […]. Freedom of speech and access to information would be subject to automated judgement calls determined by software designers. Under this system, a separate assessment of the necessity and proportionality of blocking a specific content could not take place."[214]

Art. 19 of the International Covenant on Civil and Political Rights explicitly states that the exercise of the right carries with it ''special duties and responsibilities'' and that it ''may therefore be subject to certain restrictions.'' Art. 20 of the Covenant creates an obligation on states to prohibit propaganda for war, incitement to discrimination, hostility, racial or religious hatred or violence.

Blocking or ordering of deletion of such content would not only be permitted but arguably required by the International Covenant on Civil and Political Rights.

Striking the balance and applying the appropriate blocking measures is a major challenge which is addressed in a variety of ways by different countries. The following are examples of such country specific implementations of "blocking laws and regulations" (based on the country Survey).[215]

In Denmark the police can impound a web site (pursuant to a court order).

In the United Kingdom and Tunisia take down notices and filtering are used.

In Hungary, the amendment of the Criminal Code that entered into force on 1 July 2013 introduced a new measure of rendering "*electronic data that realizes a crime permanently inaccessible.*" The main purpose of rendering data inaccessible is to remove the illegal content (delete it from the server). If such deletion is not possible, a court may order "*the temporary prevention of access to electronic data.*"

In India, suspension of ISP license may be ordered in addition to blocking.

In Australia, Australian hosted extremist material can be removed if it is found to be:

- advocating terrorist acts
- offending the standards of morality, decency and propriety
- promotion, incitement or instruction in matters of crime or violence.

Where content is not hosted in Australia and is prohibited, the Commissioner will notify the content to the suppliers of approved filters, so that access to the content using such filters is blocked. The Commissioner will also notify material found to advocate terrorist acts to the Australian Federal Police.

In addition, Section 313 of the Telecommunications Act 1997 enables Commonwealth, State and Territory government agencies to request Internet Service Providers (ISPs) to provide such help as is reasonably necessary to disrupt the operation of illegal online services by blocking access to websites. This could allow agencies to block access to a website containing terrorist propaganda.

---

214 Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on combating terrorism - Impact Assessment [COM (2007) 650 final - SEC (2007) 1425].

215 Source: Country answers to The Questionnaire - Annex 1.

In Germany, take down notices, blocking with a right of response (where hate speech appears in a journalistic article the persons affected have a right to reply) are used.

Under the Trade Regulation Act, the competent authority can order an enterprise to terminate operations under certain conditions and suspend the ISP license in extreme cases.

In the Seychelles, confiscation of devices may be ordered.

In Slovakia, in Act no 46/1993 Coll. On Slovak information service, section 16a there is stated: *a legal or natural person who is intermediary of a website, or who provides domain name is required according to a court order which is issued on the proposal of Slovak information service in accordance with paragraph 3 to prevent service of the web site or access to a domain name if the use of such web site or the domain name occurs supporting the dissemination of ideas that support or promote terrorism, political or religious extremism, extremism manifested in a violent manner or harmful sectarian groupings*."

In Finland, certain blocking orders may expire after a certain period of time unless criminal charges or civil action is brought in relation to the content.

In Sweden, media protected by the Fundamental Law on Freedom of Expression, *inter alia* part of the Internet the administration is prohibited from restricting freedom of speech in ways that are not prescribed in the Fundamental Law. Blocking and filtering are not prescribed in the Fundamental Law on Freedom of Expression.

Judges or law enforcement agencies cannot act preventively. In order to act there must be an ongoing criminal investigation regarding a particular crime. The coercive measures available to law enforcement agencies are seizure and search warrant. Such measures, however, cannot be taken against a particular homepage, but are used primarily to seize hard drives, servers and other material to get access to electronically stored information

In Iraq, take down notices, filtering and blocking are used.

Take down notices, blocking, refusal of access and link deletion are authorized in Spain.

Under Section 83.223 of the Criminal Code of Canada, a judge who is satisfied by information on oath that there are reasonable grounds to believe that there is material — that is terrorist propaganda or computer data that makes terrorist propaganda available — stored on and made available to the public through a computer system that is within the court's jurisdiction, may order the computer system's custodian to ensure that the material is no longer stored on and made available through the computer system.

The following laws are relevant to take-down notices in Singapore:

Section 10 of the Sedition Act. The court may prohibit the issuing and circulation of seditious publications.

For convictions under Section 298 (uttering words etc., with deliberate intent to wound the racial or religious feelings of any person) of the Penal Code, the court may issue take down orders against the offending material.

In Belgium, filtering, take-down notices and blocking are authorized.

In Poland, the new Anti-Terrorism Law gives the Director of the Internal Security Agency authority to order the immediate blocking of specific websites with no prior judicial authorization. After a five-day period, a court must confirm that the ISA's order to block the website was justified.

In New-Zealand, filtering and blocking are measures taken by the authorities but only with regards to digital child exploitation. ISPs voluntarily adopt the system.

Under Art. 12 of the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission pursuant to Section 70(2) of the Nigerian Communications Act of 2003, *"ISPs must have in place a procedure for receiving and promptly responding to content related complaints, including any notice to withdraw or disable access to identified content issued by the Commission or other legal authority ("takedown notices")"*. Nigeria also conducts filtering and blocking.

In the United Arab States, Art. 41 of the Federal Decree-law N°5 of 2012 on Combating Cybercrimes reads:

"Without prejudice to the right of bona fide third-party, shall be ordered, in all instances, the confiscation of devices, programs or means used in the commission of any of the crimes specified in this Decree-Law or the money accrued thereof, or deletion of the information and statements or their killing, as to the closure of the domain or site in which any of these crimes is committed whether permanent closure or for a specified period as determined by court."

In France, the Decree N°2015-125 of 5 February 2015 allows the French government to block websites accused of promoting terrorism without a court order. ISPs must take down offending websites within 24 hours from receipt of the government order.

The Russian telecommunications regulator Roskomnadzor has the authority to order content to be taken down, if it considers an online article or post to be extremist in nature, offensive to religious believers or to call into question the integrity of Russian territory.

In Germany, Austria, the Netherlands, the United Kingdom, Ireland, Poland, the Czech Republic and Switzerland, Finland, France, Hungary, Portugal, the Russian Federation, Spain and Turkey blocking is authorized by law.[216]

In the European Union voluntary blocking may violate the General Data Protection Regulation.[217]

The concern is that voluntary blocking may not properly take into account due process and appeal remedies.

- o –

It may be concluded that whilst blocking and similar measures are applied worldwide there are important legal differences in terms of procedure (court order, administrative decision), judicial oversight, legal basis, time limitation and remedies.[218]

---

216 Most countries have procedures in place to ensure that human rights (freedom of speech and religion and right to privacy in particular) are not violated in the process of delivering and enforcing blocking orders. The Country Survey provides further information under question number 13.

217 Recitals 13 and 15 of the Regulation.

218 For further details, see annex 1 "Country Questionnaire" point 11

Harmonization should be attained.

The African Declaration on Internet Rights and Freedoms (2015) provides guidelines to such harmonization:

Content blocking, filtering, removal and other technical or legal limits on access to content constitute serious restrictions on freedom of expression and can only be justified if they strictly comply with international human rights law as reiterated in Article 3 of this Declaration. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

Section 6: Policy Recommendations

We have seen how freedom of speech protection offline and online is aligned and in particular that the **general** exceptions to free speech as embodied in the International Covenant on Civil and Political Rights Art. 19.3 and Art. 17 in the European Convention for the Protection of Human Rights and Fundamental Freedoms to apply equally online.

We have furthermore seen that the legitimacy of restricting speech content in various **specific** fields is broadly recognized.

Applying specific restrictions to "radicalizing content" meets the above standards and is consistent with International Human Rights Law.

We have dealt with the subject of jurisdiction/extraterritoriality and the principle of legality mandating proper definition as a pre-condition for such specific restrictions. The Report has also covered theories of State liability based on a country of origin principle (the territory from where radicalizing content originates or through whose borders it transits).

We have analyzed private sector duties and obligations by reference to different theories (least cost avoider, outsourcing/delegation/concession or license-based analogies, the pursuit of efficiency and recognition of necessity as a consequence of private sector control of infrastructure and technology).

Finally, we have described liability standards derived from complicity, due diligence, bad faith and product liability theories.

We shall now turn to the policy recommendations.

In light of the above and on the basis of our analysis of current legislation in the 32 countries surveyed, international treaties and resolutions, case law, Non-Governmental Organizations' recommendations, news coverage, academic literature, interviews with Internet Service Providers and experts on Internet security and content regulation as well as law enforcement Officers, Judges and Ministers of Justice/Interior, the following policy recommendations have been developed for further elaboration and drafting.

Indeed, the harm of radicalizing content is portentous and its positive contribution to truth and enlightenment is undetectable.

Radicalizing content does not deserve protection. It is incompatible with the rule of law.[219] Granting freedom of speech protection to radicalizing content amounts to a negation of the value from which freedom of speech derives its justification.

> *"No liberty is made more secure by holding that its abuses are inseparable from its enjoyment* […] *The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact".* [220]

Policy Recommendation 1

It appears legitimate to prescribe certain **legal duties on ISPs** in an effort to reinforce the effectiveness of a Counter Radicalization Policy. Such duties may be justified by different theories including the least cost avoider theory and by reference to the unique technological capabilities under ISP control combined with their de facto gatekeeper role. Indeed, given the growing policy demands for ISP liability and the current legal theories that might already provide an enforceable liability standard (product liability, complicity, due diligence obligations described above under Section 1) it is increasingly necessary that ISPs receive clear legislative guidance rather than potential liability developed through concrete and not necessarily consistent case law. A general liability standard expounded as a legislative precept would however face the immediate challenge of ISP immunity under the Communications Decency Act.

Irrespective of a possible, but not likely, adaptation of the Act (on this particular point in the short term[221]) accommodating different approaches enacted in laws in other countries, it must be underscored that ISP immunity is not a Human Right.

Specific approaches include notice and take-down schemes similar to those governing copyright infringement under the Digital Millennium Copyright Act and the e-Commerce Directive.[222]

---

219 Mahoney, K. (1992); "The Canadian constitutional approach to freedom of expression in hate propaganda and pornography". Calgary, Canada: Law and Contemporary Problems, p.77-105.

220 *Terminiello v. City of Chicago* [1949], 337 U.S. 1, Justice Jackson dissenting opinion (Supreme Court of the United States). See also: Wittes, B.; Blum, G. (2015) The future of violence: Robots and germs, hackers and drones - Confronting the new age of threat. Gloucestershire, United Kingdom: Amberley Publishing.

221 In July 2013, some 50 Attorneys General in the United States urged Congress to amend the Communication Decency Act Article 250 c in order to allow prosecution of unlawful content. The initiative failed. Source: Kumar Doran, A.; Grant, J. (2013): "State Attorneys General Propose Dramatic Amendment to Section 230". Available at: http://www.medialawmonitor.com/2013/08/state-attorneys-general-propose-%E2%80%A8dramatic-amendment-to-section-230/ [Accessed 30 September 2016].
A recent development in the United States may open up for a possible fissure in the Communication Decency Act immunity (*Hassell v. Bird* [2013], No. CGC-13-530525 (Cal. Sup. Ct.)).
The case related to defamatory postings on Yelp. The plaintiff obtained a judgment against the author of the defamatory content and an injunction against Yelp to remove the posting in spite of Communication Decency Act immunity. Yelp appealed the judgement before the California Court of Appeals which confirmed the judgment (*Hassell v. Bird* [2016], 247 Cal. App. 4th 1336, Court of Appeal Case No. A143233). Yelp then appealed to the Supreme Court of California which agreed to review the case on 21 September 2016. Source: Thanawala, S. (2016): "California Supreme Court to consider suit over Yelp review". Available at: http://www.usnews.com/news/business/articles/2016-09-21/california-supreme-court-to-consider-suit-over-yelp-review [Accessed 27 September 2016].

222 See PUBLIC LAW 105–304—OCT. 28, 1998, Digital Millennium Copyright Act, § 512 - ''(g) REPLACEMENT OF REMOVED OR DISABLED MATERIAL AND LIMITATION ON OTHER LIABILITY"; Directive2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directive on electronic commerce), Art. 21.

Such schemes automatically entail ISP liability (the Digital Millennium Copyright Act however also provides for liability against actors who make take-down requests in bad faith).

Similar procedures could obligate ISPs to remove radicalizing content upon notice lest they forfeit immunity.

It makes little sense that personal creativity (intellectual property rights) should deserve better protection than personal integrity and that an ISP engages its liability for infringements of the former, but not the latter.

Third-party liability (*i.e*. ISP liability) is justified when a party may relatively effortlessly redress or prevent harm without exposing itself to disproportionate consequences.

ISP duties may be **passive** (implementation of "blacklists" provided by government agencies, Non-Governmental Organizations or user generated notices/flagging) or **active** (employment of content identifying software possibly with Deep Packet Inspection capability).

Any imposition of content regulation duties must meet the standards set by International Human Rights Law and notably with regard to duties that include **active** obligations given the corollary of ISP accountability. ISP duties must be predicated upon an operable definition (or at least workable guidance) of the illicit content in question.

Given the complexity of not only delimitation of illicit content, but also of technological potential such legal obligations should only be promulgated after careful consultation with industry stakeholders.

Passive obligations with implied accountability must be contingent upon clear and practical notice/flagging procedures.

The recommendations of the UK Home Affairs Committee House of Commons should be implemented[223]:

In addition to authors, editors and publishers of content, ISPs should be given the opportunity – in their own right - to challenge "block lists", administrative or judicial orders and user or Non-Governmental Organization generated notices/flagging.

---

[223] Radicalization: the counter-narrative and identifying the tipping point (2016), Eighth Report of Session 2016–17, House of Commons - Home Affairs Committee:
"The Internet has a huge impact in contributing to individuals turning to extremism, hatred and murder. Social media companies are consciously failing to combat the use of their sites to promote terrorism and killings. Networks like Facebook, Twitter and YouTube are the vehicle of choice in spreading propaganda and they have become the recruiting platforms for terrorism. They must accept that the hundreds of millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of responsibility and ownership for the impact that extremist material on their sites is having. There must be a zero tolerance approach to online extremism, including enticement to join extremist groups or commit attacks of terror and any glorification of such activities. Manuals for terrorists and extremists should be removed from the Internet. It is therefore alarming that these companies have teams of only a few hundred employees to monitor networks of billions of accounts and that Twitter does not even proactively report extremist content to law enforcement agencies. These companies are hiding behind their supranational legal status to pass the parcel of responsibility and refusing to act responsibly in case they damage their brands. If they continue to fail to tackle this issue and allow their platforms to become the 'Wild West' of the Internet, then it will erode their reputation as responsible operators […].
We do not see why the success of the Internet Watch Foundation cannot be replicated in the area of countering online extremism.
The Government must also require the companies to be transparent about their actions on online extremism; instead of the piecemeal approach we currently have, they should all publish quarterly statistics showing how many sites and accounts they have taken down and for what reason. Facebook and Twitter should implement a trusted flagger system similar to Google's and all social media companies must be more willing to give such trusted status to smaller community organisations, thereby empowering them in the fight against extremism. In short, what cannot appear legally in the print or broadcast media, namely inciting hatred and terrorism, should not be allowed to appear on social media"

Such remedies should however not suspend the obligations inherent in the "block list", orders etc. given the gravity of the likely consequences of radicalizing content.

In view of the difficulty in some cases of qualifying specific content as "radicalizing" and in recognition of the caveats expressed for instance by the German Supreme Court Judgement of 25 October 2011.[224] ISPs should not be held liable for failure to take down or block access to content unless it is obvious for a reasonable person that the challenged content is of a radicalizing nature.

In order to protect freedom of speech to the fullest extent realistically possible a fast track dispute resolution procedure or Content Qualification Procedure (CQP) should be created. Such a procedure will allow all interested parties (the government, private parties, Non-Governmental Organizations, authors, editors, ISPs and publishers of content) to obtain an authoritative qualification assessment.

As the Guiding Principles on Business and Human Rights of the United Nations Geneva 2011 read:[225]

> […] *Having effective grievance mechanisms in place is crucial in upholding the state's duty to protect and the corporate responsibility to respect. The UNGPs dictate that non-judicial mechanisms, whether state-based or independent, should be legitimate, accessible, predictable, rights-compatible, equitable, and transparent. Similarly, Company-level mechanisms are encouraged to operate through dialogue and engagement, rather than with the company acting as the adjudicator of its own actions.*

The Content Qualification Procedure should be free of cost for the party in whose favor the assessment is delivered.

Abusive challenges and flagging should be sanctioned economically.

ISPs should have the right to make removal or blocking contingent upon a legally binding indemnification commitment.

ISPs should be compensated by the government in case specific investigations and unusual efforts are required.[226] Time limitation on blocking orders along the lines of the system in Finland should be introduced in order to mitigate repressive orders.

The authority to deliver a Content Qualification Assessment could vest in an Ombudsmand Institution appointed in each country by the judiciary (or at least with judicial oversight relative to the impartiality of the appointment). A Content Qualification Assessment would be treated neither as a judgement nor as an arbitration award. The Assessments would not be legally binding, but provide authoritative guidance on interpretation/qualification. The parties would be free to choose to follow or not to follow the Assessment.

Acting in accordance with a Content Qualification Procedure would however relieve the ISP from any future penal or civil sanctions including claims made by authors, editors, publishers or any third party relative to the specific content covered by the Assessment.

---

224 BGH (Federal Court of Justice), judgment of 25 October 2011, Az. VI ZR 93/10.

225 Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (2011), Human Rights Council (A/HRC/17/31). Available at: *http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf* [Accessed 30 September 2016].

226 Reducing terrorist use of the Internet (2013). Den Haag, Netherlands: Clean IT Project.

In case of non-compliance with the Assessment the party in question will not be immune to sanctions of an administrative or judicial nature. Imposition of fines should be allowed against ISPs for every post containing radicalizing content and not taken down within 24 hours from the Assessment. Later litigation will not suspend the Assessment (*i.e.* the parties may continue to rely on the Assessment throughout the litigation process).
Specialized tribunals allowing fast track procedures and the authority to enjoin take down or blocking orders, daily penalties in the case of non-compliance and any other interlocutory measures should be created. Injunctions should provide unequivocal instructions to the ISPs and the other parties involved as to the precise steps and scope of the action required (territorial scope as well as DNS, URL or IP blocking identification and inclusion as the case may be of reintroduced content).

A very recent example of the predicament that ISPs may find themselves in (lacking a swift third party Content Qualification Procedure) is the recent cooperation agreement between Facebook and the government of Israel.[227] This Agreement was forthwith met with protests from the Palestinian Authority.[228]

Clearly it is not acceptable to expose a private actor to this sort of dilemma. If the international community wishes to engage the active assistance of the private sector in protecting its citizens, the very least it can do is offer efficient remedies against not only legal liability but also commercial and "political" exposure which show no signs of abating.

Detailed procedural rules covering costs, appointment of members of the Ombudsmand Institutions and the steps involved in obtaining a Content Qualification Assessment must be drafted.

The procedural rules could to a certain extent derive inspiration from the existing fast track dispute resolution mechanisms developed by for instance eBay involving submission of cases to private online dispute resolution institutions which are able to pass decisions quickly and efficiently. Recourse to the judiciary must however always be available.[229]

Alternative Dispute Resolution Mechanisms have already been mandated in several legal instruments.[230]

---

227 Solomon, S. (2016): "Israel, Facebook to set up joint anti-incitement teams", *The Times of Israel*. Available at: http://www.timesofisrael.com/israel-facebook-to-set-up-joint-anti-incitement-teams/ [Accessed 29 September 2016]

228 Barghouti, A. (2016):" Palestinians launch drive against Facebook 'censorship'", *Anadolu Agency*, Available at: http://aa.com.tr/en/middle-east/palestinians-launch-drive-against-facebook-censorship/655335 [Accessed 29 September 2016]

229 EBay's dispute resolution mechanisms employ computer-assisted negotiation and mediation. Ebay has furthermore decided to outsource these services to the company Square Trade some 1,5 million disputes are resolved this way per year. We may also mention the so-called "CISA's-scheme" ("Communications and Internet Services Adjudication Scheme") approved by Ofcom.

230 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services:
Article 34
Out-of-court dispute resolution
1. Member States shall ensure that transparent, simple and inexpensive out-of-court procedures are available for dealing with unresolved disputes, involving consumers, relating to issues covered by this Directive.
See also: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market:
Recital (52): *"The effective exercise of the freedoms of the internal market makes it necessary to guarantee victims effective access to means of settling disputes; […]"*
"Article 17 - Out-of-court dispute settlement: 1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means."
See also: United Nations Plan of Action to Prevent Violent Extremism (2015), Seventieth session Agenda items 16 and 117:
Recital (49): *"[…]*

In the field of Intellectual Property Rights recourse to dispute settlement is frequent and has been adopted in a number of instruments including the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). For trademark/domain names the "Uniform Domain Name Dispute Resolution Policy" (UDRP) of ICANN applies.

The Ombudsmand Institution could be combined with an advisory board encouraging users to actively participate in a self-regulatory effort.

UNESCO is well placed to take the lead in the implementation of such a policy thereby harmonizing country based content qualification programs and in general raise awareness of corporate accountability and user empowerment.

Policy Recommendation 2

The contentious question of "**global reach**" has recently attracted renewed attention pursuant to Facebook's decision to block access to radicalizing content as a result of its cooperation agreement with the Israeli government. It appears that such content will only be blocked for users accessing it from the Israeli territory[231]. In other words, that it will still be fully accessible to everyone else.

The conflicting views may be summarized as follows:

- Including domains other than specific country domains (for example "*.de*" for Germany) and in particular "*.com*" has "exorbitant extraterritorial effect" since it restricts access to content to users based in other countries.
- The counter argument stresses that in order to avoid "*lex imperfecta*" (i.e. laws void of effect) and by virtue of Art. 13 of the Treaty of Lisbon[232] blocking, dereferencing and other content regulation must necessarily have global reach since in the alternative such injunctions would be manifestly frustrated.

(d) Explore opportunities to introduce alternative dispute resolution mechanisms, such as mediation, arbitration and restorative justice, to resolve conflict and achieve sustainable peace;"

231 The author has not been able to verify this information, but for the purposes of this Report the main point is that is raises the difficult and controversial debate of "global reach".

232 Article 13: *"1. The Union shall have an institutional framework which shall aim to promote its values, advance its objectives, serve its interests, those of its citizens and those of the Member States, and ensure the consistency, effectiveness and continuity of its policies and actions."* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (2007/C 306/01). Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12007L%2FTXT [Accessed 30 September 2016].

The so-called "Article 29 Data Protection Working Party" (an independent European Advisory Body of Data Protection Agencies in Europe)[233] supports this latter view and the French Data Protection Agency (*Commission Nationale de l'Informatique et des Libertés* - CNIL) has enforced it by imposing a fine of 100.000 € on Google for failure to comply with a global de-referencing order.[234]

Google has challenged this decision before the Conseil d'Etat and the case is still pending.

The Court in Paris applied a "global reach" theory in its judgment of 16 September 2014.[235]

In Canada the Equustek case applies the same theory. The question of legality of the injunction (a "Worldwide Order" upheld by the Supreme Court of British Columbia on 13 June 2014) is however pending before the Supreme Court of Canada (Supreme Court of Canada 36602 Google Inc and Equustek Solutions Inc) and the Attorney Generals of Canada and Ontario et. al. are expected to submit their brief shortly in support of Google Inc pursuant to the global reach injunction:

> *[158] In determining whether this interim injunction should be granted, I am mindful of Madam Justice Newbury's admonition that a court should not permit a defendant to frustrate orders of the court and that "courts must, in order to preserve the effectiveness of their judgments, adapt to new circumstances":*

---

233 Article 29 Data Protection Working Party (set up under Article 29 of Directive 95/46/EC), *Guidelines on the Implementation of the Court of Justice of the European Union Judgment On "Google Spain and Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131*/12. Available at: http://ec.europa.eu/justice/data-protection/index_en.htm; [Accessed 30 September 2016]:
"7. Territorial effect of a de-listing decision
In order to give full effect to the data subject's rights as defined in the Court's ruling, delisting decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com".

234 CNIL (2016) : "Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google". Available at: https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu [Accessed 30 September 2016].
"*Dans sa décision du 10 mars 2016, la formation restreinte considère que :*

- *le service de moteur de recherche de Google constitue un traitement unique, les différentes extensions géographiques (« .fr », « .es », « .com », etc.) ne pouvant être considérées comme des traitements distincts. En effet, la société exploitait initialement son service sur le seul « .com » et a créé les extensions au fil du temps pour fournir un service adapté à la langue nationale de chaque pays.*
  Ainsi, pour que le droit au déréférencement des personnes résidant en France soit efficacement respecté, conformément à la décision de la CJUE, il doit être exercé sur l'ensemble de ce traitement, et donc sur toutes les extensions du moteur de recherche.
- *contrairement à ce qu'affirme Google, le déréférencement sur toutes les extensions ne limite pas la liberté d'expression dans la mesure où il n'entraîne aucune suppression de contenu sur Internet. En effet, il consiste uniquement à retirer, à la demande d'une personne physique, de la liste des résultats d'une recherche effectuée à partir de ses prénom et nom, des liens renvoyant vers des pages de sites web. Ces pages demeurent accessibles lorsque la recherche est opérée à partir d'autres termes.*

En conséquence, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 100.000 euros à l'encontre de Google."

235 *M. et Mme X et M. Y c. Google France*, Tribunal de grande instance de Paris, Ordonnance de référé du 16 septembre 2014.

> *[159] The Court must adapt to the reality of e-commerce with its potential for abuse by those who would take the property of others and sell it through the borderless electronic web of the internet. I conclude that an interim injunction should be granted compelling Google to block the defendants' websites from Google's search results worldwide. That order is necessary to preserve the Court's process and to ensure that the defendants cannot continue to flout the Court's orders.*[236]

Art. 2 (1) and (2) of the International Covenant on Civil and Political Rights may be interpreted as conferring jurisdiction on the *"State Party"* to *"ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the […] Covenant […] and "[…] each State Party to the […]*

Covenant […] undertake to take the necessary steps […]to adapts such laws […] as may be necessary to give effects to the rights recognized in the […] Covenant".

Clearly, "territorial reach" seriously limits the effects of blocking orders. Not only will the radicalizing content remain visible from other territories, but the order is very easily circumvented. It has been suggested that circumvention could be stopped by geolocalization (*i.e.* blocking all domains accessed from a given territory and not limit the blocking to country specific domain). The efficiency of this approach is however disputed.

In the event a Content Qualification Procedure is developed it seems that global reach is the legitimate approach.

Policy Recommendation 3

Sanctions against states and authors of radicalizing content

The Canadian laws of 2012 authorizing Canada to seize assets as a sanction against non-State and State actors may be generalized.[237]

Sanctions against authors of radicalizing content could be extended to cover monetary enforcement on a global basis. Typically, the author will have assets in more than just one jurisdiction. These assets may include bank accounts and banks could be under an obligation to freeze such accounts (A similar obligation already applies to terrorist activity and money laundering).

Non-cooperating countries as defined by the Sanctions Committee under the United Nations Security Council could include countries that fail to actively take part in the effort to block/take down radicalizing content finding its origin in the jurisdiction in question.

Such sanctions could be directed against the Country of Origin and the group/association initiating or controlling the authoring of the radicalizing content.

---

[236] *Equustek Solutions Inc v. Jack*, BCSC 1063, Supreme Court of British Columbia, 13 June 2014. For further information on "global reach" please see the Country Questionnaire under point 12.

[237] The State Immunity Act, R.S.C., 1985, c. S-18 (as amended in 2012) and The Canadian Justice for Victims of Terrorism Act (March 13, 2012) could serve as a paradigm for sanctions. "*The purpose of this Act is to deter terrorism by establishing a cause of action that allows victims of terrorism to sue perpetrators of terrorism and their supporter*s".

Governments should include state cooperation in the struggle against online radicalization in foreign policy.

Policy Recommendation 4

A theory allowing "**preventive blocking**" or "blocking by reference to potential radicalization" must necessarily be developed albeit with full recognition of the caution that such an effort requires. This challenge will obviously be demanding and controversial, but nonetheless imperative.

The problem may be illustrated by sites like "Inspire" (authored by Al Qaida) or "Dabiq" (Isis). A substantial portion of content on these and similar sites may not be qualified as "radicalizing" or otherwise illicit.[238]

Yet the sites as such should be blocked on the basis of an "anticipation or prevention theory" due to their general association with radicalization

By analogy it could prove useful to recall the action that allows dissolving certain associations, "sects" and political parties known to preach hatred, engage in criminal activity and or "indoctrination/manipulation" of their members/followers.

Such associations etc. may be dissolved notwithstanding the likelihood that their activities are not 100% illicit.

Furthermore, dissolution necessarily applies to the future and therefore constitutes a form of preventive content regulation.

In France, the Dieudonné case[239] may be cited:

> *"* […] *to prohibit the performance of the show in St. Herblain [...] the prefect of the Loire-Atlantique noted that this show [...] contains anti-Semitic comments, inciting racial hatred, and are, contrary to the dignity of the human person , advocating discrimination, persecutions and exterminations perpetrated during the Second World War [...] the challenged decree of the prefect precised that Mr. Dieudonné M'Bala M'Bala has been, in the past, criminally convicted nine times, including seven definitive, for comments of the same nature [...] the reality and seriousness of the risks of disturbances to public order referred to by the contested order are established [...] allegations whereby these criminally reprehensible and likely to undermine national cohesion statements noted at meetings held in Paris would not be expressed again in Nantes not sufficient to prevent the serious risk to see new severe violations of the respect for the values and principles, including the*

238 From the sites that the author has accessed in a controlled environment for the purpose of the present Report it transpires that significant contributions to the sites do not per se call for violence or incite hatred. The sites combine radicalizing content with religious exegesis and historic or pseudo-historic accounts interspersed with more or less idyllic scenes/descriptions of life in the caliphate. In Australia, the legislation that allows website blocking specifically mentions that it cannot be applied to websites that are mainly operated for a legitimate purpose, but contain a small amount of infringing content. In Portugal, there is also a de minisis rule (applicable primarily to copyright infringement).

239 *Ministre de l'Intérieur v. Société Les Productions de la Plume et M. Dieudonné M'Bala M'Bala* [2014], 374508 Conseil d'Etat

dignity of the human person, enshrined in the Declaration of the Rights of Man and of the Citizen and in the republican tradition." [the author's translation].

Preventive content regulation incorporates a criterion of recidivism.

A reference to the "risk to public order" as a means of prohibiting certain potential expressions of a radicalizing nature has been seen as recently as in the decision of 26 August 2016 from the Conseil d'Etat[240] in France censoring the ban on burkinies on public beaches.

The decision of the Conseil d'Etat not to allow those municipal restrictions of expression did not amount to rejecting that such restrictions could be justified by reference to public order, but that the specifically alleged threat to public order has not been substantiated.

How to justify the blocking of an entire site if only part of it contains illegal content and on what legal grounds to interdict it for the future is a complex and contentious question. Could such blocking be based on the illicit nature of the content "by association"?

Blocking a site supposes that an offense has been committed, but the offence in question will be content - not site - related. Is it possible to take preventive action against online content in case of a "risk to public order"?

This notion has already allowed prohibiting demonstrations because of the violence that had accompanied previous events with the same purpose, organizers or speakers.

The notion of habituability could be used to take preventive action with regard to radicalizing content considering that when a site "habitually" contains illicit content / pages, its access could be blocked for this reason.

The question must be raised whether it may be possible – while still complying with international human rights standards - to block/ take down a site in its entirety on account of the fact that its content originates with or is associated with an individual or an entity that is generally considered instrumental in radicalization and/or terrorism (on the basis of "recidivism" or "habituality") or figures on the United Nations, European Union or United States State Department's "list of terrorist organizations" - independently of a concrete analysis of the content in question.

Preventive blocking should not be restricted to sites that will most likely disseminate radicalizing content in the future, but should also be allowed by countries where the radicalizing content/websites have not - yet – been accessed.

In this regard the judge in Court of Appeal (London) held in an intellectual property rights case (Cartier International AG, Montblanc Simplo, Richemont etc.) that:

"If and in so far as the target websites had not yet been accessed by consumers in the United Kingdom using the services of each of the ISPs there was plainly a real risk that they would be in the future. The judge was entitled to make an order to try to ***prevent*** *this happening."*[241]

---

240 *Ligue des droits de l'homme et autres - association de défense des droits de l'homme collectif contre l'islamophobie en France* [2016], 402742 and 402777, Conseil d'Etat

241 *Cartier International AG, Montblanc-Simplo GMBH, Richemont International SA v. British Sky Broadcasting Limited, British Telecommunications plc and others* [2016] EWCA Civ 658 (Court of Appeal Civil Division).

Policy Recommendation 5

In order to develop user empowered self-regulation of radicalizing content it should be considered to create user **reporting mechanisms**: notice-take-down, flagging or centralized reporting with third parties (Non-Governmental Organizations) ensuring anonymity and procedural efficiency.

Flagging/report button systems should be implemented on browsers which would directly alert the ISP in question.

Providers of chat boxes, e-mail services, messaging systems, social networks, retailing sites, voice over Internet protocol and web forums, should have flagging systems.
The INHOPE initiative could serve as a model for such user driven self-regulation and vigilance:

INHOPE is an active and collaborative network of 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.[242] [243]

Policy Recommendation 6

The approach adopted by "**The Sakinah Campaign**" in Saudi Arabia should be generalized.

The Sakinah Campaign is conducted by an independent Non-Governmental Organization. It seeks to engage in dialogue with individuals who use the Internet to promulgate a radical view of religious convictions and interpretations. The dialogue and counter arguments are administered by highly qualified theologians and scholars whose views carry considerable authority. Refuting the ideology of *takfir* is an important element of the counter dialogue. A transcript of the exchange is made available online.

In Singapore and the Seychelles, the government has encouraged a group of volunteer religious scholars and teachers to launch a website which dispenses arguments that rebut violent extremist teachings and beliefs.

A general right of response or counter narrative should be created (based on Media Law).

Policy Recommendation 7

A product liability (*i.e.* civil damages) inspired standard should be applied for those online services/products that employ intrinsically "dangerous" properties *e.g.* Virtual Private Networks offering IP anonymity, encryption and confidentiality, encryption anonymizers (proxy servers), Content Distribution Networks[244] and certain cloud services.

---

242 INHOPE - International Association of Internet Hotlines, Available at: http://www.inhope.org/gns/home.aspx [Accessed 29 September 2016]: "*INHOPE Hotlines offer the public a way of anonymously reporting Internet material including child sexual abuse material if suspected to be illegal. The Hotline will ensure that the matter is investigated and if found to be illegal the information will be passed to the relevant Law Enforcement Agency and in many cases the Internet Service Provider hosting the content*."

243 For further details, see annex 1 "Country Questionnaire" point 7

244 Content Distribution Networks provide websites with enhanced protection against *i.e.* Distributed Denial of Service (DDoS) attacks. The Content Distribution Networks serve as a protective screen and also secure anonymity.

The risk that these services be used for radicalization purposes is not negligible.

Such a liability standard would be consistent with a theory of liability for dissemination of infected/malware apps (applying a vetting obligation on distribution platforms).

Indeed, if ISP liability might be engaged for failure to properly vet applications and sites referred to on hyperlinks as well as failure to warn it makes little sense that liability should not be encountered for dissemination of content that causes unspeakable harm and grievance, just as it seems hard to accept that ISPs are currently liable for IP-infringements (after notice or knowledge), but not for radicalizing content.

The United Nations Counter-Terrorism Implementation Task Force Working Group Compendium confirms that[245]": *[…] The wide availability of "bullet-proof" hosted cloud computing resources means that terrorists are able to host their propaganda and digital content online with little fear of identification or reprisal.*

Even more advanced website hiding techniques, such as "double-flux" allow the domain name servers (DNS) which resolve web host names to be moved rapidly from server to server […]"

Isis has recommended using the following instant messaging applications owing to their "confidentiality": Signal, Chatsecure, Telegram, Silent text, Silent phone, LinPhone and Surespot.[246]

The French government is likely to take the initiative at the EU level to see tougher regulation of encryption capability (obviously with the risk of infringing privacy laws and the benefits of encryption technology to free speech in a repressive environment as well as *bona fide* protection against industrial espionage).[247]

The Apple San Bernardino case and the recent WhatsApp case in Brazil both related to provision of encryption keys.[248]

Providers of applications that contain encryption capability notoriously utilized for radicalization purposes should be under enhanced diligence obligations.

Technological solutions which will allow blocking the use of such encrypted applications for radicalization purposes should be developed together with industry.

---

245 *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects* (2011), United Nations Counter-Terrorism Implementation Task Force - Working Group Compendium.

246 O'Neill, P. (2016): "ISIS recommends list of secure-messaging apps amid heated U.S. encryption debate", The Daily Dot. Available at: http://www.dailydot.com/layer8/isis-telegram-encryption-messenger-recommendations/ [Accessed 26 September 2016].

247 Berthet, C. (2016) : « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible ». Available at: http://cnnumerique.fr/tribune-chiffrement/ [Accessed 29/09/2016].

248 Freedom House. (2016) WhatsApp Suspended in Brazil. Available at: https://freedomhouse.org/article/whatsapp-suspended-brazil [Accessed 29/09/2016]:
On July 19, 2016 a Brazilian court issued on order against WhatsApp for its refusal to turn over encryption data. The court ruled that providers that do not cut off access to WhatsApp be fined the equivalent of $15,300 a day until they comply. The decision of 19 July is the fourth against WhatsApp since February 2015.

Policy Recommendation 8

It is not advisable in the author's opinion to establish a general standard of complicity through "material support". Complicity should require intent and not just knowledge or awareness.

Policy Recommendation 9

"Defensive hacking" or "hack back" based on the Israeli (the bill providing for this measure was not passed) and Dutch models should not be implemented. Anticipatory self-defense is ruled out by Art. 51 of the United Nations Charter.

The United Nations Counter-Terrorism Implementation Task Force Working Group Compendium "Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects (May 2011)" considered that

Given the significant impediments to blocking terrorist content in cyberspace, some participants raised the possibility of utilizing even more active measures, such as the launching of distributed denial of service (DDOS) attacks against terrorist websites. Doing so, however, has many challenges. First, the legality of such an approach under international law is highly suspect.

One of the main legal impediments to state authorized "defensive attacks" against content hosted abroad is that of extraterritorial **enforcement**. Notwithstanding the legality of extraterritorial adjudicatory and prescriptive jurisdiction (under certain conditions) enforcement of state authority outside its borders is generally not recognized.

Policy Recommendation 10

In the long term the Internet should be included under the Common Heritage of Mankind (CHM) concept.

Indeed, the Internet may be deemed to have attained the quality of such Common Heritage already. This status would allow its regulation and governance to be subject to international consensus.

At the Council of Europe Meeting (30 March 2016) the topic of "Internet Governance (Council of Europe Strategy 2016-2019)[249] included CHM references (implicitly):

> *"...the NETmundial Multistakeholder Statement, recognized that the Internet is a global resource which should be managed in the public interest. It also reaffirmed the importance of human rights to the Internet and provided a set of Internet governance principles, as well as a roadmap for the future evolution and improvement of the existing Internet governance framework, ensuring the full involvement of all stakeholders. The NETmundial Initiative recognizes the NETmundial Internet governance process principles: democratic, multi-stakeholder, open, participative, consensus-driven, transparent, accountable, inclusive and equitable, shared, collaborative, and enabling meaningful participation."*

[249] Internet Governance – Council of Europe Strategy 2016-2019: Democracy, Human Rights and the Rule of Law in the Digital World (2016), Council of Europe [CM (2016)10-final].

President Obama's initiative to cede oversight of the Internet to the international community was moved a decisive step forward by a ruling issued on 30 September 2016 by a federal judge not to suspend the transition process as petitioned by opposing State attorneys.[250]

The immediate move towards ICANN oversight is budget driven and concerns the administration of domain names, but it may signal a more profound shift in Internet governance. Whether that shift will be defined by industry or the world community is the true question.

UNESCO provides the natural forum where consensus on the future of Internet governance under the auspices of ICANN may be reached. ICANN's remit could include the Content Qualification Assessment Procedure developed above under point 1.

Policy Recommendation 1 1

Content regulation could benefit from an international treaty along the lines of the European Union e-commerce Directive integrating the principles of "rule of origin", "home country control" and Media Law.
State Liability for injurious consequences of acts committed under its territorial jurisdiction or control could extend to the harmful consequences of radicalizing content. We find such state liability in a number of Treaties.

An example is the "Draft articles on Prevention of Transboundary Harm from Hazardous Activities (2001)[251] Art. 3:

"*The State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof*."

---

250 Romm, T. (2016): "Court says Obama's Internet transition can go forward", Politico. Available at: http://www.politico.com/story/2016/09/obama-internet-transition-courts-228992 [Accessed 30 September 2016].

251 Report of the International Law Commission to the United Nations General Assembly (A/56/10):
"*General commentary*
(1) The articles deal with the concept of prevention in the context of authorization and regulation of hazardous activities which pose a significant risk of transboundary harm. Prevention in this sense, as a procedure or as a duty, deals with the phase prior to the situation where significant harm or damage might actually occur, requiring States concerned to invoke remedial or compensatory measures, which often involve issues concerning liability.
(2) The concept of prevention has assumed great significance and topicality. The emphasis upon the duty to prevent as opposed to the obligation to repair, remedy or compensate has several important aspects. Prevention should be a preferred policy because compensation in case of harm often cannot restore the situation prevailing prior to the event or accident.
(6) The first criterion to define the scope of the articles refers to "activities not prohibited by international law". This approach has been adopted in order to separate the topic of international liability from the topic of State responsibility. The employment of this criterion is also intended to allow a State likely to be affected by an activity involving the risk of causing significant transboundary harm to demand from the State of origin compliance with obligations of prevention although the activity itself is not prohibited.
(14) As to the element of "risk", this is by definition concerned with future possibilities, and thus implies some element of assessment or appreciation of risk. The mere fact that harm eventually results from an activity does not mean that the activity involved a risk, if no properly informed observer was or could have been aware of that risk at the time the activity was carried out. On the other hand, an activity may involve a risk of causing significant transboundary harm even though those responsible for carrying out the activity underestimated the risk or were even unaware of it. The notion of risk is thus to be taken objectively, as denoting an appreciation of possible harm resulting from an activity which a properly informed observer had or ought to have had."

Policy Recommendation 12

More accurate filtering/blocking and monitoring software should be developed and installed by ISPs including a mandatory bot application. The use of automated detection systems by Internet companies must be made known to the public.

Certain ISPs, platforms and special networks argue that monitoring obligations are not technically possible for content.

As to this latter observation, it appears that when it comes to identifying ad-blockers, current technology does offer practical solutions, which amount to a form of general monitoring.

The application Ad Block actually prevents ads from gaining access to Facebook pages of individual users. In view of the potential consequences to the company's business model Facebook has developed a « counter-application » allowing both for the identification of ads and the neutralization of AdBlocking[252].

ISPs also already use spam filtering and virus blocking.

Critics claim that website blocking is an exercise in futility as website operators shift sites - the so-called "whack-a-mole" effect—but the United Kingdom's approach shows that this can be countered through dynamic blocking orders. ISPs are required to block the website named in the initial court order, and when notified in writing, any other IP address or URL whose sole or predominant purpose is to facilitate access to the named website.

The judge in the recent Court of Appeals judgement (London, 6th July 2016) summarized the effectiveness of blocking as follows (Case Cartier International AG, Montblanc Simpo, Richemont etc.):

> *"Overall, the conclusion which I draw from the evidence is that,* […] *blocking of targeted websites has proved reasonably effective in reducing use of those websites in the UK. No doubt it is the casual, inexperienced or lazy users who stop visiting those websites, whereas the experienced and determined users circumvent the blocking measures; but that does not mean that it is not* […] *worthwhile"*

Deep Packet Inspection Capability should however only be deployed in cases of qualified suspicion.

Policy Recommendation 13

ISPs should forward radicalizing content to a designated law enforcement agency (along the lines of suspicion of money laundering reporting) when they become aware themselves or are made aware by users or Non-Governmental Organizations hereof.

ISPs that do not cooperate in taking down/blocking or alerting law enforcement to radicalizing content could be barred from public procurement. Advertisers should also include ISPs governance in their Procurement Policy.

[252] Berthet, C. (2016) : « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible ». Available at: http://cnnumerique.fr/tribune-chiffrement/ [Accessed 29/09/2016].

In 2013, the Women Action and Media Group (WAM) in the UK launched a campaign against abusive graphic content on Facebook. In response major companies suspended their advertisements.

Such programs may be efficient if introduced in a global and transparent manner.

Policy Recommendation 14

The following (selected) recommendations concerning ISP liability and duties from the Clean It Project for Best Practices[253] could be implemented (adapted to radicalizing content):

Law enforcement agents should be allowed to 'patrol' on social media. This includes having a profile, joining user groups, sending and receiving messages on the platform. Agent provocateur techniques should only be authorized under strict conditions.

Knowingly providing hyperlinks on websites to radicalizing content should be prohibited (either by way of "reproduction" or willful dissemination and or complicity). The recent judgement from the European Court of Justice (8 September 2016 *GS Media v. Sanoma et al*.) would confirm the legal basis for such an obligation (*supra* p.53).

Individuals and organizations on the United Nations or European Union terrorist sanction list should not be allowed access to disseminate content on the Internet.

ISPs should have sufficiently (trained) staff support to handle reports on radicalizing content. These staff should have experience in applicable laws, regulations and international reporting procedures (manuals similar to those at financial institutions for the purposes of detecting and reporting money laundering should be readily available).

ISP's should assure that content that has been removed once cannot be uploaded onto the platform again, including when the content has been slightly modified to the extent this can be achieved technologically and at reasonable cost.

253 Clean It Project (2012) *Clean It Project – Detailed Recommendations Document for Best Practices and Permanent Dialogue*, https://www.edri.org/files/cleanIT_sept2012.pdf. [Accessed 30 September 2016].

Policy Recommendation 15

A Data Protection Officer should be designated by each ISP (as per the General Data Protection Regulation Art. 37: *"The controller and the processor shall designate a data protection officer* […]*"*).

A model for the Data Protection Officer's mandate, protection and liability could be that of Compliance Officers in financial institutions. [254]

[254] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC:
Article 37- Designation of the data protection officer
1. The controller and the processor shall designate a data protection officer in any case where:
(a)
the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b)
the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c)
the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Article 39 - Tasks of the data protection officer
1. The data protection officer shall have at least the following tasks:
(a)
to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b)
to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(d)
to cooperate with the supervisory authority;
(e)
to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

BIBLIOGRAPHY

- **Statutes and Regulations**

H.R. 1955 (110th): Violent Radicalization and Homegrown Terrorism Prevention Act of 2007. Available at: https://www.govtrack.us/congress/bills/110/hr1955/text [Accessed 27 September 2016].

H.R. 1304 (111th): Free Speech Protection Act of 2009 (Free Speech Protection Act of 2009. Available at: https://www.congress.gov/bill/111th-congress/house-bill/1304/text [Accessed 27 September 2016].

H.R. 4922 (103rd): Communications Assistance for Law Enforcement Act of 1994. Available at: https://www.congress.gov/bill/103rd-congress/house-bill/4922 [Accessed 30 September 2016].

H.R. 4411 (109th): Internet Gambling Prohibition and Enforcement Act of 2006. Available at: https://www.govtrack.us/congress/bills/109/hr4411/text [Accessed 30 September 2016].

H.R.1004 (104th): Communications Decency Act of 1996. Available at: https://transition.fcc.gov/Reports/tcom1996.txt. [Accessed 30 September 2016].

H.R.491 (113th Congress) Global Online Freedom Act of 2013 referred in 2013 to the Subcommittee on Africa, Global Health, Global Human Rights and International Organizations. Available at: https://www.govtrack.us/congress/bills/113/hr491 [Accessed 30 September 2016].

18 U.S. Code § 2339A - Providing material support to terrorists. Available at: https://www.law.cornell.edu/uscode/text/18/2339A [Accessed 30 September 2016].

18 U.S. Code § 2339B - Providing material support or resources to designated foreign terrorist organizations. Available at: https://www.law.cornell.edu/uscode/text/18/2339B [Accessed 30 September 2016].

18 U.S. Code § 2333 - Civil remedies. Available at: https://www.law.cornell.edu/uscode/text/18/2333 [Accessed 30 September 2016].

H.R. 3076, September 11 Marque and Reprisal Act of 2001. Available at https://www.gpo.gov/fdsys/pkg/BILLS-107hr3076ih/pdf/BILLS-107hr3076ih.pdf [Accessed 27 September 2016].

H.R.2281 (105th): Digital Millennium Copyright Act of 1998. Available at: https://www.congress.gov/bill/105th-congress/house-bill/2281. [Accessed 30 September 2016].

State Immunity Act, R.S.C., 1985, c. S-18 (as amended in 2012). Available at: http://laws-lois.justice.gc.ca/eng/acts/S-18/page-1.html [Accessed 30 September 2016].

Justice for Victims of Terrorism Act, S.C. 2012, c. 1, s. 2 (2012). Available at: http://laws-lois.justice.gc.ca/eng/acts/j-2.5/page-1.html [Accessed 30 September 2016].

S.2040 (114th): Justice Against Sponsors of Terrorism Act. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/2040 [Accessed 30 September 2016].

Coalition Provisional Authority Order Number 91 (2004), CPA/ORD/02. Available at: http://www.iraqcoalition.org/regulations/20040607_CPAORD91_Regulation_of_Armed_Forces_and_Militias_within_Iraq.pdf [Accessed 30 September 2016].

Ordonnance de Louis XIV Roy de France et de Navarre, donnée à Fontainbleau au mois d'aoust, touchant la marine de commerce (1681).

The Constitution of the United States of America (1787). Available at: https://www.law.cornell.edu/constitution/overview [Accessed 30 September 2016].

- **International Conventions and Declarations**

Globalization (2002) Declaration of Responsibility and Human Duties, adopted by a high-level group chaired by Richard j. goldstone under the auspices of the city of Valencia and UNESCO initiated and organized by the Valencia third millennium foundation. Available at: https://fr.scribd.com/document/69837465/Declaration-of-Responsibilities-and-Human-Duties [Accessed 27 September 2016].

Convention on Third Party Liability in the Field of Nuclear Energy of 29th July 1960, as amended by the Additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982. Available at: https://www.oecd-nea.org/law/nlparis_conv.html [Accessed 27 September 2016].

Arab Convention on Combating Information Technology Offences (2010), League of Arab States.

Déclaration réglant divers points de droit maritime (1856). Available at: https://ihl-databases.icrc.org/applic/ihl/dih.nsf/Article.xsp?action=openDocument&documentId=52C3B93E8698E114C12563BD002B802F [Accessed 30 September 2016].

The African Declaration on Internet Rights and Freedoms (Amended as of 2015). Available at: http://africaninternetrights.org/articles/ [Accessed 27 September 2016].

The International Convention Concerning the Use of Broadcasting in the Cause of Peace (1936). Available at: http://treaties.fco.gov.uk/docs/fullnames/pdf/1938/TS0029%20(1938)%20CMD-5714%201936%2023%20SEP,%20GENEVA%3B%20INTL%20CONVENTION%20CONCERNING%20USE%20OF%20BROADCASTING%20IN%20CAUSE%20OF%20PEACE.pdf). [Accessed 30 September 2016].

The Arab Charter on Human Rights (2004), League of Arab States. Available at: http://hrlibrary.umn.edu/instree/loas2005.html. [Accessed 30 September 2016].

The African Charter on Human and People's Rights (1981), African Union. Available at: http://www.achpr.org/instruments/achpr/ [Accessed 30 September 2016].

The Cairo Declaration on Human Rights in Islam (1990), Organisation of the Islamic Conference. Available at: http://www.oic-oci.org/english/article/human.htm [Accessed 30 September 2016].

The ASEAN Human Rights Declaration (2012), Association of Southeast Asian Nations. Available at: http://www.mfa.go.th/asean/contents/files/other-20121217-165728-100439.pdf [Accessed 30September 2016].

The American Declaration of the Rights and Duties of Man (1948), Organization of the American States. Available at: http://www.cidh.org/basicos/english/Basic2.American%20Declaration.htm [Accessed 30 September 2016].

- **United Nations Resolutions and Principles**

Charter of the United Nations and Statute of the International Court of Justice (1945), San Francisco, United States. Available at: https://treaties.un.org/doc/publication/ctc/uncharter.pdf [Accessed 30 September 2016].

U.N. Security Council (2003), Resolution 1456 on combating terrorism. Available at: http://dag.un.org/bitstream/handle/11176/25388/S_RES_1456%282003%29-EN.pdf?sequence=3&isAllowed=y [Accessed 27 September 2016].

U.N. Security Council (2015), Resolution 2250 on Maintenance of international peace and security. Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2250.pdf [Accessed 27 September 2016].

General Assembly (2006), The United Nations Global Counter-Terrorism Strategy: Resolution 60/288. Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terr%20ARES60288.pdf [Accessed 27 September 2016].

United Nations (1996), The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, E/CN.4/1996/39. Available at: http://hrlibrary.umn.edu/instree/johannesburg.html [Accessed 27 September 2016].

General Assembly (2016), Secretary-General's Plan of Action to Prevent Violent Extremism: Resolution 70/254. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/L.41 [Accessed 30 September 2016].

General Assembly (2001), Combating the criminal misuse of information technologies: Resolution 55/63. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [Accessed 30 September 2016].

General Assembly (1966), International Covenant on Civil and Political Rights: Resolution 2200A (XXI). Available at: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf [Accessed 30 September 2016].

General Assembly (2000), United Nations Convention Against Transnational Organized Crime: Resolution 55/25 and Protocol (2001) Resolution 55/255. Available at: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf [Accessed 30 September 2016].

United Nations Security Council (2001), Resolution 1373 Adopted on 28 September 2001. Available at: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf. [Accessed 27 September 2016].

General Assembly (1999), United Nations Convention for the Suppression of the Financing of Terrorism: Resolution 54/109. Available at: http://www.un.org/law/cod/finterr.htm [Accessed 30 September 2016].

- **European Union Law**

Charter of Fundamental Rights of the European Union (2000/C 364/01). Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf [Accessed 30 September 2016].

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (2007/C 306/01). Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12007L%2FTXT [Accessed 30 September 2016].

Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0919&from=EN [Accessed 27 September 2016].

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031 [Accessed 27 September 2016].

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008F0913 [Accessed 27 September 2016].

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001L0029 [Accessed 27 September 2016].

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040. [Accessed 30 September 2016].

Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849. [Accessed 30 September 2016].

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31999L0093. [Accessed 30 September 2016].

Regulation 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32014R0910. [Accessed 30 September 2016].

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services. Available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0022. [Accessed 30 September 2016].

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32002L0058. [Accessed 30 September 2016].

Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG. [Accessed 30 September 2016].

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R(01) [Accessed 30 September 2016].

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 30 September 2016].

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0013 [Accessed 30 September 2016].

- **<u>European Union Internal documents</u>**

EU Counter-Terrorism Coordinator (2016), Note 6785/16 to Council of the European Union on the State of play on implementation of the statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015. Available at: http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/en/pdf [Accessed 27 September 2016].

Commission staff working document (2007), Accompanying document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on combating terrorism Summary of the impact assessment {COM (2007) 650 final} {SEC (2007) 1424}. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007SC1425&from=EN [Accessed 27 September 2016].

Article 36 Committee (2007), Note 8457/3/07 to COREPER / Council on Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web"). Available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%203 [Accessed 27 September 2016].

Directorate-General for Internal Policies, European Parliament (2014), “Preventing and Countering Youth Radicalization in the EU”, Study for the LIBE Committee. Available at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/IPOL-LIBE_ET(2014)509977_EN.pdf [Accessed 27 September 2016].

Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on combating terrorism - Impact Assessment [COM (2007) 650 final - SEC (2007) 1425]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007SC1424 [Accessed 30 September 2016].

Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0289 [Accessed 30 September 2016].

- **European Union External Documents**

Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment: addressing the factors contributing to violent radicalization [COM (2005) 313 final]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52005DC0313. [Accessed 30 September 2016].

Safer Social Networking Principles for the European Union (2009). Available at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf [Accessed 30 September 2016]

Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities [COM/2016/0287 final-2016/0151 COD]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN [Accessed 30 September 2016].

Comprehensive Economic and Trade Agreement between Canada of the one part, and the European Union and its Member States, of the other part. Available at: http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf [Accessed 30 September 2016].

European Commission Press release (2016): "Antitrust: Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules". Available at: http://europa.eu/rapid/press-release_IP-16-2532_en.htm [Accessed on 27 September 2016].

- **Council of Europe Law, Decisions and Reports**

Convention for the Protection of Human Rights and Fundamental Freedoms (1950). Available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed 30 September 2016].

Council of Europe (2001), Convention on Cybercrime, 23.XI.2011. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 27 September 2016].

Council of Europe (2011), Convention on preventing and combating violence against women and domestic violence, Istanbul, 11. V.2011. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008482e [Accessed 27 September 2016].

Ministers' Deputies (2016), 1252nd meeting of the Ministers' Deputies, "Internet Governance - Council of Europe Strategy 2016-2019", CM (2016)10-final. Available at: http://www.coe.int/en/web/cm/meetings-2016/-/asset_publisher/OZPU3QR7b5uC/content/1252nd-meeting-of-the-ministers-deputies-30-march-2016- [Accessed 27 September 2016].

Council of Europe (2005), Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, 16.V.2005. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3811 [Accessed 30 September 2016].

Council of Europe (2003), Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f [Accessed 30 September 2016].

Comparative Study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe (2015), 14-067. Lausanne, Switzerland: Swiss Institute of Comparative Law, Excerpt p. 773-800. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806575b4 [Accessed 30 September 2016].

Council of Europe (2016), Internet Governance – Council of Europe Strategy 2016-2019: Democracy, human rights and the rule of law in the digital world (2016), CM (2016)10-final. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60 [Accessed 30 September 2016].

- **Books**

Keen, A. (2015) *The Internet Is Not the Answer*, Atlantic Monthly Press, pp. 149, 151, 153 and 155.

Kissinger, H. (2014) *World Order: Reflections on the Character of Nations and the Course of History*, Penguin Press.

Derieux, E. (2015) *Droit des Médias, Droit français, Européen et International*, 7th ed., LGDJ, pp. 397-597.

Wittes, B.; Blum, G. (2015) *The future of Violence: Robots and Germs, Hackers and Drones - Confronting the New Age of Threat*. Gloucestershire, United Kingdom: Amberley Publishing

Van Eeten, M.; Mueller, M. and Van Eijk, N. (2014) *The Internet and the State: A Survey of Key Developments*. Den Haag, Netherlands: Raad voor Maatschappelijke Ontwikkeling.

MacCarthy, M. (2009) *What Internet Intermediaries Are Doing About Liability and Why It Matters*, Washington, United States: ExpressO, Georgetown University

Brown, I. (2010) *Internet Self-Regulation and Fundamental* Rights. Oxford, United Kingdom: University of Oxford - Oxford Internet Institute, Index on Censorship Vol. 1

Breindl, Y. (2013) *Internet Content Regulation in Liberal Democracies. A Literature Review*. Göttingen, Germany: Institute of Political Science, Georg-August-Universität Göttingen

Stern, J.; Berger, J.M. (2015) *Isis: The state of terror*. New York, United States: Ecco Press

Drew, J. (2013) *A Social History of Contemporary Democratic Media*. New York, United States: Routledge

Combacau, J.; Sur, S. (2010) *Droit International Public*, 9ème Edition. Paris, France : Montchrestien

Daillier ; P. ; Pellet, A. ; Forteau, M. (2009) *Droit international Public*, 8ème Edition. Paris, France : L.G.D.J.

Erelle, A. [2015] *Dans la peau d'une djihadiste : Enquête au cœur des filières islamistes.* Robert Laffont.

Harris, S. [2014] *@ war: The rise of Cyber Warfare*. London, United Kingdom: Headline Publishing Group.

Erelle, A. [2015] *Undercover Jihadi Bride: Inside Islamic State's Recruitment Network*. London, United Kingdom: HarperCollins Publishers.

Vigna, P.; Casey, M. J. 2015] *The Age of Cryptocurrency: How Bitcoin and Digital Money are challenging the Global Economic Order*. New York, United States: St Martin's Press.

Angwin, J. [2014] *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York, United States: St Martin's Press.

Lucas, E. (2015), Cyberphobia*: Identity, Trust, Security and the Internet*. Bloomsbury USA.

Spinello, R.A.; Tavani H.T. (2002) Readings in Cyberethics. Boston, United States. Jones and Bartlett Publishers

- **Articles**

Lacey, M. (2007): "10 Years Later, Chiapas Massacre Still Haunts Mexico", *The New York Times*. Available at: http://www.nytimes.com/2007/12/23/world/americas/23acteal.html?_r=0 [Accessed 27 September 2016].

Thompson, R. L. (2011): "Radicalization and the Use of Social Media", *Journal of Strategic Security*, Volume 4, No. 4, Winter 2011, Article 9, p. 167. Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1146&context=jss [Accessed 27 September 2016].

Charvat, J. (2010): "Radicalization on the Internet", Defence Against Terrorism Review, Vol. 3, No. 2, Fall 2010, Congressional Research Service, p. 75. Available at: http://www.coedat.nato.int/publication/datr/volumes/datr6.pdf [Accessed 27 September 2016].

Dominguez, R. (2010) : "La désobéissance civile électronique, Inventer le Futur du Théâtre d'Agitprop En-Ligne", *Multitudes*, Volume 2010/2 No. 41, p. 238. Available at: http://www.cairn.info/revue-multitudes-2010-2-page-204.htm [Accessed 27 September 2016].

Wray, S. (1998): "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics", paper presented at The World Wide Web and Contemporary Cultural Theory Conference, Drake University, November 1998. Available at: http://switch.sjsu.edu/web/v4n2/stefan/ [Accessed 27 September 2016].

Stempel J36., Frankel A., (2016): "Twitter sued by U.S. widow for giving voice to Islamic State", *Reuters*. Available at: http://www.reuters.com/article/us-twitter-isis-lawsuit-idUSKCN0US1TA [Accessed 27 September 2016].

Institute for strategic Dialogue (2011): "Radicalisation: The role of the Internet, A working Paper on the PPN". Available at: https://www.counterextremism.org/resources/details/id/11/ppn-working-paper-radicalisation-the-role-of-the-internet [Accessed 30 September 2016].

Koehler D., (2014): "The Radical Online: Individual Radicalization Processes and the Role of the Internet", *Journal for Deradicalization*, Volume 2014/15 No. 1, pp. 116, 118. 119, 120, 121, 122, 125, 128, 130-131. Available at: http://journals.sfu.ca/jd/index.php/jd/article/view/8 [Accessed 30 September 2016].

Pantucci, R., (2011): "A typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists", *Developments in Radicalization and Political Violence*). Available at: http://www.trackingterrorism.org/sites/default/files/chatter/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf [Accessed 27 September 2016].

Rahimullah, R.; Larmar, S.; Abdalla, M. (2013): "Understanding Violent Radicalization amongst Muslims: A Review of the Literature", *Journal of Psychology and Behavioral Science*, Volume 1 No. 1, p. 19. Available at: http://www98.griffith.edu.au/dspace/bitstream/handle/10072/59871/93055_1.pdf?sequence=1 [Accessed 27 September 2016].

Holmer, I. (2016): "Explaining the appeal of militant Salafism in a Norwegian context", *FLEKS*, Volume 3, No. 1, p. 1. Available at: https://journals.hioa.no/index.php/fleks/article/view/1679/1530 [Accessed 30 September 2016].

Rascoff S. (2012): "Establishing Official Islam? *The Law and Strategy of Counter-Radicalisation*", *Stanford Law Review*, Volume 64, Issue 1, p. 125. Available at: https://www.stanfordlawreview.org/print/article/establishing-official-islam/ [Accessed 27 September 2016].

King & Spalding LLP (2007): "Free Speech Group Petitions U.S. Trade Representative to File WTO Complaint to End Chinese Internet Censorship, Reports", *Business Wire*. Available at: http://www.businesswire.com/news/home/20071210005945/en/Free-Speech-Group-Petitions-U.S.-Trade-Representative [Accessed 27 September 2016].

Sableman, M.; Thomson Coburn LLP (2013): "ISPs and content liability: The original Internet law twist". Available at: http://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2013-07-09/isps-and-content-liability-the-original-internet-law-twist [Accessed 27 September 2016].

Breteau, P. (2016) : "Que risquent les auteurs d'une fausse alerte terroriste ?", *Le Monde*. Available at: http://www.lemonde.fr/les-decodeurs/article/2016/09/19/que-risquent-les-auteurs-d-une-fausse-alerte-terroriste_4999873_4355770.html#kSbtxsGtc5VuuLot.99 [Accessed 27 September 2016].

Price, M. (2009): "Satellite Transponders and Free Expression". Available at http://www.cardozoaelj.com/wp-content/uploads/Journal%20Issues/Volume%2027/Issue%201/Price.pdf [Accessed 30 September 2016].

Price, M. (2010): "Orbiting Hate? Satellite Transponders and Free Expression", *Derecho Comparado de la Informacion*, p. 164. Available at: http://docplayer.net/9423929-Orbiting-hate-satellite-transponders-and-free-expression.html [Accessed 30 September 2016].

Segura-Serrano, A. (2006): "Internet Regulation and the Role of International Law", Max Planck UNYB, p. 206. Available at: http://www.mpil.de/files/pdf3/06_antoniov1.pdf [Accessed 30 September 2016].

King, K. (2011): "Personal jurisdiction, Internet commerce, and privacy: The pervasive legal consequences of modern geolocation technologies", *ALB. L.J. SCI. & TECH*, Volume 21.1, p. 61. Available at: http://www.albanylawjournal.org/Documents/Articles/21.1.61-King.pdf [Accessed 30 September 2016].

Goldman, E. (2016): "AdWords Buys Using Geographic Terms Support Personal Jurisdiction–Rilley v. MoneyMutual", *Technology & Marketing Law Blog*. Available at: http://blog.ericgoldman.org/archives/2016/08/adwords-buys-using-geographic-terms-supports-personal-jurisdiction-rilley-v-moneymutual.htm [Accessed 27 September 2016].

Fewster, S. (2016): "Dr Janice Duffy preparing second Google defamation claim, less than a year after $115,000 victory", *The Advertiser*. Available at*:* http://www.adelaidenow.com.au/news/south-australia/dr-janice-duffy-preparing-second-google-defamation-claim-less-than-a-year-after-115000-victory/news-story/bfaec391c4b7c02b1676b90a2e860658 [Accessed 27 September 2016].

Bauml, J. (2011): "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship," *Federal Communications Law Journal*, Volume 63, issue 3, Article 6, p. 697. Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1600&context=fclj [Accessed 27 September 2016].

Reuters (2016): "$1 Billion Lawsuit Accuses Facebook of Enabling Palestinian Attacks". Available at: http://fortune.com/2016/07/11/facebook-lawsuit-hamas-attacks/ [Accessed 28 September 2016].

Greer, D. (2013): "Google Inc's liability in defamation under English law for material posted on Blogger.com". Available at: http://www.lexology.com/library/detail.aspx?g=27427989-9bfa-4f74-b569-aad7645a0afb [Accessed 28 September 2016].

RT (2016): "Facebook, Twitter & YouTube 'consciously failing' to tackle online extremism – MPs". Available at: https://www.rt.com/uk/357148-online-extremism-social-media/ [Accessed 28 September 2016].

Berthet, C. (2016) : "Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible". Available at: http://cnnumerique.fr/tribune-chiffrement/ [Accessed 29 September 2016].

Mahoney, K. (1992): *"The Canadian constitutional approach to freedom of expression in hate propaganda and pornography"*. Calgary, Canada: Law and Contemporary Problems, p.77-105. Available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4123&context=lcp [Accessed 30 September 2016].

Freedom House. (2016): "WhatsApp Suspended in Brazil". Available at: https://freedomhouse.org/article/whatsapp-suspended-brazil [Accessed 29 September 2016].

Cohen, T. (2016): "Israel eyes law to remove online content inciting terrorism". Available at: http://www.reuters.com/article/us-israel-security-socialmedia-idUSKCN0Z8174 [Accessed 29 September 2016].

Mills, E. (2012): "Google now scanning Android apps for malware". Available at: https://www.cnet.com/news/google-now-scanning-android-apps-for-malware/ [Accessed 30 September 2016].

Welch, C. (2015): "Android apps are now reviewed by Google before you can download them". Available at: http://www.theverge.com/2015/3/17/8231125/android-apps-now-reviewed-by-google [Accessed 30 September 2016].

Landers and Rogers Lawyers (2015): "Duffy v. Google – Is this the end of the internet as we know it?". Available at: http://www.landers.com.au/publications/dispute-resolution/duffy-v-google-is-this-the-end-of-the-internet-as-we-know-it/ [Accessed 30 September 2016].

Paresh, D. (2016): "California Supreme Court votes to review a libel case over negative Yelp reviews". Available at: http://www.latimes.com/business/technology/la-fi-tn-yelp-ava-bird-20160921-snap-story.html [Accessed 30 September 2016].

Thanawala, S. (2016): "California Supreme Court to consider suit over Yelp review". Available at: http://www.usnews.com/news/business/articles/2016-09-21/california-supreme-court-to-consider-suit-over-yelp-review [Accessed 27 September 2016].

Fischer, D. (2015): “Google Wins, Movie Studios Lose as Court Blocks ITC Control Over Data”. Available at: http://www.forbes.com/sites/danielfisher/2015/11/10/appeals-court-rejects-international-trade-commission-power-to-block-electronic-data/#6abc1708727f [Accessed 30 September 2016].

Solomon, S. (2016): “Google, Facebook must be held accountable for criminal content – justice minister”. Available at: http://www.timesofisrael.com/hold-google-facebook-accountable-for-content-justice-minister/ [Accessed 30 September 2016].

Constine, J. (2016): “Facebook ads still slipping past Adblock Plus via stripped-down code”. Available at: https://techcrunch.com/2016/09/18/faceblock/ [Accessed 30 September 2016].

Kumar Doran, A.; Grant, J. (2013): “State Attorneys General Propose Dramatic Amendment to Section 230”. Available at: http://www.medialawmonitor.com/2013/08/state-attorneys-general-propose-%E2%80%A8dramatic-amendment-to-section-230/ [Accessed 30 September 2016].

Perotti, E. (2015): “The European Ruling on the Right to Be Forgotten and Its Extra-EU Implementation”, World Association of Newspapers and News Publishers (WAN-IFRA). Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703325. [Accessed 30 September 2016].

Solomon, S. (2016): “Israel, Facebook to set up joint anti-incitement teams”. Available at: http://www.timesofisrael.com/israel-facebook-to-set-up-joint-anti-incitement-teams/ [Accessed 29 September 2016].

Barghouti, A. (2016): “Palestinians launch drive against Facebook 'censorship'”. Available at: http://aa.com.tr/en/middle-east/palestinians-launch-drive-against-facebook-censorship/655335 [Accessed 29 September 2016].

Libération (16 November 2015) : “François Hollande annonce une révision de la Constitution”. Available at: http://www.liberation.fr/france/2015/11/16/francois-hollande-annonce-une-revision-de-la-constitution_1413859 [Accessed 30 September 2016].

Treppoz, E. (2014) : “L’extraterritorialité des injonctions sur un site internet, Mélanges en l’honneur du Professeur Bernard Audit”. Paris, France: L.G.D.J.

Whitman, R. (2012): “Circumventing Google’s Bouncer, Android’s anti-malware system”. Available at: http://www.extremetech.com/computing/130424-circumventing-googles-bouncer-androids-anti-malware-system [Accessed 27 September 2016].

CBS News (04 July 2016): “Beware downloading some apps or risk "being spied on"”. Available at: http://www.cbsnews.com/news/mobile-phone-apps-malware-risks-how-to-prevent-hacking-breach/ [Accessed 30 September 2016].

Steinhauer J.; Mazzetti M.; Hirschfeld Davis J. (2016): “Congress Votes to Override Obama Veto on 9/11 Victims Bill. Available at: http://www.nytimes.com/2016/09/29/us/politics/senate-votes-to-override-obama-veto-on-9-11-victims-bill.html?_r=0 [Accessed 30 September 2016].

CNIL (2016) : ”Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l’encontre de Google”. Available at: https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu [Accessed 30 September 2016].

Pilkington, E.; Roberts, D. (2016): “FBI and Obama confirm Omar Mateen was radicalized on the internet”, The Guardian. Available online at: https://www.theguardian.com/us-news/2016/jun/13/pulse-nightclub-attack-shooter-radicalized-internet-orlando [Accessed 30 September 2016].

Watt, H.M. (2003): "Yahoo! Cyber-Collision of Cultures: Who Regulates?". University of Michigan Law School.

Romm, T. (2016): "Court says Obama's Internet transition can go forward", *Politico.* Available at: http://www.politico.com/story/2016/09/obama-internet-transition-courts-228992 [Accessed 30 September 2016].

Akehurst, M. B. (1985): "International liability for injurious consequences arising out of acts not prohibited by international law", NYIL, volume 16, pp. 3-16.

Boyle, A. E. (1990): "State responsibility and international liability for injurious consequences of acts not prohibited by international law: a necessary distinction?", International and Comparative Law Quaterly, volume 39, pp. 1-26.

O'Neill, P. (2016): "ISIS recommends list of secure-messaging apps amid heated U.S. encryption debate", *The Daily Dot*. Available at: http://www.dailydot.com/layer8/isis-telegram-encryption-messenger-recommendations/ [Accessed 26 September 2016].

Légipresse (2014), Google condamné en référé à déréférencer des liens renvoyant vers des articles diffamatoires. N°320, pp. 522-523.

Finn, P.; Horwitz, S. (2013): "U.S. charges Snowden with espionage". Available at: https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html. [Accessed 30 September 2013].

Dyson, E.; Gilder, G.; Keyworth, G.; Toffler, A. (1994): "Cyberlaw and the American Dream: A Magna Carta for the Knowledge Age". Progress & Freedom Foundation.

McEvoy, C. (2013): "Google Dodges Class Action over Vulnerable Android Aps", *Law 360*. Available at: http://www.law360.com/articles/414105/google-dodges-class-action-over-vulnerable-android-apps [Accessed on 27 September 2016].

- **Reports**

Bhatt, A.; Silber M.: "Radicalization in the West: The Homegrown Threat" (2007), the New York City Police Department. Available at: http://eurabia.parlamentnilisty.cz/UserFiles/document/NYPD.pdf [Accessed 27 September 2016].

Arif, K. (2006), Informational Report No. 3964 conducted by Rapporteur Member of Parliament Kader Arif under the presidency of Member of Parliament Jean-Frédéric Poisson on ISIS' resources published on 13 July 2016. Available at: http://www.assemblee-nationale.fr/14/rap-info/i3964-tI.asp [Accessed 30 September 2016]

Von Behr, I.; Reding, A.; Edwards, C.; Gribbon L. (2013): Radicalisation in the digital era The use of the internet in 15 cases of terrorism and extremism", RAND. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf [Accessed 30 September 2016]

Report of the Secretary-General (2015), The United Nations Global Counter-Terrorism Strategy: "Plan of Action to Prevent Violent Extremism" (A/70/674). Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674 [Accessed 27 September 2016].

Executive Board, UNESCO (2015), Unesco's Role in Promoting Education as a Tool to Prevent Vioment Extremism, 197 EX/46. Available at: http://unesdoc.unesco.org/images/0023/002348/234879e.pdf [Accessed 27 September 2016].

OSCE (2014), Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach. Available at: http://www.osce.org/atu/111438?download=true [Accessed 27 September 2016].

Stevens T; Neumann P. (2009), Countering Online Radicalisation, A Strategy for Action, Policy report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR). Available at: http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf [Accessed 27 September 2016].

Directorate-General Justice, Freedom and Security, European Commission (2009), "Manual for trainers", Community Policing Preventing Radicalisation & Terrorism. Available at: http://www.coppra.eu/dl%5Cpreview%20trainers%20manual.pdf [Accessed 27 September 2016].

WSIS Executive Secretariat (2004), Report of the Geneva Phase of the World Summit on the Information Society, Geneva-Palexpo, 10-12 December 2003, WSIS-03/GENEVA/9(Rev.1)-E. Available at: https://www.forsaetisraduneyti.is/media/Onnur_Gogn_Innri/WSIS_2004.pdf [Accessed 27 September 2016].

La Rue, F. (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, United Nations, A/HRC/17/27. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [Accessed 27 September 2016].

Gagliardone, I.; Gal, D.; Alves, T.; Martinez, G. (2015), Countering Online Hate Speech, UNESCO Publishing. Available at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf [Accessed 27 September 2016].

NATO Cooperative Cyber Defence Centre of Excellence (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press. Available at: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [Accessed 30 September 2016].

OECD (2012), The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy, OECD Digital Economy Papers, No. 209. OECD Publishing, (p. 10). Available at: http://www.oecd-ilibrary.org/docserver/download/5k8zq930xr5j.pdf?expires=1475241639&id=id&accname=guest&checksum=87023F8929F48F6BB11888A067E1F0DC [Accessed 30 September 2016].

Linden, A. (2016), Qualified person's report on measures to withdraw, block and declassify unlawful websites through administrative channels. Paris, France: CNIL. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf [Accessed 30 September 2016].

EU Internet Referral Unit - Year One Report Highlights (2016), Europol. Available at: https://www.europol.europa.eu/content/eu-internet-referral-unit-year-one-report-highlights [Accessed 30 September 2016].

Cory, N. (2016), How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet". Washington, United States: Information Technology & Innovation Foundation. Available at: http://www2.itif.org/2016-website-blocking.pdf?_ga=1.176630501.1900676568.1475143839 [Accessed 30 September 2016].

Clean IT Project (2012) Detailed Recommendations Document for Best Practices and Permanent Dialogue. Available at: https://www.edri.org/files/cleanIT_sept2012.pdf [Accessed 30 September 2016]

Clean IT Project (2013), Reducing terrorist use of the Internet. Den Haag, Netherlands. Available at: https://www.nctv.nl/binaries/reducing-terrorist-use-of-the-internet_tcm31-30257.pdf [Accessed 30 September 2016].

ARTICLE 19 (2013), Internet intermediaries: Dilemma of Liability (2013). London, United Kingdom. Available at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf [Accessed 30 September 2016].

United Nations Counter-Terrorism Implementation Task Force - Working Group Compendium (2011), Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects. Available at: http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf [Accessed 30 September 2016]

Mackinnon, R.; Hickok, E.; Bar, A.; Lim H. (2014), Fostering freedom online: The role of internet intermediaries. Paris, France : UNESCO. Available at : http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [Accessed 30 September 2016].

Ducol, B. (2015), Devenir jihadiste à l'ère numérique : Une approche processuelle et situationnelle de l'engagement jihadiste au regard du Web. Québec : Université Laval. Available at : http://theses.ulaval.ca/archimede/fichiers/31398/31398.pdf [Accessed 30 September 2016].

Willetts, P. (2010), Non-Governmental Organizations in World Politics: The Construction of Global Governance. Milton Park, United Kingdom: Routledge. Available at: http://samples.sainsburysebooks.co.uk/9781136848537_sample_840287.pdf [Accessed 30 September 2016].

UNESCO (2015), Outcome Document of the "Connecting the Dots: Options for Future Action" Conference, 38 C/53 10. Available at: http://unesdoc.unesco.org/images/0023/002340/234090e.pdf [Accessed 30 September 2016].

Stephens, T.; French, D. (2014 and 2016), Study Group on Due Diligence in International Law. Lincoln, United Kingdom: International Law Association. Available at: http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045 [Accessed 30 September 2016].

- **Guidelines**

OECD (2011), Guidelines for Multinational Enterprises. Available at: http://www.oecd.org/daf/inv/mne/48004323.pdf [Accessed 27 September 2016].

UNESCO (2013), Riga Guidelines on Ethics in the Information Society. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/ifap/ifap_riga_guidelines_ethics_in_information_society_en.pdf [Accessed 27 September 2016].

Office of the High Commissioner (2011), Guiding Principles on Business and Human Rights, Implementing the United Nations "Protect, Respect and Remedy" Framework. Available at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf [Accessed 27 September 2016].

ISPA UK Code of Practice (1999, as amended in 2007). Available at: http://www.ispa.org.uk/about-us/ispa-code-of-practice/ [Accessed 30 September 2016].

Manila Principles on Intermediary Liability, Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation (Version 1.0, March 24, 2015). Available at: https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf [Accessed 30 September 2016]

Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001), International Law Commission, Supplement No. 10 (A/56/10), chp.IV.E.1. Available at: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Accessed 30 September 2016].

ICRC (2008), The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict. Available at: https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf [accessed 30 September 2016].

- **Government publications**

Home Office, Department for Culture, Media & Sport (2016), Speech: Baroness Shields calls for united action in tackling online extremism. Available at: https://www.gov.uk/government/speeches/baroness-shields-calls-for-united-action-in-tackling-online-extremism [Accessed 27 September 2016].

National Counter Terrorism Security Office, (2015), Guidance Online radicalization. Available at: https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation [Accessed 27 September 2016].

Secretary of State for the Home Department (2011), Prevent Strategy, Presented to Parliament by Command of Her Majesty. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf [Accessed 27 September 2016].

Royal Canadian Mounted Police, National Security Criminal Investigations (2009), Radicalization - A Guide for the Perplexed. Available at: http://publications.gc.ca/collections/collection_2012/grc-rcmp/PS64-102-2009-eng.pdf [Accessed 27 September 2016].

Digital Economy Bill 2016-17, introduced to the House of Commons and given its First Reading on 5 July 2016. Available at: http://services.parliament.uk/bills/2016-17/digitaleconomy.html [Accessed 30 September 2016].

House of Commons - Home Affairs Committee (2016), Radicalisation: the counter-narrative and identifying the tipping point, Eighth Report of Session 2016–17. Available at: http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/135.pdf [Accessed 30 September 2016].

Letter from the Attorney General of the United States to the Russian Minister of Justice (2013). Available at: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/26_07_13_attorney_general_letter_to_russian_justice_minister.pdf [Accessed 30 September 2016].

- **International Court of Justice Case Law**

United States of America v. Iran, Case Concerning United States Diplomate and Consular Staff in Tehran [1980], International Court of Justice.

- **United States of America Case law**

Psinet Incorporated v. Chapman III [2004], Case No. 01-2352 (United States Court of Appeals, Fourth Circuit).

Brandenburg v. Ohio [1969], 395 U.S. 444 (Supreme Court of the United States).

Snyder v. Phelps [2011], 562 U.S. 443 (Supreme Court of the United States).

Houchins v. KQED, Inc. [1978], 438 U.S. 1, 98 S.CR. 2588 (Supreme Court of the United States).

Reno v. American Civil Liberties Union [1997], 521 U.S. 844 (Supreme Court of the United States).

Stratton Oakmont, Inc. v. Prodigy Services Co. [1995], WL 323710 (N.Y. Sup. Ct.).

Cubby, Inc. v. CompuServe Inc. [1991], 776 F.Supp. 135 (S.D.N.Y.).

Barrett v. Rosenthal [2006], 146 P.3d 510 (Cal. S.C.).

Barnes v. Yahoo!, Inc. [2005], 570 F. 3d 1096 (D. Or.).

Green v. America Online. [2003], 318 F.3d 465 (Ct. App. 3rd Cir.)

Jane Doe No. 14 v. Internet Brands, Inc., DBA Modelmayhem.com [2014], No. 12-56638 (9th Cir.).

Clearcorrect Operating Llc and Clearcorrect Pakistan Ltd., v. International Trade Commission and Align Technology Inc. [2015], 2014-1527 (Ct. App. Fed. Cir.)

Susan Harvey v. Google Inc. and Does 1-20. [2015], 15-cv-03590 (Dis. C.t East. Dis. Cal. San Jose Div.)

Holder v. Humanitarian Law Project. [2010], 561 U.S. 1 (Supreme Court of the United States)

United States of America v. Tarek Mehanna [2013], 12-1461 (Ct. App. 1st Cir.)

Larry Elliott Klayman v. Mark Zuckerberg and Facebook Inc. [2014], 13-7017 (Ct. App. Dis. Col. Cir.)

Fields v. Twitter Inc. [2016], 16-cv-00213-WHO (Dis. Ct. Nor. Dis. Cal.)

Jane Doe No. 14 v. Internet Brands Inc. and DBA Modelmayhem.com [2014], 12-56638 (Ct. App. 9th Cir.)

Dawn Hassell et al. v. Ava Bird and Yelp Inc. [2016], A143233, (Ct. App. Cal.)

Tiffany Inc. v. eBay Inc. [2010], 600 F.3d 93 (Ct. App. 2nd Cir.)

Terminiello v. City of Chicago [1949], 337 U.S. 1 (Supreme Court of the United States)

In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 [2016] (Cal. Cent. Dis. Ct.)

Ligue contre le racisme et l'antisémitisme and Union des étudiants juifs de France v. Yahoo! Inc. and Société Yahoo! France [2004], 01-17424 (Ct. App. 9th Cir.).

Als Scan, Inc. v. Digital Service Consultants, Inc. [2002], 01-1812 (Ct App. 4th Cir.).

Scott Rilley v. MoneyMutual [2016], Case No. A14-1307 (Supreme Court of Minnesota).

Sarl Louis Feraud Intern. v. Viewfinder Inc. [2005], 406 F. Supp. 2d 274 (S.D.N.Y.).

- **Inter-American Court of Human Rights Case Law**

Fontevecchia and D'Amico v. Argentina [2011].

RCTV v. Venezuela [2015].

Lopez Lone et al. v. Honduras [2015].

Velez Restrepo y Familiares v. Colombia [2012].

Uzcategui y Otros v. Venezuela [2012].

Manuel Cepeda Vargas v. Colombia [2010].

Gomes Lund et al. v. Brazil [2010].

Rios (and Perozo) et al. v. Venezuela [2009].

Lopez Alvarez v. Honduras [2006].

Ricardo Canese v. Paraguay [2004].

Ivcher-Bronstein v. Peru [2001].

Claude Reyes et al. v. Chile [2006].

Olmedo-Bustos et al. v. Chile [2001].

Palamara-Iribarne v. Chile [2005].

Kimel v. Argentina ([2008].

Norín Catriman et al. (leaders, members and activists of the Mapuche Indigenous People) v. Chile [2014].

- **African Courts on Human Rights Case Law**

Burundian Journalists Union v. The Attorney General of the Republic of Burundi [2015], n°07-2013 (East African Court of Justice, First Instance Division).

Lohé Issa Konaté v. Burkina Faso [2014], n°004/2013 (African Court on Human and Peoples' Rights).

- **European Case law**

Kasymakhunov and Saybatalov v Russia [2013], Case No. 26261/05 and 26377/06 (European court of Human Rights).

Pavel Ivanov v. Russia [2007], Case No. 35222/04, 20 February 2007 (European court of Human Rights).

Norwood v. the United Kingdom [2004], Case No. 23131/03 (European court of Human Rights).

Bankovic and Others v. Belgium and 16 Other States [2001], Decision as to the admissibility of Application No. 52207/99, European Court of Human Rights, Grand Chamber

Ben El Mahi and Others v. Denmark [2006], Application No. 5853/06, European Court of Human Rights, Fifth Section

Delfi As v. Estonia [2015], 64569/09, European Court of Human Rights, Grand Chamber

SABAM v. Netlog [2012], Case C-360/10, Court of Justice of the European Union, Third Chamber

Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González [2014], Case C-131/12, Court of Justice of the European Union, Grand Chamber

UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH [2014], Case C-314/12, Court of Justice of the European Union, Fourth Chamber

Cengiz and Others v. Turkey [2015], 48226/10 and 14027/11, European Court of Human Rights, Chamber

Ahmet Yıldırım v. Turkey [2012], 3111/10, European Court of Human Rights, Second Section

GS Media BV v. Sanoma Media Netherlands BV and Others [2016], Case C-160/15, Court of Justice of the European Union, Second Chamber

Société Neptune Distribution v. Ministre de l'Économie et des Finances [2015], Case No. C-157/14 (European Court of Justice, Fourth Chamber).

Philip Morris Brands SARL e.a. v. Secretary of State for Health [2016], Case No. C-547/14 (European Court of Justice, Second Chamber).

Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen and Others [2014], Case C-201/13, Court of Justice of the European Union, Grand Chamber.

- **European National Courts Case Law**

Parquet général près la cour d'appel de Montpellier v. Cindy A. et a. [2016], 15-86412 (Cass. Crim.)

Tamiz v. Google Inc. [2013] EWCA Civ 68

Byrne v. Deane. [1937] 1 KB 818
Google Blogspot [2011] VI ZR 93/10 (BGH)

Google v. Vividown [2010],1972 (Milan Ct. 1st Inst.)

Google v. Vividown [2012] (Milan Ct. App.)

Google v. Vividown [2014], 5107/2014 (Ital. Supreme Court of Cassation)

Cartier International AG, Montblanc-Simplo GMBH, Richemont International SA v. British Sky Broadcasting Limited, British Telecommunications plc and others [2016] EWCA Civ 658 (Court of Appeal Civil Division).

UEJF v. Twitter Inc. [2013], 13/06106 (C.A. Paris, P. 1 ch. 5)

Association « L'oeuvre française » et a. [2014], 372322 (Conseil d'Etat)

Ministre de l'Intérieur v. Société Les Productions de la Plume et M. Dieudonné M'Bala M'Bala [2014], 374508 Conseil d'Etat

Ligue des droits de l'homme et autres - association de défense des droits de l'homme collectif contre l'islamophobie en France [2016], 402742 and 402777, Conseil d'Etat

Davison v. Habeeb [2011], EWHC 3031 (QB) HHJ Parties QC

Deltour, Perrin, Halet v. Ministère Public [2016]. Tribunal d'arrondissement du Luxembourg, douzième chambre.

Ligue contre le racisme et l'antisémitisme and Union des étudiants juifs de France v. Yahoo! Inc. and Société Yahoo! France [2000], 00/0538 (Tribunal de Grande Instance de Paris)

The People v. Felix Somm [1999], File no. 20 Ns 465 Js 173158/95 (Munich Regional Court)

- **Canadian Case Law**

Saskatchewan Human Rights Commission v. Whatcott [2013], 2013 SCC 11 (Supreme Court of Canada).

Equustek Solutions Inc v. Jack, [2014], BCSC 1063 (Supreme Court of British Columbia).

- **Australian Case Law**

Duffy v. Google Inc [2015] SASC 170 (Supreme Court of South Australia).

Gutnick v. Dow Jones [2002] HCA 56 (High Court of Australia).

- **Websites**

FBI (2016) Available at: www.cve.fbi.gov; [Accessed 27 September 2016**].**

Resist (2016), Available at: http://www.resist.com/ [Accessed 27 September 2016].

Stormfront (2016), Available at: https://www.stormfront.org/forum/ [Accessed 27 September 2016].
God hates fags (2016), Available at: http://www.godhatesfags.com/ [Accessed 27 September 2016].

Jew watch, Available at: http://www.jewwatch.com/ [Accessed 27 September 2016].

Info-radical (2016), Definition. Available at: https://info-radical.org/fr/radicalisation/definition/ [Accessed 27 September 2016].

Internet Corporation for Assigned Names and Numbers. Available at: https://www.icann.org/fr [Accessed 29 September 2016].

Internet Watch Foundation. Available at: https://www.iwf.org.uk/ [Accessed 29 September 2016].

INHOPE - International Association of Internet Hotlines, Available at: http://www.inhope.org/gns/home.aspx [Accessed 29 September 2016].

Center for Copyright Information - The Copyright Alert System. Available at: http://www.copyrightinformation.org/the-copyright-alert-system/ [Accessed 29 September 2016].

Google Play Developer Distribution Agreement (2016), Available at: https://play.google.com/about/developer-distribution-agreement.html [Accessed 30 September 2016].

Communications and Internet Services Adjudication Scheme. Available at: https://www.cedr.com/cisas/ [Accessed 29 September 2016].

CloudFlare, Inc. Available at: https://www.cloudflare.com/fr/ [Accessed 29 September 2016].

Wikipedia. Available at: https://www.wikipedia.org/ [Accessed 29 September 2016].

Women, Action, and the Media: WAM!. Available at: http://www.womenactionmedia.org/ [Accessed 29 September 2016].

Everyday Sexism Project. Available at: http://everydaysexism.com/ [Accessed 29 September 2016].
Tor Project: Anonymity Online. Available at: https://www.torproject.org/ [Accessed 29 September 2016].

Storymaps (2016), Available at: http://storymaps.esri.com/stories/2016/terrorist-attacks/ [Accessed 30 September 2016].

StopBadWare. Available at: www.stopbadware.org) [Accessed 24 September 2016].

Microsoft Corporate Blogs (2016) *Microsoft's approach to terrorist content online.* Available at http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.00001h2dtloh9jcwxu7z4shpvnryd [Accessed 30 September 2016].

ANNEX 1

Country Survey relative to the Report on

"Policy Options and Regulatory Mechanisms for Managing Radicalization on the Internet"

Prepared for the Conference

"Internet and the Radicalization of Youth: Preventing, Acting and Living Together"

Québec, Canada, October 31st and November 1st 2016.

***

Drawn up by individual specialist Dan Shefet

(1) Is the act of radicalization as such a penal offence in your country? **a) In the affirmative please list citations to the relevant statutes/regulations including a specific reference to the definition of radicalization employed.** **b) 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?**	**STATES**
a) Not directly. But sections 114 c, 114 d and 114 e of the Danish Criminal Code is applicable for recruitment, training and dissemination of terror propaganda. Section 114 c: (1) Imprisonment for a term not exceeding ten years is imposed on any person who recruits another person to commit or facilitate any act falling within section 114 or 114a or to join a group or an association for the purpose of facilitating the commission of illegal acts of this nature by the group or association. In particularly aggravating circumstances the sentence may increase to imprisonment for a term not exceeding 16 years. Especially situations involving offences committed in a systematic or organised manner are considered particularly aggravating circumstances. (2) Imprisonment for a term not exceeding six years is imposed on any person who recruits another person to commit or facilitate any act falling within section 114b or to join a group or an association for the purpose of facilitating the commission of illegal acts of this nature by the group or association. (3) Imprisonment for a term not exceeding six years is imposed on any person who accepts being recruited to commit any act falling within section 114 or 114a. If the relevant person is a member of armed forces, the sentence may increase to imprisonment for a term not exceeding ten years, or in particularly aggravating circumstances to imprisonment for a term not exceeding 16 years. Especially situations in which the relevant person has participated in combat are considered particularly aggravating circumstances. Section 114 d: (1) Imprisonment for a term not exceeding ten years is imposed on any person who trains, gives instruction to or otherwise teaches another person to commit or facilitate any act falling within section 114 or 114a knowing that such other person intends to use his skills for such purpose. In particularly aggravating circumstances, the sentence may increase to imprisonment for a term not exceeding 16 years. Especially situations involving offences committed in a systematic or organised manner are considered particularly aggravating circumstances. (2) Imprisonment for a term not exceeding six years is imposed on any person who trains, gives instruction to or otherwise teaches another person to commit or facilitate any act falling within section 114b knowing that such other person intends to use the skills acquired for such purpose. (3) Imprisonment for a term not exceeding six years is imposed on any person who accepts being trained, given instruction or taught how to commit any act falling within section 114 or 114a. Section 114 e: (1) Imprisonment for a term not exceeding six years is imposed on any person who otherwise facilitates the activities of a person, a group or an association committing or intending to commit an act falling within section 114, 114a, 114b, 114c or 114d (terrorism). (2) If the person affiliated to an armed force, can the imprisonment for a term exceed to ten years or under special circumstances exceed to sixteen years. Special circumstance can be if the person has participated in fighting.	Denmark
a) Terrorism Act 2006 section.2 makes it a criminal offence to encourage terrorism by directly or indirectly inciting or encouraging others to commit acts of terrorism. This includes an offence of "glorification" of terror – people who "praise or celebrate" terrorism in a way that may encourage others to commit a terrorist act. The maximum penalty is seven years' imprisonment.	United Kingdom

Since August 2015 with the coming into force of the Counter Terrorism and Security Act 2015, local authorities – along with schools, prisons and NHS trusts – are required to take specific action to stop people being drawn into terrorism under new rules that have been laid out in the new Anti-Radicalisation Law as part of the Counter Terrorism and Security Act, which states "a specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism." It is otherwise referred to as the "Prevent Duty". Part 5 of the Act addresses the risk of being drawn into terrorism. Chapter 1 creates a duty for specified bodies to have due regard, in the exercise of their functions, to the need to prevent people from being drawn into terrorism. It also gives the Secretary of State a power to publish guidance to which specified bodies must have regard when fulfilling this duty. The legislation puts the existing Prevent programme on a statutory footing. Chapter 2 provides that each local authority must have a panel to provide support for people vulnerable to being drawn into terrorism. The legislation puts the existing voluntary programme for people at risk of radicalisation on a statutory footing (in England and Wales this is the "Channel Programme").	
Article 13 of the Law 26/2015 on countering terrorism and the repression of money laundering, essentially paragraph 8. Article 6 of the Tunisian Constitution provides that the State "commits to prohibiting and preventing accusation of apostasy and incitement to hatred and violence and to contain them."	Tunisia
a) The Law 98/2014 "On prohibition of joining the armed conflicts outside the country of Albanian citizens", approved by the parliament on the 3rd of September 2014, amended the Penal Code by adding Article 231, 232 (a) and 265 that criminalizes the participation in foreign conflicts. Article 231 of the Criminal Code punishes "Recruitment of persons for the purpose of committing terrorist acts". Article 232 (a) of the Criminal Code punishes "Promotion, public call and propaganda for committing offenses with terrorist purposes", Article 265 (c) of the Criminal Code punishes the act of "Inciting hatred or disputes between nationalities, races and religions". The latter provides for a punishment up to 3 years in prison for calling for participation in violent military actions in a foreign country	Albania
a) The act of radicalization is not as such a penal offence. **b)** According to the Act C from 2012 which is in the Criminal Code, analogy - in a narrower sense - is forbidden in criminal cases. Section 1 of the CC sets the rules for the principle of legality. With that in mind, if an act, that can be regarded as radicalization - which does not enjoy an internationally accepted definition - coincides with the elements of a criminal offence provided by the Criminal Code [e.g. incitement to hatred (section 312), violence against a member of a community (section 216), homicide (section 160), public denial of the crimes of national socialist or communist regimes (section 333), libel (section 226), defamation (section 227), terrorist act (section 314) etc.], then the perpetrator can be brought to justice for that criminal act.	Hungary
a) Currently, the act of radicalization specifically is not a penal offence in India. The issue of radicalization, by and large, has not been legally addressed in India. **b)** Sometimes, cases pertaining to the same are sought to be addressed by invoking the incitement of hatred provisions, under existing law.	India
a) The pure act or process of radicalization (in terms of thoughts or beliefs without accompanying conduct) is not an offence in Australia.	Australia

The Australian Government's Criminal Code Act 1995 (Criminal Code) includes offences for conduct such as urging violence of advocating terrorism. Division 80.1 of the Commonwealth Criminal Code includes the following offences prohibiting urging violence and advocating terrorism: • Section 80.2A: Urging violence against groups—a person commits an offence if the person urges another person, or a group, to use force or violence against a group distinguished by race, religion, nationality, national or ethnic origin or political opinion intending that force or violence will occur. • Section 80.2B: Urging violence against members of groups—a person commits an offence if the person urges another person, or a group, to use force or violence against a person because they a member of a group distinguished by race, religion, nationality, national or ethnic origin or political opinion intending that force or violence will occur. • Section 80.2C: Advocating terrorism—a person commits an offence if the person advocates the doing of a terrorist act or the commission of a terrorism offence and is reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. The meaning of 'advocates' includes to 'counsel, promote, encourage or urge' the doing of a terrorist act or commission of a terrorism offence. The maximum penalties for these offences range from five to seven years' imprisonment. For each of these offences there is a specific defense available where the person's conduct was done in good faith. In addition, Australia's states and territories have enacted legislation applicable in their individual jurisdictions, prohibiting certain conduct related to racial hatred or racial vilification.	
a) The act of radicalization is not as such a penal offence. **b)** However, publishing radicalization content on the internet may constitute the offence of "incitement to hatred" (German term: "Volksverhetzung") under Section 130 of the German Criminal Code. According to that provision, criminal liability occurs where the offender, in a manner capable of disturbing the public peace 1. incites hatred against a national, racial, religious group or a group defined by their ethnic origins, against segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population or calls for violent or arbitrary measures against them; or 2. assaults the human dignity of others by insulting, maliciously maligning an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population, or defaming segments of the population. If the person publishing the content uses propaganda material of unconstitutional organizations this may, in addition, constitute an offence under Section 86 (Dissemination of propaganda material of unconstitutional organizations) or Section 86a (Using symbols of unconstitutional organizations) of the Criminal Code. Other provisions of the Criminal Code relevant for the prosecution of hate speech are: • Section 185 (insult). • Section 111 (Public incitement to crime) under which anyone who publicly, in a meeting or through the dissemination of written materials (including audio-visual media) incites the commission of an unlawful act, shall be held liable as an abettor to that act. • Section 130a (Attempting to cause the commission of offences by means of publication) under which anyone who disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (including audio-visual media) capable of serving as an instruction for certain severe unlawful acts and intended by its content to encourage or cause others to commit one of those acts, shall be liable. The same applies to anyone who disseminates or makes publicly available such material in order to encourage or cause others to commit such an act. • Section 140 (Rewarding and approving of offences) under which anyone who 1. rewards or 2. publicly, in a meeting or through dissemination of written materials (including audio-visual media), and in a manner that is capable of disturbing the public peace, approves of one of certain severe unlawful acts after it has been committed or attempted, shall be liable • Section 241 para 1 (Threatening the commission of a felony) under which anyone who threatens a person with the commission of a felony against him or a person close to him shall be liable.	Germany

a) The act of radicalization is not as such a penal offence. **b)** Hate speech" and "incitement to hatred" are offences under S.55(1)(b) of the Penal Code of Seychelles. "Apology for genocide" is not an offence. "Solicitation of murder" is an offence under S.377A and S.381 of the Penal Code. "Defamation" is a criminal offence under Chapter 18 of the Penal Code. Additionally, a broad offence of "Incitement to violence and disobedience of the law" is provided for under Section 89A of the Penal Code. These are existing provisions in law independent of whether internet radicalization is an offence or not.	Seychelles
a) The act of radicalization is not as such a penal offence. **b)** The Israeli criminal legislation contains several offences analogical to acts of radicalization. Incitement to racism (Sections 144A-144D1): • Section 144A – definition of racism: persecution, humiliation, degradation, a display of enmity, hostility or violence, or causing violence against a public or parts of the population, all because of their color, racial affiliation or national ethnic origin. • Section 144B – definition of the offence of prohibited publication: If a person publishes anything in order to incite to racism, then he is liable to five years' imprisonment. • Section 144C – definition of permitted publications: a true and fair report of an act defined in section 144B, or quotes from religious scriptures or prayer books or the observance of a religious ritual do not constitute offences, as long as they are not done with intent to incite to racism. • Section 144D – definition of the offence of possession of publications: If a person holds a prohibited publication, he is liable to one-year imprisonment. • Section 144E – an indictment for the above-mentioned offences shall only be brought pursuant to the Attorney General's written consent. Incitement to violence and terror (Sections 144D2-144D3): • Section 144D2 – definition of the offence of prohibited publication: If a person publishes calls to commit an act of violence or terror, or praise, words of approval, encouragement, support or identification with an act of violence or terror, then he is liable to five years' imprisonment. This section also provides that a true and fair report of such a publication does not constitute an offence. • Section 144D3 - definition of the offence of possession of publications: If a person holds a prohibited publication, he is liable to one-year imprisonment. • Section 144E - an indictment for the above-mentioned offences shall only be brought pursuant to the Attorney General's written consent. • Hate offences (Section 144F): • If a person commits an offence out of a racist motive as defined under Article 144A he shall be liable to double the penalty set for that offense or to ten years' imprisonment, whichever is the lesser penalty. Injury to religious sentiment (Section 173): • The offence criminalizes publications that are liable to crudely offend the religious faith or sentiment of others. Enticement (Solicitation) (Section 30): • If a person causes another to commit an offense by means of persuasion, encouragement, demand, and cajolery or by means of anything else that constitutes the application of pressure, then he entices to an offense. Defamation offences as well as the incitement to genocide are also offences that can be analogical to acts of radicalization.	Israel
a) The act of radicalization is not an offence termed in those explicit terms.	Slovakia

b) However, an act of radicalization is considered and can be subsumed under elements (subject of matter) of the offences of extremism. Penal offences of extremism are specified in section 140(a) of the Criminal Code: "Penal offences of extremism are the Crime of Supporting and Promoting Groups Aimed at Suppression of Fundamental Rights and Freedoms under § 421 and 422, Crime of Manufacturing of Extremist Materials to § 422a, Crime of Dissemination of Extremist Materials according to § 422 (b), Crime of Possession of Extremist Materials according to § 422c, Crime of Denial and Approval of the Holocaust and Crimes Committed in Political Regimes under § 422d, Crime of Defamation of Nation, Race and Belief under § 423, Crime of Incitement of National, Racial and Ethnic Hatred under § 424, Crime of Incitement, Defamation and Threatening to Persons because of their Affiliation to Race, Nation, Nationality, Complexion, Ethnic Group or Family Origin to § 424a and the offenses committed on specific motifs under § 140 point. d) and f)."	
a) The act of radicalization is not an offence termed in those explicit terms, but our Criminal Code does provide self-study to commit terrorist offenses as an expression of radicalization that leads to terrorism. **b)** According to Article 575.2º: "Any person who, with the same objective of enabling himself to carry out any of the offences defined in this Chapter (Terrorist Offences), carries out by himself any of the activities set out in the previous provision (instruction in military or combat matters, in technology for the development of chemical or biological weapons, in the manufacture or preparation of explosive, inflammable, incendiary or asphyxiating substances or apparatus), shall be punished by imprisonment for a period from two to five years. A person shall be understood to commit this offence if he intentionally in a habitual manner gains access to one or more communication services available to the public on-line or by way of the internet, or to an electronic communication service, the contents of which are intended or are particularly suited to give incitement to join a terrorist organization or group, or to collaborate with any such group or its aims." The Spanish Criminal Code also provides for offences such as incitement to hatred, hostility, discrimination or violence against individuals or groups because of their group membership, anti-Semitic or other reasons related to ideology, religion or belief, family status, belonging to an ethnic group, race or nation, national origin, gender, sexual orientation or gender-identity, illness or disability (Article 510.1º CC). Offence of dissemination of material that incites to the behavior described above (art.510.1b) CC). Offence of denial, trivialization or public glorification of genocide. There is an aggravated behavior when previous crimes are committed through a social media, internet or information technologies (Article 510.3 CC). Offence of incitement to commit any of the above offences or murder for discriminatory reasons aforementioned described (Article 17, 18, 22.4 and 138 CC).	Spain
a) Sweden has no criminal legislation specifically aimed at 'radicalization'. That term does not exist in Swedish criminal law. There are, however, certain provisions that impose criminal liability on those who urge or otherwise attempt to entice people to commit criminal acts. The Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crimes imposes particular criminal liability on those who in a message to the public, urge or otherwise attempt to entice people to commit particularly serious crime (public provocation) or seek to induce another person, in a case other than that specified above, to commit or otherwise participate in particularly serious crime (recruitment). 'Particularly serious crime' means inter alia terrorist offences, offences referred to in certain specified international agreements and other serious crimes if the intent is to intimidate a population or a group of population or to compel a government or an international organization to perform an act or abstain from acting. **b)** The Swedish Penal Code contains a provision on inciting rebellion. According to this provision a person who orally, before a crowd or congregation of people, or in a publication distributed or issued for distribution, or in	Sweden

other message to the public, urges or otherwise attempts to entice people to commit a criminal act shall be sentenced for inciting rebellion.	
a) Radicalization is an offence in Iraq. The Iraqi Constitution bans radicalization and spreading of radical ideology in its Article 7. The Counter Terrorism Law No. 13 of 2005 criminalized whomever persuades and promotes radicalization.	Iraq
a) The Criminal Code of Canada does not have a specific offence of radicalizing someone to commit a terrorism offence or a terrorist activity, but it does have numerous terrorism offences that can be used to address the active encouragement of someone to commit a "terrorism offence" or a "terrorist activity". The Criminal Code has a comprehensive set of terrorism offences and a definition of "terrorist activity". The Criminal Code definition of "terrorist activity" has two parts. First, "terrorist activity" means an act or omission that is committed in or outside Canada and that, if committed in Canada, is an offence referred to in different subsections of section 7 of the Criminal Code that implement various United Nations counter-terrorism conventions or protocols. These include, for example, the section 431.2 offence that implements the International Convention for the Suppression of Terrorist Bombings, and which is referred to in subsection 7(3.72) of the Criminal Code. The second part of the definition of "terrorist activity" reads, as follows: "an act or omission, in or outside Canada, (i) that is committed (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and (ii) that intentionally (A) causes death or serious bodily harm to a person by the use of violence, (B) endangers a person's life, (C) causes a serious risk to the health or safety of the public or any segment of the public, (D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C) … Canada has extensive criminal law provisions that address incitement to terrorism. First, by the operation of section 22 of the Criminal Code, a person who counsels the commission of any crime is a party to that offence. Subsection 22(3) of the Criminal Code defines "counsel" to include procure, solicit or incite. By section 464 of the Criminal Code, it is also a crime to counsel the commission of a crime which is not committed. Secondly, the definition of "terrorism offence", in section 2 of the Criminal Code, provides, in paragraph (d) of the definition, that "terrorism offence" includes conspiracy or an attempt to commit, or being an accessory after the fact to, or any counselling in relation to a terrorism offence. Thirdly, the definition of "terrorist activity" in subsection 83.01(1) of the Criminal Code includes a conspiracy, attempt or threat to commit a terrorist activity, or being an accessory after the fact or counselling in relation to any terrorist activity. Hence, someone who, for example, incites another (inciting being one way to counsel) to commit an act or omission that constitutes "terrorist activity" engages in "terrorist activity". "Terrorist activity" is a key element found in the definitions of many terrorism offences, such as knowingly facilitating a terrorist activity (section 83.19 of the Criminal Code), knowingly instructing any person to carry out a terrorist activity (section 83.22 of the Criminal Code), or committing an indictable offence that constitutes a terrorist activity (paragraph 2(c) of the Criminal Code definition of "terrorism offence").	Canada

For example, one of the terrorism offences in the Criminal Code is set out in subsection 83.18(1) of the Criminal Code, that of knowingly participating in or contributing to any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity. It has a maximum punishment of ten years' imprisonment. The term "participating in or contributing to an activity of a terrorist group" is defined to include providing, receiving or recruiting a person to receive training, or providing or offering to provide a skill or expertise for the benefit of a terrorist group. Thus, as previously indicated, counselling the commission of this terrorism offence, as for all terrorism offences, is a crime. Finally, there is also an offence of knowingly advocating or promoting the commission of terrorism offences in general while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed (section 83.221 of the Criminal Code). **b)** The Criminal Code contains three hate propaganda offences: advocating and promoting genocide against an identifiable group (subsection 318(1)), inciting hatred against an identifiable group in a public place that is likely to cause a breach of the peace (subsection 319(1)), and wilfully promoting hatred against an identifiable group other than in a private conversation (subsection 319(2)). "Identifiable group" is defined as any section of the public distinguished by colour, race, religion, national or ethnic origin, age, sex, sexual orientation or mental or physical disability. The offence of advocating or promoting genocide carries a maximum penalty of five years imprisonment, while the offences of inciting hatred or wilfully promoting hatred are punishable by a maximum penalty of two years imprisonment. These offences would be investigated by the relevant law enforcement agency where the crime took place. For the offences of advocating or promoting genocide and wilfully promoting hatred, Attorney-General consent is required before a prosecution can be instituted. By the application of subsections 22 and 464 of the Criminal Code, counselling the commission of murder is a crime, including whether or not the murder is committed. Canada also has a crime of publishing a defamatory libel knowing it to be false, found in section 300 of the Criminal Code, which has a maximum punishment of five years imprisonment. The lesser crime of publishing a defamatory libel, found in section 301 of the Criminal Code and which has a maximum punishment of two years imprisonment, has been held by some lower courts to be unconstitutional.	
a) Singapore does not have a specific penal offence against the act of radicalisation as such. However, the Internal Security Act is used preventively against radicalised individuals. **b)** The following penal laws in Singapore can be used to counter radicalisation. However, they can and have been used in in situations where the criminalised conduct would not amount to the level of radicalisation associated with terrorism and extremism leading to terrorism. • Sedition Act, which criminalises acts with a tendency to "promote feelings of ill-will and hostility between different races or classes of the population of Singapore." This law has been applied against material on the Internet. • Penal Code, section 298A, which makes it a criminal offence to knowingly promote or attempt to promote "disharmony or feelings of enmity, hatred or ill-will between different religious or racial groups", or to commit any act that the offender knows is "prejudicial to the maintenance of harmony between different religious or racial groups and which disturbs or is likely to disturb the public tranquillity." This law has been applied against material on the Internet. Separately, the Media Development Authority of Singapore (MDA) is empowered under the Broadcasting Act (BA) to issue and administer the Internet Code of Practice (ICOP), which Internet Service Providers (ISPs) and Internet Content Providers (ICPs) licensed under the Broadcasting (Class Licence) Notification are required to comply with. Individual news licensees are also required to comply with the ICOP as part of their licence conditions. The ICOP sets out what is considered as prohibited material, which includes: • Para 4f – "… whether the material depicts detailed or relished acts of extreme violence or cruelty".	Singapore

• Para 4g – "… whether the material glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance"." However, there are no penal sanctions under the BA for breaches of the ICOP. Instead, the BA allows MDA to take regulatory actions such as suspending/cancelling a broadcasting licence and imposing financial penalties (see section 12 of BA). Broadcasting without a licence could then attract criminal penalties under section 46 of BA. MDA may also direct ICPs to take down prohibited content that contravenes the ICOP and/or require that ISPs restrict access to such content (see section 16(1), (2) of BA), i.e. site blocking. The contravention of such directions may attract penal penalties (see section 16(3) of BA).	
a) No **b)** The Norwegian Penal Code criminalizes the following acts, not through analogy as mentioned, but as stand-alone crimes. The different offenses can in varying degree apply when a person is in the process of radicalization. (1) Participation in military operations against Norway (s. 119) (2) Terrorist acts (s. 131) (3) Terrorist conspiracy (s. 133) (4) Terrorist threats (s. 134) (5) Terrorist financing (s. 135) (6) Incitement, recruitment and instruction of terrorist acts, including training and being trained for terrorism (s. 136) (7) Participation in a terrorist organization (s. 136 a) (8) Aiding and abetting to evasion from punishment for terrorist acts (s. 137) (9) Hate speech (s. 185) (10) Public incitement to committing a criminal act (s. 183)	Norway
a) Article 3(15) of the Law on Intelligence and Security of 1999 (amended) provides for a definition of radicalization. It defines it as a process influencing an individual or group of individuals in such way that the said individual or group of individuals is mentally prepared or disposed to engage in terrorist acts." (originally in the Ministry Circular GPI 78 of 31 January 2014 of the Ministry of Interior relating to the processing of information in favor of an integrated approach of terrorism and violent radicalization by the police). However, the act of radicalization is not as such a penal offence in Belgium. Terrorist-related offences can be used to counter radicalization. • Article 140 bis of the Criminal Code prohibits public provocation to commit a terrorist offence • Article 140 quarter punishes the fact of giving instructions on how to create weapons to be used for terrorism. • Article 140 quinquies punished the fact of giving instructions or taking a course on how to commit a terrorist act. **b)** The Law of 30 July 1981prohibits racist or xenophobic acts and incitement to hatred or violence against a person, group, community, on the grounds of their race, skin color, ethnic or national identity, etc. These acts can be punished of 1 month to a 1-year imprisonment and / or from EUR50 to EUR 1000 fine.	Belgium

a) Pursuant to Article 12 D of the Prevention of Terrorism Act of 2012, No. 19 of 2014, s. 62, radicalization refers to "a person who adopts or promotes an extreme belief system for the purpose of facilitating ideologically based violence to advance political, religious or social change commits an offence and is liable on conviction, to imprisonment for a term not exceeding thirty years." **b)** Other offences are relevant: • According to Article 27 of the same Act, incitement is defined as "a person who publishes, distributes or otherwise avails information intending to directly or indirectly incite another person or a group of persons to carry out a terrorist act commits an offence and is liable, on conviction, to imprisonment for a term not exceeding thirty years. » • Article 30 C of the same Act provides: "(1) A person who travels to a country designated by the Cabinet Secretary to be a terrorist training country without passing through designated immigration entry or exit points shall be presumed to have travelled to that country to receive training in terrorism. (2) Despite subsection (l), a person who ordinarily resides in Kenya within an area bordering a designated country is exempt from the provisions of subsection (1)." • Article 13 of the National Cohesion and Integration Act from 2008 provides that: "(1) A person who— (a) uses threatening, abusive or insulting words or behavior, or displays any written material; (b) publishes or distributes written material; (c) presents or directs the performance the public performance of a play; (d) distributes, shows or plays, a recording of visual images; or (e) provides, produces or directs a programme, which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behavior commits an offence if such person intends thereby to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up. (2) Any person who commits an offence under this section shall be liable to a fine not exceeding one million shillings or to imprisonment for a term not exceeding three years or to both. (3) In this section, "ethnic hatred" means hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins."	Kenya[1]
a) The act of radicalization is not as such a penal offence under Japanese law. **b)** Other offences are relevant: • Japan enacted its first anti-hate speech law in May 2016. The Bill defines hate speech as unjust discriminatory words and behavior toward people of foreign origin, including threats of harm to their bodies or lives and significant insults, intended to incite exclusion from communities. However, there is no penalty for using hate speech in this law. • Under Article 230-1 of the Criminal Code of Japan: "(1) A person who defames another by alleging facts in public shall, regardless of whether such facts are true or false, be punished by imprisonment with or without work for not more than three (3) years or a fine of not more than 500,000 yen." • Article 61 of the Criminal Code: Any person who induces a crime, directly or through an intermediary, is subject to sentencing as though the inducer had been one of the material executors of the offence.	Japan[2]

[1] Official answer not received. Answers provided by the author's research team.

[2] Official answer not received. Answers provided by the author's research team.

a) Egyptian Law does not have a specific offence relating to the act of radicalization but has a number of provisions contained in its Anti-Terrorism Law of 2015 that touches upon the issue. • Article 1 of Anti-Terrorism Law of 2015: "In the application of the provisions of this Law, the following expressions and words shall bear the meaning indicated next to them: […] (B) Terrorist: Any natural person who commits, attempts to commit, incites, threatens, or plans a terrorist crime domestically or abroad by any means, even if individually, collaborates in such a crime in the context of a joint criminal venture, or commands, leads, manages, founds, or establishes or of any terrorist entity as stipulated in Article (1) of President of the Arab Republic of Egypt Decree by Law No. 8 of 2015 on the designation of terrorists, terrorist entities, or any person who funds such entities or contributes to their activity knowingly. (C) Terrorist Crime: Any offense stipulated in this Law and any felony or misdemeanor committed by using a means of terrorism or in order to achieve or carry out a terrorist act, call to commit any crime of the above, or threaten to commit such a crime, without prejudice to the provisions of the Criminal Code". […] • Article 6 of Anti-Terrorism Law 2015: "Incitement to commit a terrorist crime shall be punished with the same penalty prescribed for the completed offense, whether the incitement is directed at a specific person or group, in public or private, regardless of the method used, and even if such incitement does not result in any impact. Anyone who collaborates or helps, in any manner, to commit the offenses referred to in the first paragraph of this article shall be punished by the same penalty prescribed for the completed offense, even if the crime did not occur based on this agreement or assistance." • Article 28 of Anti-Terrorism Law of 2015: "Whoever promotes or prepares to promote, directly or indirectly, the perpetration of any terrorist crime, whether verbally, in writing, or by any other means, shall be punished by imprisonment for no less than five years. Indirect promotion shall include the promotion of ideas and beliefs inciting the use of violence by any of the means set forth in the preceding paragraph of this Article. The penalty shall be imprisonment for no less than seven years if the promotion occurs inside houses of worship, among members of the armed or police forces, or in locations belonging to such forces. Whoever possesses or acquires any public means of printing or recording used or intended for use, even if temporarily, for the purpose of printing, recording, or broadcasting the aforementioned shall be punishable by the same penalty set forth in the first paragraph of this Article." • Article 29 "Whoever establishes or uses a communications site, website, or other media for the purpose of promoting ideas or beliefs calling for the perpetration of terrorist acts or broadcasting material intended to mislead security authorities, influence the course of justice in any terrorist crime, exchange messages, issue assignments among terrorist groups or their members, or exchange information relating to the actions or movement of terrorists or terrorist groups domestically and abroad shall be punished by imprisonment with hard labor for no less than five years. Whoever unduly or illegally accesses websites affiliated with any government agency in order to obtain, access, change, erase, destroy, or falsify the data or information contained therein in order to commit an offense referred to in the first paragraph of this Article or prepare it shall be punishable by imprisonment with hard labor for no less than ten years." **b)** Other offences can be used to counter radicalization. Article 86 bis of the Criminal Code punished the participation in groups "the purpose of which is to call by any method, for interrupting the provisions of the constitution or laws, or preventing any of the Slate's institutions or public authorities from exercising its works, or encroaching on the personal freedom of citizens or other freedoms and public rights as guaranteed by the constitution or the law, or impairing the national unity or social peace." According to Article 98 F of the Criminal Code, "Detention for a period of not less than six months and not exceeding five years, or paying a fine of not less than five hundred pounds and not exceeding one thousand pounds shall be the penalty inflicted on whoever exploits and uses the religion in advocating and propagating	Egypt[3]

[3] Official answer not received. Answers provided by the author's research team.

by talk or in writing, or by any other method, extremist thoughts with the aim of instigating sedition and division or disdaining and contempting any of the heavenly religions or the sects belonging thereto, or prejudicing national unity or social peace".	
a) The act of radicalization is not as such a penal offence in Brazil. However, the Anti-Terrorism law of 2016 prohibits and punishes terrorist-related offences: • Promotion of and Preparation for Terrorism In addition, whoever promotes, creates, takes part in, or provides assistance to, in person or through an intermediary, a terrorist organization will be punished upon conviction with five to eight years in prison and a fine (id. art. 3). Whoever performs acts to prepare for acts of terrorism will receive the same punishment, which can be reduced by one-quarter to one-half of the punishment under circumstances not defined in the Law. (Id. art. 5.) • Terrorist Recruitment and Training The same punishment of five to eight years' imprisonment and a fine applies to those who, for the purpose of practicing acts of terrorism, recruit, organize, transport, or equip with ammunition individuals traveling to a country other than that of their residence or nationality or who provide or receive training in a country other than that of their residence or nationality. (Id. art. 5(§1).) • Terrorist Financing Receiving, providing, offering, obtaining, storing, keeping on deposit, requesting, or investing in any way (directly or indirectly) resources, assets, property, rights, valuables or money, or services of any kind for the planning, preparation, or execution of the crimes established in Law No. 13,260 will result in a sentence of 15 to 30 years in prison upon conviction. (Id. art. 6.) Whoever offers or receives, obtains, stores, keeps on deposit, requests, invests or otherwise contributes to the acquisition of assets or financial resources, in order to fund, in whole or in part, a person, group of people, association, organization, or criminal organization whose principal or secondary activity, even if occasionally, is the crimes set forth in Law No. 13,260 will incur the same punishment. (Id. art. 6 (sole para).) provisions contained in its Anti-Terrorism Law of 2015 that touches upon the issue. **b)** Brazilian legislation also condemns crimes against public peace, such as incitement to criminal behavior or apology of crime.	Brazil[4]
a) The act of radicalization is not as such a penal offence in Poland. However, a new Anti-Terrorism Law was adopted and signed by the President on June 22. It includes a provision for a 14-day detention without charge, for persons suspected of association with or involvement in an "act of a terrorist nature" acts. These include: the expression of "fundamentalist slogans" by representatives of Muslim institutions in Poland; information indicating the intent of a foreign national from a "high risk" country coming to Poland for academic training or to study; details relating to conferences/seminars/meetings of foreigners from "high risk" countries on Polish territory; details of plans to establish Islamic universities in Poland; information regarding the participation of Polish nationals in Internet platforms (chat rooms and forums) on so-called "radical Muslim websites"; and visits to detention/prison facilities by Islamic clerics or representatives of organizations associated with the Muslim faith. **b)** Other offences can be used to counter radicalization. • Article 119 of the Criminal Code: "§ 1. Whoever uses violence or makes unlawful threat towards a group of person or a particular individual because or their national, ethnic, political or religious affiliation, or because of their lack of religious beliefs, shall be subject to the penalty of the deprivation of liberty for a term of between 3 months and 5 years. § 2. The same punishment shall be imposed on anyone, who incites commission of the offence specified under § 1."	Poland[5]

4 Official answer not received. Answers provided by the author's research team.
5 Official answer not received. Answers provided by the author's research team.

• Article 255 of the Criminal Code: "§ 1. Whoever publicly incites to the commission of an offence, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years. § 2. Whoever publicly incites to the commission of a crime shall be subject to the penalty of deprivation of liberty for up to 3 years. § 3. Whoever publicly praises the commission of an offence, shall be subject to a maximum of 180 times the daily fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year." • Article 256 of the Criminal Code: "Whoever publicly promotes a fascist or other totalitarian system of state or incites hatred based on national, ethnic, race or religious differences or for reason of lack of any religious denomination shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years." • Article 257 of the Criminal Code: "Whoever publicly insults a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his lack of any religious denomination or for these reasons breaches the personal inviolability of another individual shall be subject to the penalty of deprivation of liberty for up to 3 years."	
a) The act of radicalization is not as such a penal offence in the United States. However, Section 2332b of the 18 U.S. Code regarding acts of terrorism transcending national boundaries sanctions threats to commit a terrorist act: "(a) Prohibited Acts. — (1) Offenses. —Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)— (A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or (B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States; in violation of the laws of any State, or the United States, shall be punished as prescribed in subsection (c). (2) Treatment of threats, attempts and conspiracies. — Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under subsection (c)."	United States of America[6]
a) The act of radicalization is not as such a penal offence in New Zealand. **b)** The Human Rights Act of 1993 provides for prohibitions that can help counter radicalization. • Section 61 Racial disharmony "(1) It shall be unlawful for any person: (a) to publish or distribute written matter which is threatening, abusive, or insulting, or to broadcast by means of radio or television or other electronic communication words which are threatening, abusive, or insulting; or (b) to use in any public place as defined in section 2(1) of the Summary Offences Act 1981, or within the hearing of persons in any such public place, or at any meeting to which the public are invited or have access, words which are threatening, abusive, or insulting; or (c) to use in any place words which are threatening, abusive, or insulting if the person using the words knew or ought to have known that the words were reasonably likely to be published in a newspaper, magazine, or periodical or broadcast by means of radio or television,—being matter or words likely to excite hostility against or bring into contempt any group of persons in or who may be coming to New Zealand on the ground of the colour, race, or ethnic or national origins of that group of persons." The Crimes Act of 1991 can also be useful:	New Zealand[7]

6 Official answer not received. Answers provided by the author's research team.
7 Official answer not received. Answers provided by the author's research team.

• Section 66 Parties to offences "(1) Every one is a party to and guilty of an offence who (a) actually commits the offence; or (b) does or omits an act for the purpose of aiding any person to commit the offence; or (c) abets any person in the commission of the offence; or (d) incites, counsels, or procures any person to commit the offence."	
a) The act of radicalization is not as such a penal offence in China. However, the Counter-Terrorism law of 2015 can be used to counter radicalized content. • Article 2 of the Counter-Terrorism Law (2015): "The State opposes all kinds of terrorism, bans terrorist organizations according to law, and pursues legal responsibilities of anyone who organizes, plots, prepares to carry out, or carry out terrorist activities; or who advocates terrorism, incites to commit terrorist activities, organizes, leads, joins terrorist organizations, or aids terrorist activities." • Article 3 of the Counter-Terrorism Law (2015) : "Terrorist Activities" as used in this law refers to the following acts of a terrorist nature: […] (2) Advocating terrorism, inciting others to commit terrorist activities, unlawfully possessing items that advocate terrorism, or compelling others to wear or bear clothes or symbols that advocate terrorism in a public place;" • Article 3 of the Counter-Terrorism Law: "Pursue criminal responsibility in accordance with law of those who organize, plan, prepare to implement, or carry out terrorist activities; or who advocate terrorism, who incite the carrying out of terrorist activities; who illegally possess items advocating terrorism; who force others to wear clothes or symbols advocating terrorism in public places; who organize, lead, or join terrorist organizations; who provide aid to terrorist organizations, terrorist personnel, the execution of terrorist activities or terrorist activity training." **b)** Offences under the Chinese Criminal Code can be used by way of analogy. • Article 120-3 of the criminal code: "Advocating terrorism or extremism through methods such as producing or distributing items such as books or audio-visual materials advocating terrorism; or advocating terrorism or extremism by giving instruction or releasing information; or inciting the perpetration of terrorist activity; is sentenced to up to five years imprisonment, short-term detention, controlled release or deprivation of political rights and a concurrent fine; where circumstances are serious, the sentence is five or more years imprisonment and a concurrent fine or confiscation of property." • Article 120-4 of the criminal code: "Using extremism to incite or coerce the masses to undermine the implementation of legally established systems such as for marriage, justice, education or social management is sentenced to up to three years imprisonment, short-term detention or controlled release and a concurrent fine; where circumstances are serious, the sentence is between three and seven years imprisonment and a conncurrent fine; where circumstances are especially serious, the sentence is seven or more years imprisonment and a concurrent fine or confiscation of property." • Article 120-5 of the criminal code: "Where methods such as violence or coercion are used to compel others to wear or adorn themselves with apparel or emblems promoting terrorism or extremism, it is punished by up to three years imprisonment, short-term detention or controlled release, and a concurrent fine."	China[8]
a) The act of radicalization is not as such a penal offence in Argentina.	Argentina[9]

[8] Official answer not received. Answers provided by the author's research team.
[9] Official answer not received. Answers provided by the author's research team.

b) Other offences can be used to counter radicalization. Article 41 of the reformed criminal code doubles the penalties for any crime committed with the aim of terrorizing the people or pressuring the national authorities or foreign governments or agents of an international organization to take some action. Article 213 the Argentine Criminal Code provides for the offence of advocacy of crime.	
a) Yes. 1) Administration of Criminal Justice Act, 2015. 2) Cybercrime (Prohibition and Prevention) Act, 2015. 3) Terrorism (Prevention) (Amendment) Act, 2013. The Terrorism Act of 2013 can be used to counter radicalization. • Section 1: "(2) A person or a body in or outside Nigeria directly or indirectly willingly (a) does, attempts or threatens any act of terrorism, (b) commits an act preparatory to or in furtherance of an act of terrorism, (c) omits to do anything that is reasonably necessary to prevent an act of terrorism, (d) assists or facilitates the activities of persons engaged in an act of terrorism or is an accessory to any offence under this Act, (e) participates as an accomplice in or contributes to the commission of any act of terrorism or offences under this Act, (f) assists, facilitates, organizes or directs the activities of persons or organizations engaged in any act of terrorism, (g) is an accessory to any act of terrorism, or (h) incites, promises or induces any other person by any means whatsoever to commit any act of terrorism or any of the offences referred to in this Act, commits an offence under this Act and is liable on conviction to maximum of death sentence." • Section 5: "(1) Any person who knowingly, in any manner, directly or indirectly, solicits or renders support - (a) for the commission of an act of terrorism, or (b) to a terrorist group, commits an offence under this Act and is liable on conviction to imprisonment for a term of not less than twenty years. (2) For the purposes of subsection (1) of this section, "support" includes - (a) incitement to commit a terrorist act through the internet, or any electronic means or through the use of printed materials or through the dissemination of terrorist information;" • Section 11: "Any person, who knowingly (a) incites or promotes the commission of a terrorist act, (b) incites or promotes membership in a terrorist group, or (c) solicits property for the benefit of a terrorist group or for the commission of a terrorist act, commits an offence and is liable on conviction to imprisonment for a term of not less than twenty years."	Nigeria[10]
a) The act of radicalization is not as such a penal offence in the United Arab Emirates. However, other offences can be used to counter radicalization.	United Arab Emirates[11]

[10] In addition to the official answer, information provided by the author's research team.

[11] Official answer not received. Answers provided by the author's research team.

- Article 34 of Federal Law No. (7) of 2014 On Combating Terrorism Offences:

"1. Temporary imprisonment for no more than 10 years shall be imposed on whoever knowingly promotes or supports a terrorist organisation, person or offence, whether verbally, in writing or by any other method.
2. Temporary imprisonment for no more than 10 years shall be imposed on whoever:
a- Knowingly possesses, in person or through someone else, any documents, print or recordings of any kind, that encompass promotion or supporting of any terrorist organisation, person or offence if intended for distribution or access by others.
b- Knowingly possesses or acquires any printing, recording or publishing mean used or intended to be used, even if temporarily, for the printing, recording, circulating or publishing any of the aforementioned."

b) Other offences can be useful.

- Article 26 of the Federal Decree-law no. (5) of 2012 on Combating Cybercrimes:

"Shall be punished by imprisonment for a period of at least five years and a fine not less than one million dirhams and not in excess of two million dirhams whoever establishes, manages or runs a website or publishes information on the computer network or information technology means for the interest of a terrorist group or any unauthorized group, association, organization, or body with the intent to facilitate communication with their leaders or members or attract new members, or to promote or praise their ideas, finance their activities or provide actual assistance thereof or for the purpose of publishing methods for manufacturing incendiary devices or explosives or any other devices used in terrorism acts".

- Article 7 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred:

"Any person, who commits any act involving hate speech by any means of expression or by any other means, shall be sentenced to imprisonment for a period not less than five years and to a fine not less than five hundred thousand dirhams and not exceeding one million dirhams or either one of these two penalties."

- Article 10 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred:

"Any person, who misuses religion to call individuals or groups as infidels by any means aiming to achieve their own interests or illegal purposes, shall be sentenced to temporary imprisonment. The sentence shall be death penalty if the call of infidelity was associated with death, and where the crime was committed as a result thereof."

- Article 11 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred:

"Any person who produces, manufactures, promotes, offers for sale or circulates products, goods, publications, recordings, movies, tapes, discs, software, smart applications or information in the field of electronic service or any other industrial materials or other things involving the means of expression, which may incite to commit blasphemy, or provoke discrimination or hate speech, shall be sentenced to imprisonment for a period not exceeding seven years and to a fine of not less than five hundred thousand dirhams and not exceeding two million dirhams."

- Article 12 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred:

"Any person, who acquires or possesses documents, publications, recordings, movies, tapes, discs, software, smart applications or information in the field of electronic services or any industrial materials or other things involving the means of expression that are intended for distribution or open for public aiming to offend religions, provoke discrimination or hate speech, shall be sentenced to imprisonment for a period not less than one year, and to a fine not less than fifty thousand dirhams and not exceeding two hundred thousand dirhams. Moreover, the same punishment shall apply to any person who acquires or possesses any means of printing, recording, storage, sound or visual recording devices or other means of publication, broadcasting or promotion that are used, with his knowledge, in the commission of any of the crimes set forth in the present Federal Decree."

- Article 13 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred

"Any person, who establishes, sets up, organizes or manages an association, centre, entity, organization, league or group or any branch thereof or uses any other means aiming to offend religions, or provoke discrimination or hate speech or any act involving encouragement or promotion of the same shall be sentenced to imprisonment for a period not less than ten years."

a) The act of radicalization is not as such a penal offence in France. **b)** Other offences can be used to counter online radicalization. • Article 24 of the Press Law of 1881 criminalizes incitement to racial discrimination, hatred, or violence on the basis of one's origin or membership (or non-membership) in an ethic, national, racial, or religious group. • Article 6 of Law No. 2004-575 of 21 June 2004 on confidence in the digital economy provides for the blocking of websites inciting racial hate and for one-year imprisonment and a 15 000 euro fine for the publisher. • Article R 625-7 of the Criminal Code makes it an offense to incite to racial hate via private communication.	France[12]
a) The act of radicalization is not as such a penal offence in Tanzania. However, other terrorist-related offences can be used to counter radicalization. • Article 6 (1) of the Prevention of Terrorism Act of 2002: "Where two or more persons associate for the purpose of, or where an organization engages in any act for the purpose of; […] (b) promoting, encouraging or exhorting others to commit an act of terrorism; or […]" • Article 7 (1) of the Prevention of Terrorism Act 2002. A person commits an offence who, in any manner or form; (a) solicits support for, or tenders support in relation to, an act of terrorism, or (b) solicits support for, or tenders support to, a proscribed organization. (2) "Support" as used in subsection (1), means and includes; (a) instigation to the cause of terrorism; (c) offering of or provision of moral assistance, including invitation to adhere to a Proscribed organization; […] • Article 25 (1) of the Prevention of Terrorism Act 2002. "Every person who […] (b) professes to be a member of, a terrorist group, is guilty of an offence and shall, on conviction, be liable to imprisonment for term not less than eighteen years." Moreover, there are relevant provisions as stipulated in the Part II of the Cybercrime Act of 2015. • Article 16 - Publication of false information "Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or counseling commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both." • Article 17 - Racist and xenophobic material "(1) A person shall not, through a computer system - (a) Produce racist or xenophobic material for the purposes of distribution; (b) Offer or make available racist or xenophobic material; or (c) Distribute or transmit racist or xenophobic material. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both."	Tanzania[13]

[12] Official answer not received. Answers provided by the author's research team.

[13] Official answer not received. Answers provided by the local UNESCO delegate and the author's research team.

• Article 18 - Racist and xenophobic motivated insult **"**(1) A person shall not insult another person through a computer system on the basis of race, color, descent, nationality, ethnic origin or religion. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both. • Article 19 - Genocide and crimes against humanity **"**(1) A person shall not unlawfully publish or cause to be published, through a computer system, a material which incites, denies, minimizes or justifies acts constituting genocide or crimes against humanity. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than ten million shillings or to imprisonment for a term of not less than three years or to both. (3) For the purpose of this section, "genocide" shall have a meaning ascribed to it under the Convention on the Prevention and Punishment of the Crime of Genocide, 1948."	
a) The act of radicalization is not as such a penal offence in the Federation of Russia. However, other terrorist-related offences can be used to counter radicalization. • Article 205 of the Criminal Code reads: "1. Terrorism, that is, the perpetration of an explosion, arson, or any other action endagering the lives of people, causing sizable property damage, or entailing other socially dangerous consequences, if these actions have been committed for the purpose of violating public security, frightening the population, or exerting influence on decision-making by governmental bodies, and also the threat of committing said actions for the same ends, shall be punishable by deprivation of liberty for a term of five to ten years. 2. The same deeds committed: a) by a group of persons in a preliminary conspiracy; b) repeatedly; c) with the use of firearms shall be punishable by deprivation of liberty for a term of eight to fifteen years. 3. Deeds stipulated in the first or second part of this Article, if they have been committed by an organized group or have involved by negligence the death of a person, or any other grave consequences, and also are associated with infringement on objects of the use of atomic energy or with the use of nuclear materials, radioactive substances or sources of radioactive radiation, shall be punishable by deprivation of liberty for a term of 10 to 20 years. Note: A person who has taken part in the preparation of an act of terrorism shall be released from criminal responsibility if he facilitated the prevention of the act of terrorism by timely warning governmental bodies, or by any other method, unless the actions of this person contain a different corpus delicti." • Article 205.1. Involvement of a Person in the Commission of Crimes of Terrorist Nature or Otherwise Assisting in Their Commission "1. Involvement of a person in the commission of the crime stipulated by Articles 205, 206, 208, 211, 277 and 360 of this Code or persuading a person to participate in a terrorist organization, the arming or training of a person with the aim of perpetrating the said crimes as well as the financing of an act of terrorism or an terrorist organization shall be punishable by deprivation of freedom for a term of four to eight years. 2. The same deeds perpetrated by the person repeatedly or through the use of his official position shall be punishable by deprivation of freedom for a term of seven to fifteen years with confiscation of property, or without such confiscation. Note. A person who has committed the crime specified in this Article shall be released from criminal responsibility if through his voluntary and timely warning of the authorities or otherwise he assisted to prevent the act of terrorism or suppress the crime of terrorist nature named in this article, unless the actions of this person contain a different corpus delicti." • Article 208. Organization of an Illegal Armed Formation, or Participation in It "1. Creation of an armed formation (unit, squad, or any other group) that is not envisaged by a federal law, and likewise operating of such a formation, shall be punishable by deprivation of liberty for a term of two to seven years.	Russia[14]

[14] Official answer not received. Answers provided by the author's research team.

2. Participation in an armed formation that is not provided for by a federal law shall be punishable by restraint of liberty for a term of up to three years, or by arrest for a term of up to six months, or by deprivation of liberty for a term of up to five years. Note: A person who has ceased to take part in an illegal armed formation of his own free will, and has handed in his weapons, shall be released from criminal responsibility unless his actions contain a different corpus delicti." **b)** Hate speech offences can also be used. Article 1 of the Federal Law No. 114-FZ contains a definition of extremist materials. It includes: (1) calling for extremist; (2) supporting the necessity of extremist activity; (3) justifying the necessity of extremist activity; and (4) extremist information by virtue of the law.	
(2) 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?	**STATES**
It follows from section 23 of the Criminal Code that the penalty provided for an offence also applies to those who are intermediaries. Section 23 also applies in regards to sections 114 c, 114 d and 114 e in the Criminal Code. • Section 23 "(1) The penalty provided for an offence applies to everybody who is complicit in the act by incitement or aiding and abetting. The punishment may be reduced where a person intended only to provide minor assistance or support an intent already formed, and where the offence has not been completed or intentional complicity failed. (2) The punishment may also be reduced where a person is complicit in the breach of a special duty to which he is not subject. (3) Unless otherwise provided, the punishment for complicity in offences that do not carry a sentence of imprisonment for a term exceeding four months may be remitted where the accomplice intended only to provide minor assistance or support an intent already formed, and where his complicity was due to negligence."	Denmark
Specified authorities will be expected to ensure those accessing the internet are safe from terrorist and extremist material that could lead to radicalisation. Councils will need to demonstrate they are protecting citizens – in particular children – from being drawn into terrorism by establishing appropriate levels of internet filtering and putting safeguarding policies in place to identify those who may be at risk, and intervening as appropriate. Local councils will be required to make checks on the use of its public buildings, its internet filters and any unregulated out of school settings, including after-school clubs and groups, supplementary schools and tuition centres to support home education. Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This guidance is issued under section 29 of the Act. The Act states that the authorities subject to the provisions must have regard to this guidance when carrying out the duty. Also see Schedule 6 for the Specified Authorities who have a duty to prevent extremism. http://www.legislation.gov.uk/ukpga/2015/6/schedule/6/enacted The Internet Service Providers' Association gave evidence to the Committee claiming that ISPs were happy to comply with take down requests under the Terrorism Act but were otherwise "not best placed to determine what constitutes violent extremism and where the line should be drawn". "This is particularly true of a sensitive area like radicalisation, with differing views on what may constitute violent extremist," the Association said.	United Kingdom
Yes, by analogy with the text of the Law on the countering of terrorism: notably Article 5 and 7.	Tunisia
No.	

	Albania
According to Art. 12 of the Criminal Code the perpetrator - of a crime that is defined in the Criminal Code - includes the offender (who actually commits the crime), the indirect offender (who is a person who commits the intentional criminal offence by using another person who cannot be punished for a specific, e.g. reason of minority, mental disorder etc.) and the co-actor (who is engaged in the commission of an intentional criminal offence jointly, having knowledge of each other's activities) (hereinafter together as: offenders), as well as the instigator (who intentionally persuades another person to commit a criminal offence) and the abettor (who intentionally helps another person to commit a criminal offence) (hereinafter together as: accomplices). Moreover, it can be mentioned that the Criminal Code also provides the rules for the punishability regarding attempt and preparation (sections 10-11 of the Criminal Code)	Hungary
Currently, India does not extend criminal penalty on Internet radicalization for intermediaries. However, India recognizes intermediaries as distinct legal entities. Further, under Section 79 of the Indian Information Technology Act, 2000, intermediaries have mandated to exercise due diligence while discharging their obligations under the law. Various parameters for due diligence have been defined under the law. The word "radicalization does not find mention amongst the kind of information that intermediaries are mandated to inform the users of their computer resources not to host, display, upload, transmit or publish or share the relevant information. However, intermediaries are mandated to inform their users that they shall not use intermediaries' platform for violating any law for the time being in force or for public order for incitement to the commission of any cognizable offence. Further, such intermediaries are required to inform their users that they shall not host, display, modify, publish, transmit, update or share any information on the intermediaries' computer resources that is grossly harmful, harassing, blasphemous, defamatory, libelous, hateful, racially or ethnically objectionable or otherwise unlawful in any manner whatsoever.	India
Pursuant to section 11.2 of the Criminal Code, it is an offence for a person to aid, abet, counsels or procure the commission of another offence ('complicity and common purpose').	Australia
German criminal law does not explicitly extend the penal liability for internet radicalization. Unless the law expressly provides for criminal liability based on negligence (which is not the case as regards the offences mentioned above) only intentional conduct attracts criminal liability. Thus intermediaries cannot usually be considered to have committed one of the offences mentioned above themselves. However, depending on the individual case, intermediaries could be liable in accordance with the provisions for abetting or for aiding. According to Section 26 of the Criminal Code any person who intentionally induces another to intentionally commit an unlawful act (abettor) is liable to be sentenced as if he were a principal. According to Section 27 of the Criminal Code any person who intentionally assists another in the intentional commission of an unlawful act shall be convicted and sentenced as an aider. When applying those provisions the special rules for host providers must be regarded though. Under Article 14 of the EU e-commerce Directive (Directive 2000/31/EC) and the corresponding German implementing legislation a host provider shall not be liable for the information that he stored at the request of the recipient of his service on condition that (a) the provider does not have actual knowledge of illegal activity or information and (b) the provider, upon obtaining such knowledge, acts expeditiously to remove or to disable access to such information. Thus host providers are normally exempt from criminal liability. Besides criminal liability, intermediaries may be subject to media law and youth protection law. Under the relevant pieces of that legislation (Rundfunkstaatsvertrag der Länder - Inter-state Treaty on Broadcasting - and Jugendmedienschutz-Staatsvertrag - Inter-state Treaty on the Protection of Human Dignity and the Youth in electronic media -) the competent supervisory authority may order the blocking of the whole or parts of a service violating laws provided the blocking is proportionate and its purpose cannot be achieved otherwise. However, according to jugendschutz.net, the competence centre for the protection of children and young people on the Internet and one of the German hotlines, the most effective way to remove illegal content is to notify the relevant host providers and request them to take down the illegal hate speech content. In the framework of the	Germany

Task Force „Together Against Hate Speech“ (see below Q8) the internet companies (Google/YouTube, Facebook, Twitter) committed themselves to remove illegal hate speech quickly. Alternatively, reports can be transferred to the Federal Review Board for Media Harmful to Minors (Bundesprüfstelle für jugendgefährdende Medien - BPjM), which is able to enter content into the list of media harmful to minors. For such content restrictions for its distribution to young people apply under youth protection legislation.	
If the offences in the Penal Code analogous to radicalisation as described in 1(b) are committed, the offences of abetment/complicity/conspiracy would arise. There is however no specific law that addresses the liability of intermediaries on internet radicalisation.	Seychelles
The Israeli Penal Law enables extending penal liability to intermediaries.	Israel
In Slovak national law there is no concrete crime that would deal with internet radicalization explicitly. In connection with internet Criminal code deals with the term “publicly” that serves as determination of the way how was the crime committed. “Publicly” is defined as: *„The criminal offence is considered as having been committed in public if it is committed* *a) through the content of a printed matter or a disseminated written material, through a film, through the radio, television, with the use of a computer network, or using the means of similar effect, or* *b) in the presence of more than two persons“* but there is need to be mentioned that this element of publicity serves as the aggravating circumstance. Following mentioned information, we can assume that also intermediaries could be liable for the internet radicalization but with presumption that they would fill all elements of crime (e.g. intention, object etc.). Intermediaries shouldn´t be fully responsible for the contain of the web site. We deduce this thesis from the Judgment of the Court of the Justice of the EU (further only, ECJ”) from 16th February 2012, C-360/2010, SABAM, ECLI:EU:C:2012:85. Generally, this case was connected with violation of copyright, but that could be also considered as the crime and ECJ was questioning liability of intermediaries. Result was that liability of intermediaries of any website for its content is limited, if they only store information, respectively content provided by users of the website, at his request, and if intermediaries are not aware of the illegality of content storage or unlawful user activity, and if intermediaries found out that there is some of illegal content they eliminate that from the web site or at least prevent access to it. Therefore, we think that intermediaries could be liable but not in every single case.	Slovakia
Once fulfilled the requirements established by the law, intermediaries, whether natural or legal persons, could be led criminally liable. This liability is regulated both in the Criminal Code and in specific legislation on services of the information society and electronic trade (Law 34/2002) in case intermediaries (service providers) are aware that they host illegal content, and do not voluntarily proceed to the withdrawal of such content.	Spain
Sweden has no criminal legislation on internet radicalization. Punishment for public provocation and recruitment as provided for in the Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crimes and inciting rebellion in the Penal Code shall be imposed not only on the person who committed the act but also on anyone who furthered it by advice or deed. Special rules apply when the crime has been committed through media protected by the Fundamental Law on Freedom of Expression, inter alia part of the internet. In such cases the principle of sole responsibility prescribes that only one person in a chain of responsibility – in most cases the publisher – may be held criminally liable. Furthermore, there is no liability for instigation of the crime or aiding the crime.	Sweden
	Irak

Any criminal act that a main person convicted for has extended liability for partners, cooperators and persuaders under same crime act based of articles 47, 48,49 of Iraqi penal law no. 111 of year 1969.	
Penal liability is determined by the application of the various terrorism offences, including counselling the commission of, attempting to commit, conspiring to commit, or being an accessory after the fact to the commission of, such offences. The concepts of counselling, attempting, conspiring, or being an accessory after the fact have long been part of the English common law and they appear in statutory form in the Criminal Code.	Canada
There is no penal liability for internet radicalisation, but the following statutes are applicable in relation to the Acts mentioned in the response to question 1: • Under the Sedition Act, an intermediary that intentionally publishes seditious publications would be liable for sedition. • Under the Penal Code, an intermediary that conspires to commit the relevant offence would be criminally liable. • Under the Broadcasting Act, broadcasting without a licence, or in contravention of MDA's directions, can attract criminal penalties.	Singapore
Norway has not criminalized internet radicalization as such. For the abovementioned offences, an intermediary can be held responsible on the basis of complicity under certain circumstances (Norwegian Penal Code s. 15).	Norway
In Belgium, liability (not necessarily criminal) of intermediaries is dealt by Articles XII.1 to XII.20 of the Code of Economy Article XII.17 – Mere conduit activity: In case of the providing of a service regarding the transfer, on a communications network, of data provided by the user or regarding the access to a communications network, the service provider is not responsible of the transmitted data, if the following conditions are met: 1) is not an initiator of the transmission, 2) does not select the recipient of data, and 3) does not delete or modify the data being subject to transmission. […] Article XII.18 - Storage under temporary copies of data In case of the providing of a service regarding the transfer, on a communications network, of data provided by a user, the service provider is not liable for the automatic, temporary and intermediary storage of that data […] if the following conditions are met: 1) the service provider does not modify the data; 2) the service provider complies with the conditions of access to data; 3) the service provider complies with the rules relating to the updating of the data […] 4) the service provider does not violate the legal use of technology, largely recognized and used in the industry; 5) the service provider acts promptly for the removal of the data stored or to make access to the said data impossible when it has knowledge of the data behind the transmission has been removed from the network or of the fact that the access to the data has been made impossible, or of the fact that an administrative authority or judicial authority has ordered the removal of the data or of rendering the access to the latter impossible, in accordance with article XII.19, §3. Article XII.19. § 1- Hosting activity In case of the providing of a service consisting in the storage of data provided by a user, the provider is not liable for the data stored under the request of the user if: 1° the provider did not have knowledge of the activity or of the illicit data, or, regarding civil actions in compensation, it did not have knowledge of the facts or circumstances showing the illicit nature of the activity or data; or 2° the provider act promptly when knowing the fact sin order to remove the data or make the access impossible and if it complies with the procedure described in paragraph 3.	Belgium

§2 Paragraph 1 does not apply when the user of the service acts under the authority or under the control of the provider. §3 When the provider has knowledge of an illicit activity or data it communicates it immediately to the King's Attorney General who takes the useful measures in accordance with Article 39 bis of the Criminal Code. […] Article XII.20 - Monitoring obligation § 1. For the providing of the services mentioned in Articles XII.17, XII.18 et XII.19, the providers do not have any general obligation to monitor data transferred or stored, nor a general obligation to actively research the facts or circumstances relating to illicit activities. […] The former paragraph foes not prevent competent judicial authorities to impose a temporary monitoring obligation in a specific case, when such possibility is provided for in the law. §2. Providers mentioned in paragraph 1 have an obligation to inform without delay competent judicial or administrative authorities of illicit activities that users would be engaged in, or illicit data that the latter would provide. […] The same providers have the obligation to communicate to the competent judicial or administrative authorities, at their request, all data they dispose and useful to seek out and ascertain offences committed through them.	
Pursuant to Article 62 of the National Cohesion and Integration Act from 2008, "(1) any person ho utters words intended to incite feelings of contempt, hatred, hostility, violence or discrimination against any person, group or community on the basis of ethnicity or race, commits an offence and shall be liable on conviction to a fine not exceeding one million shillings, or to imprisonment for a term not exceeding five years, or both. (2) A newspaper, radio station or media enterprise that publishes the utterances referred to in subsection (1) commits an offence and shall be liable on conviction to a fine not exceeding one million shillings."	Kenya
The Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders Act No. 37 of 2001 limits the extension of liability to ISPs. • Article 3 - Limitation of Liability for Damages: "1) When any right of others is infringed by information distribution via specified telecommunications, the specified telecommunications service provider who uses specified telecommunications facilities for said specified telecommunications hereinafter in this paragraph referred to as a "relevant service provider" shall not be liable for any loss incurred from such infringement, unless where it is technically possible to take measures for preventing such information from being transmitted to unspecified persons and such event of infringement falls under any of the following items. However, where said relevant service provider is the sender of said information infringing rights, this shall not apply. i) In cases where said relevant service provider knew that the infringement of the rights of others was caused by information distribution via said specified telecommunications. ii) In cases where said relevant service provider had knowledge of information distribution by said specified telecommunications, and where there is a reasonable ground to find that said relevant service provider could know the infringement of the rights of others was caused by the information distribution via said specified telecommunications."	Japan
It appears that media law governs the liability of intermediaries in Egypt. • Pursuant to Article 102 bis of the Criminal Code: "Detention and paying a fine of not less than fifty pounds and not exceeding two hundred pounds shall be inflicted on whoever deliberately diffuses news, information/data, or false or tendentious rumors, or propagates	Egypt

exciting publicity, if this is liable to disturb public security, cast horror among the people, or cause harm and damage to public interest. Imprisonment and paying a fine of not less than one hundred pounds and not exceeding five hundred pounds shall be the inflicted penalty if the crime occurs in time of war. The penalties prescribed in the first clause shall be inflicted on any one who obtains, personally or through an intermediary, or possesses written documents or printed matter comprising some of the provisions prescribed in the first clause, if they are prepared and provided for distribution or access by third parties. Also, whoever obtains or possesses any means and methods for printing, recording, or for public announcement, which are appropriated, even temporarily, for printing, recording, or diffusing part of the foregoing, shall be liable to the said penalties." • Article 195 of the Criminal Code: "Subject to the criminal liability, in relation to the author of the text or the designer of the drawing, or such other representation methods, the chief editor of the paper or the editor in charge of the section wherein the, publication took place, if there is not chief editor in his quality of original doer of the crimes that were committed by his paper. However, he shall be exempted from the criminal liability: 1. If he establishes that the publication took place without his knowledge, and from the beginning of the investigation he submits all the information and papers he has, in order to assist in knowing the person responsible for publication. 2. Or if during the investigation he directs about the perpetrator of the crime, and submits all information and papers he has in order to establish his responsibility, and proves in addition that if he had not published he would have exposed himself to losing his position in the newspaper, or to another serious damage. " • Article 196 of the Criminal Code: "In the cases where the inscription, drawing, pictures, photos, symbols, or other methods of representation that were used in committing the crime, have been published abroad, and in all cases where it is not possible to know and recognized the perpetrator of the crime, the printer importers shall be punished in their quality of original perpetrators. If this is impossible, the sellers, the distributors, and the placard gluers shall be punished as original perpetrators, unless it transpires from the conditions of the case that it was not possible for them to know the constituents of the writing, inscription, drawing, pictures, photos, symbols, or other methods of representation." • Article 197 of the Criminal Code: "No one, in order to evade the criminal responsibility from what is prescribed in the previous Articles, shall be accepted to give a justification or provide an excuse that the inscriptions, drawings, pictures, photos, symbols, or other methods of representation have been communicated or translated from publications issued in Egypt or abroad, or that they are no more than a repetition of rumors or stories flow third parties."	
The "Brazilian Internet Bill of Rights," Federal Law no. 12.965 of 23 April 2014 introduces a liability exemption for Internet connection providers and the application of the safe harbor doctrine for other Internet application providers. Article 18 addresses the liability of Internet connection providers, grants an exception to those services regarding intermediary liability. It states that "the Internet connection provider shall not be subject to civil liability for content generated by third party". Article 19, which addresses Internet application providers (excluding connection providers) states that, "in order to ensure freedom of expression and to prevent censorship, an Internet application provider shall only be subject to civil liability for damages caused by virtue of content generated by third parties if, after specific court order, it does not take action, according to the framework and technical limits of its services and within the time-frame ordered, to make the infringing content unavailable." For a literal interpretation of the law, neither the responsibility exemption to ISPs nor the safe harbor doctrine to ISPs would apply to criminal liability.	Brazil
• According to Article 12 of the Act of 18 July 2002 on Providing Services by Electronic Means: "1. The responsibility for the conveyed data shall not be borne by the one who, while transmitting data: 1) is not an initiator of the transmission, 2) does not select the recipient of data, and 3) does not delete or modify the data being subject to transmission. 2. The releasing from responsibility, referred to in paragraph 1, shall also cover automated and short-term indirect storing of the transmitted data, if this activity aims exclusively to proceeding with transmission, and	Poland

the data are not stored longer than it is necessary for accomplishment of transmission in the ordinary conditions." • According to Article 14: "1. The responsibility for the stored data shall not be borne by the person, who, making the resources of a teleinformation system available for the purpose of the data storage by a service recipient, is not aware of unlawful nature of the data or the activity related to them, and in case of having been informed or having received a message on unlawful nature of the data or the activity related to them, makes immediately the access to the data impossible. 2. The service provider, who has received the formal notice on unlawful character of the stored data provided by a service recipient and has made access to them impossible, shall not bear the responsibility to this service recipient for any damage resulting from impossibility to access these data. 3. The service provider, who has received the reliable message on unlawful character of the stored data provided by a service recipient, and has made access to these data impossible, shall not bear responsibility to this service recipient for a damage resulting from impossibility to access these data, if he/she has immediately notified the service recipient of intention to make the access to the data impossible." • According to Article 13: "1. The responsibility for the stored data shall not be borne by the one who transmitting data and providing for automated and short-term indirect storing of the data in order to make them quickly accessible on the request of another entity: 1) does not delete or modify the data, 2) uses recognised and usually applied in such activity information techniques determining technical parameters of data access and their updating, and 3) does not interfere with using of information techniques, recognised and usually applied in this kind of activity for gathering information about usage of the collected data. 2. The responsibility for the stored data shall not be borne by the person, who, respecting the conditions referred to in paragraph 1, immediately erases the data or makes the access to the stored data impossible as soon as he/she receives the message that the data have been erased from the initial source of transmission or the access to them has been made impossible, or a court or any other competent authority has ordered to erase the data or to make the access to them impossible."	
According to Section 124 of the Films, Videos, and Publications Classification Act of 1993 and amended in 2005: "(1) Every person commits an offence against this Act who does any act mentioned in section 123 (1), knowing or having reasonable cause to believe that the publication is objectionable. (2) Every person who commits an offence against subsection (1) is liable, — (a) in the case of an individual, to imprisonment for a term not exceeding 10 years: (b) in the case of a body corporate, to a fine not exceeding $200,000." Furthermore, offences under the Human Rights Act are treated under the same absolute liability clause, which may lead ISPs to be liable for something they are not to blame for. However, it must be noted that Section 21 of the Defamation Act 1992 provides for a legal exemption for ISPs in case of innocent dissemination: "In any proceedings for defamation against any person who has published the matter that is the subject of the proceedings solely in the capacity of, or as the employee or agent of, a processor or a distributor, it is a defence if that person alleges and proves— a) That that person did not know that the matter contained the material that is alleged to be defamatory; and b) That that person did not know that the matter was of a character likely to contain material of a defamatory nature; and c) That that person's lack of knowledge was not due to any negligence on that person's part."	New Zealand
• According to Article 286-1 of the criminal code (9th amendment, 2015): "In any of the following circumstances where network service providers do not perform information network security management duties as provided by law or administrative regulations, and upon being ordered by the	China

oversight and management department to adopt rectification measures but refusing to make corrections, the sentence is up to three years imprisonment, short-term detention or controlled release, and/or a fine: (1) Where it results in the transmission of a large volume of unlawful information; (2) Where it results in disclosure or user information causing serious consequences; (3) Where it results in the destruction of evidence in a criminal case and the circumstances are serious; (4) There are other serious circumstances. Where a unit commits crimes described in the preceding paragraph, the unit is fined, and the person in charge who is directly responsible and other directly responsible persons are punished under the provisions of the preceding paragraph." • Article 84 of the Counter-Terrorism Law (2015): "In any of the following circumstances, the competent departments shall fine telecommunications operators or internet service providers between 200,000 and 500,000 yuan, and fine directly responsible managers and other directly responsible personnel up to 100,000 yuan; where circumstances are serious, the fine is 500,000 or more, and directly responsible managers and other directly responsible personnel are fined between 100,000 and 500,000 yuan, and the public security organs may detain directly responsible managers and other directly responsible personnel for between 5 and 15 days: (1) Not providing technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law. (2) not following a competent department's request to stop transmission, delete information that has terrorist or extremist content, store relevant records, or to close down relevant websites, or shut down related services; (3) Not putting into place systems for network security and supervision of information content, technological security precautionary measures, causing the transmission of information with terrorist or extremist content; where the circumstances are serious." • Article 86 of the Counter-Terrorism Law (2015): "Where telecommunications, internet, and financial business operations or service providers do not follow provisions to conduct checks of customer identification or provide service to those whose identity is unclear or who refuse to allow inspection of their identification; the competent departments shall order corrections, and where corrections are refused, give a fine of between 200,000 and 500,000 yuan, and fine directly responsible managers and other directly responsible personnel up to 100,000 yuan; where circumstances are serious, the fine is 500,000 or more, and directly responsible managers and other directly responsible personnel are fined between 100,000 and 500,000 yuan. Where lodging, long-distance passenger transport, or motor vehicle rental business operators and service providers have any of the situations provided in the preceding paragraph, the competent departments shall give a fine of between 100,000 and 500,000 yuan, and fine directly responsible managers and other directly responsible personnel up to 100,000 yuan."	
General provisions in the Argentine Civil Code can be used with regards to intermediary liability. According to Article 1.109 of the Argentine Civil Code, "Any person performing an act, which through his fault or negligence causes damage to another, is obliged to repair the damage. This obligation is governed by the same provisions to which the offenses of the civil law are subject." According to Article 1.113, "The obligation of anyone who causes damage extends to any damage caused by those who are under his/her control or by the things used or under his/her control. In cases of damages caused by things, to avoid liability the owner or custodian must evidence that he has not acted with fault or negligence. However, If the damage is caused by a risky thing or by a defect in the thing, to avoid liability the owner or custodian must evidence the fault or negligence of the victim."	Argentina
No. • According to Article 380 of the Criminal Code: "(1) In this and the next succeeding section, the term "periodical" includes any newspaper, review, magazine, or other writing or print, published periodically.	Nigeria

(2) The criminal responsibility of the proprietor, editor, or publisher, of any periodical for the publication of any defamatory matter contained therein, may be rebutted by proof that such publication took place without his knowledge and without negligence on his part." Nigeria provides for a limited liability with regards to intermediaries. • Article 11 of the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission pursuant to Section 70(2) of the Nigerian Communications Act of 2003 provides for different scenarios: "(a) Acting as Mere Conduit ISPs shall not be liable for the content of any Internet service transmission by a user of the service or for providing access to such content by other users if the ISP: (i) has not initiated the transmission; (ii) has not selected the recipient(s) of the transmission; (iii) has not selected or modified the content contained in the transmission; and (iv) acts without delay to remove or disable access to the information on receipt of any takedown notice (see paragraph 12 following), or on becoming aware that the information at the initial source of the transmission has been removed or disabled. (b) Caching ISPs shall not be liable for the transmission in a communication system of automatic, intermediate and temporarily stored information provided by a user of the service if the ISP: (i) does not modify the information; (ii) does not interfere with any conditions of access applicable to the information; (iii) complies with any rules regarding the updating of the information; (iv) does not interfere with the lawful use of technology to obtain data on the use of the information; and (v) acts without delay to remove or disable access to the information on receipt of any takedown notice (see paragraph 12 following), or on becoming aware that the information at the initial source of the transmission has been removed or disabled. (c) Hosting ISPs shall not be liable for the storage of information at the request of any user of the service if the ISP: (i) does not modify the information; (ii) does not interfere with any conditions of access applicable to the information; (iii) does not interfere with the lawful use of technology to obtain data on the use of the information; (iv) does not have knowledge of illegal activity related to the information; and (v) acts without delay to remove or disable access to the information on receipt of any takedown notice."	
Article 39 of the Federal Decree-law no. (5) of 2012 on Combating Cybercrimes reads: "Shall be punished by imprisonment and a fine or any of these two penalties any owner or operator of a website or computer network who deliberately and knowingly saves or makes available any illicit content or if he fails to remove or blocks access to this illicit content within the period determined in the written notice addressed by the competent authorities indicating the illegal content and being available on the website or the computer network."	United Arab Emirates
Similarly, to all EU member states, France has a strict liability regime regarding ISPs acting as intermediaries. According to Article 6.I of Law No. 2004-575 for the Confidence in the Digital economy, ISPs can be held liable if, once they are aware of the illegal nature of the hosted content, do not remove it promptly. The exemption applies if they have a neutral and mere technical and passive role towards the hosted content.	France
In the question of accountability and complicity dealt by intermediaries, The Cybercrime Act contains provisions that show what the implications can be for intermediaries. • Article 39 - Monitoring obligation: "(1) When providing services in accordance with the provisions of this Part, a service provider shall not (a) Monitor the data which the service provider transmit or store; or (b) Actively seek facts or circumstances indicating an unlawful activity. (2) The Minister may prescribe procedures for service providers to- (a) Inform the competent authority of alleged illegal	Tanzania

Activities undertaken or information provided by Recipients of their service; and (b) Avail competent authorities, at their request, with information enabling the identification of recipients of their service. (3) A service provider shall not be liable for disclosure, by a third party, of data lawfully made available to the third party upon proving that- (a) The third party acted without the knowledge of the service provider; or (b) The service provider exercised due care and skill to prevent the disclosure of such data. (4) Where a service provider has knowledge of illegal information, or activity he shall - (a) Remove the information in the computer system within the service providers control; (b) Suspend or terminate services in respect of that information or activity; and (c) Notify appropriate law enforcement authority of the illegal activity or information, relevant facts and the identity of the person for whom the service provider is supplying services in respect of the information. • Article 40 - Access Provider: "(1) An access provider shall not be liable for providing access, transmitting or operating computer system in respect of third-party material in the form of electronic communication to which he merely provides access to or for operating facilities via a computer system under his control, provided that he- (a) Does not initiate the transmission; (b) Does not select the receiver of the transmission; or (c) Does not select or modify the information contained in the transmission. (2) The transmission and provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place- (a) For the purpose of carrying out the transmission in the information system; (b) In a manner that makes it inaccessible to a person other than the anticipated recipient; and (c) for a period no longer than is reasonably necessary for the transmission." • Article 41 - Hosting provider: "(1) A hosting provider is not liable for information stored at the request of a user of the service, on condition that the hosting provider - (a) Immediately removes or disables access to the information after receiving an order from any competent authority or court to remove specific illegal information stored; or (b) Upon becoming aware of illegal information stored in means than a competent authority, shall immediately inform the relevant authority. (2) The provision of subsection (1) shall not apply where the user of the service is acting under the authority or control of the hosting provider." • Article 42 - Caching Provider: "A caching provider shall not be liable for the storage of information provided that the caching provider: (a) Does not modify the information; (b) Complies with conditions of access to the Information; (c) Complies with rules regarding the updating of the information; (d) Does not interfere with the lawful use of the technology widely recognized and used in the industry, to obtain data on the use of the information; and (e) Acts immediately to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or the relevant authority has ordered such removal or disablement." • Article 43 - Hyperlink provider: "A hyperlink provider is not liable for the information linked provided that the hyperlink provider: (a) Immediately removes or disables access to the information after receiving an order to do so from the relevant authority; and (b) Upon becoming aware of the specific illegal information stored by other ways than an order from a public authority, immediately informs relevant authority. Search engine provider 44. - (1) A search engine provider is not liable for search results, on condition that the search engine provider- (a) Does not initiate the transmission; (b) Does not select the receiver of the transmission; and (c) Does not select or modify the information contained in the transmission.	

(2) For the purpose of this section, "a search engine provider" is a person who makes or operates a search engine whit creates an index of internet related content or makes available electronic tools to search for information provided by third party." Further, according to Article 104 of The Electronic and Postal Communications Act of 2010: "(1) The code of conduct contemplated in this section shall (a) be binding on all Content Service Licensees; (b) prohibit the provision of content which is indecent, obscene, false, menacing or otherwise offensive in character. (2) Without derogating from the generality of subsection 1(b), the code of conduct shall be designed to achieve the following objective […] (b) the exclusion of material likely to encourage or incite the commission of crime, from content provided by content service licensees; […] (d) the presentation of religious material in a balanced and responsible manner; (e) the protection of the public against offensive and harmful content; […]"	
The Federal Law No. 126-FZ of 7 July 2003 on Communications provides in its Chapter 11. Responsibility for Violating the Legislation of the Russian Federation in the Sphere of Communications, Article 68. Responsibility for Violating the Legislation of the Russian Federation in the Sphere of Communications for an administrative and civil liability.	Russia
(3) Can legal entities: companies, associations or a group of persons be held criminally liable under your country's laws and regulations on internet radicalization?	**STATES**
Legal persons in general may be held criminally liable according to section 306 of the Criminal Code. • Section 306: (1) Companies and other incorporated bodies (legal persons) may incur criminal liability under the rules of Part 5 for violation of this Code. • Section 25: (1) A fine may be imposed on a legal person where so provided by or pursuant to statute.	Denmark
The Terrorism Act 2006 grants the home secretary greater powers to ban groups that glorify terrorism and to prevent proscribed organisations from using front organisations to continue operating. Under the 2015 Act, local councils will be required to make checks on the use of its public buildings, its internet filters and any unregulated out of school settings, including after-school clubs and groups, supplementary schools and tuition centres to support home education. Prevent activity in local areas relies on the co-operation of many organisations to be effective. Currently, such co-operation is not consistent across Great Britain. In legislating, the Government's policy intention was to make delivery of such activity a legal requirement for specified authorities and improve the standard of work on the Prevent programme across Great Britain.	United Kingdom
Yes, Article 7 of the Law on the countering of Terrorism provides that "legal persons are prosecuted if their involvement in the commission of terrorist offences are established."	Tunisia
No.	Albania
	Hungary

Yes, regarding criminal offences that were mentioned under Question 1.b. and provided by the CC. On the basis of the Act CIV of 2001 on the criminal law measures applicable to legal persons, the criminal liability of legal persons is derivative. Criminal action can only be taken against legal persons if there is a natural person who can be prosecuted. However, due to an amendment, the legislator broadened the cases for applying measures against a legal entity even if the criminal liability of the natural person perpetrator cannot be established (e.g. the perpetrator could not be identified during the investigation, the prosecutor terminated the investigation because the crime was not committed by the suspect, the procedure was suspended because the perpetrator resides at an unknown place or the perpetrator is not punishable due to his mental illness or death or the perpetrator committed the act under coercion or threat etc.), but the commission of the crime is obvious. Moreover, the crime has to be committed for the benefit of the legal person, or the crime has to be committed with the use of the legal entity.	
Since the country's laws and regulations don't specifically talk about Internet radicalization, there is no legal provision where legal entities, companies, associations or group of persons can be held criminally liable. However, they can be booked for other offences under different laws for which they can held criminally liable such as the Indian Information Technology Act, 2000 and the Indian Penal Code, 1860.	India
The offences in the Criminal Code apply to natural persons and to corporations and bodies politic (see subsection 2C(1) of the *Acts Interpretation Act 1901*).	Australia
No, they cannot. Under German law, there is no criminal liability of legal entities and companies, associations or a group of persons for offences committed by management. However, in line with EU and international standards, they can be held liable under administrative law including for offences related to internet radicalization. Nevertheless, legal persons may be liable to a fine under the Act on Regulatory Offences (German term: "Ordnungswidrigkeitengesetz"). Pursuant to Section 30 of that Act the liability of legal persons is triggered where any "responsible person" (which includes a broad range of senior managerial staff and not only an authorized representative or manager), acting for the management of the entity commits i) a criminal offence; or ii) an regulatory offence including a violation of supervisory duties leading to the commission of a criminal or regulatory offence by staff. The maximum regulatory fine is 10 million Euros (not including confiscation of proceeds which come "on top").	Germany
In so far as an offence under the Penal Code is committed, legal entities are criminally liable.	Seychelles
According to Article 23 of the Penal Law, corporations can be held criminally liable for offences requiring a criminal intent if the perpetrator's intent, under the circumstances and in light of his capacity and authority, is attributable to the corporation.	Israel
Yes, according to section 3 of the Act no 91/2016 Coll. about Legal Liability of Legal Entities.	Slovakia
Legal entities may be criminally liable for crimes of radicalization on the internet that lead to incitement to hatred, spreading online material inciting hatred or denial, trivialization or glorification of genocide through Internet under Article 510 bis PC.	Spain
As explained above, Sweden has no criminal legislation on internet radicalization. For a crime committed in the exercise of business activities a legal person can be ordered to pay a corporate fine if it for the crime is prescribed a more severe punishment than a summary fine and the entrepreneur has not done what could reasonably be required of him for prevention of the crime, or the crime has been committed by a person who has a leading position based on a power of representation of the entrepreneur or an authority to take decisions on behalf of the entrepreneur, or a person who otherwise has had a special responsibility of supervision or control of the business.	Sweden

No.	Irak
Yes. Section 2 of the Criminal Code defines “every one”, “person” and “owner” and similar expressions to include Her Majesty and an organization. “Organization” is defined in section 2 of the Criminal Code to mean: (a) a public body, body corporate, society, company, firm, partnership, trade union or municipality, or (b) an association of persons that (i) is created for a common purpose, (ii) has an operational structure, and (iii) holds itself out to the public as an association of persons; As well, “person” is defined in subsection 35(1) of the Interpretation Act to include a corporation.	Canada
It is possible for companies, associations or bodies of persons to be held criminally liable under the Sedition Act and the Penal Code. Under the Broadcasting Act, it is possible for MDA to impose penal sanctions on legal entities such as companies, associations or bodies of persons, whether incorporated or not, if they do not comply with MDA’s directions to take down/restrict access to prohibited content that contravenes the ICOP, or if they were to continue broadcasting without licence after MDA had suspended or cancelled their licence.	Singapore
For all the above mentioned offences, a company and an association can be held criminally liable pursuant to the Norwegian Penal Code s. 27. A group of persons who is not a legal entity cannot be held criminally liable as such, but as individuals e.g. as members in a terrorist organization (s. 136 a).	Norway
In Belgium, criminal liability is mentioned in Article 5 of the Criminal Code. According to Article 5 of the Criminal Code, ““all legal persons are criminally liable for offences that are intrinsically connected with the attainment of their purpose or the defense of their interests, or for offences that concrete evidence shows to have been committed on their behalf.”	Belgium
Article 23 of the Penal Code provides that “Where an offence is committed by any company or other body corporate, or by any society, association or body of persons, every person charged with, or concerned or acting in, the control or management of the affairs or activities of such company, body corporate, society, association or body of persons shall be guilty of that offence and liable to be punished accordingly, unless it is proved by such person that, through no act or omission on his part, he was not aware that the offence was being or was intended or about to be committed, or that he took all reasonable steps to prevent its commission.”	Kenya
Under Japanese law, only natural persons are subject to criminal punishment. However, juridical persons may also be criminally punished if a dual punishment provision (“ryobatsu-kitei”) exists which provides that juridical persons will also be punished, together with the offender who actually committed the violation regarding the business of the juridical persons As administrative sanctions are not considered to be criminal punishment, their application is not limited to natural persons.	Japan
As a general rule, legal entities cannot be held criminally liable.	Egypt
Article 3 of Law 9.605/98 provides for legal entities’ criminal liability: “Legal entities will incur administrative, civil and criminal liability as provided for herein in the event of violation committed as a result of a decision by its legal or contractual representative, its management board, either in the interest, or for the benefit, of the entity.”	Brazil

Article 3 of the Act on the liability of collective entities for acts prohibited under penalty of 2001 provides that, "liability can be imposed on such entities where a specific person commits a specific offence and his/her conduct has or may have resulted in the corporates' entity benefit. Those offences must be committed by persons who: "(1) act in the name or the interest of the entity pursuant to authority or obligations to represent it, undertaking in its name decisions or performing of internal reviews or by exceeding such authority or not fulfilling such obligation (art. 3 point 1 of the Law); (2) permitted to act as a result of exceeding authority or non-fulfillment of obligations by persons described in point 1(art. 3 point 2 of the Law); (3) acting in the name or on behalf of the entity, with the consent or knowledge of persons described in point 1(art. 3 point 3 of the Law)." "Offences falling within the Act (listed in Article 16) Those are offences against, inter alia: (1) Economic turnover, (2) Trading in money and securities, (3) The protection of information, (4) The reliability of documents, (5) Property, (6) Environment, (7) Bribery, corruption, (8) Fiscal offences."	Poland
Under a general principle of law, legal entities can be held criminally liable if they commit a crime.	United States of America
Section 29 of the Interpretation Act 1999 and Section 2 of the Crimes Act 1961 define 'person' so as to include a corporation sole and also a body of persons, whether corporate or unincorporate.	New Zealand
Under Article 30 of the criminal code, "A company, enterprise, institution, organization, or group which commits an act endangering society that is considered a crime under the law shall bear criminal responsibility."	China
Under a general principle of law, legal entities can be held criminally liable if they commit a crime.	Argentina
Yes. According to Section 25 of the Terrorism Act of 2013: "(1) Where an offence under this Act committed by an entity is proved to have been committed on the instigation or with the connivance of, or is attributable to any neglect on the part of a director, manager, secretary of the entity or any person purported to act in any such capacity, the officer is liable on conviction to life imprisonment. (2) Where an entity is convicted of an offence under this Act, it is liable to the forfeiture of any assets, funds or property used or intended to be used in the commission of the offence and the court may issue an order to windup the entity or withdraw the practice licence of the entity and its principal officers or both. (3) Where the court orders the entity to be wound up, its assets and properties shall be transferred to the Federation Account. (4) Nothing contained in subsections (1) and (2) of this section shall render any person liable to punishment if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence."	Nigeria
Pursuant to Article 17 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred:	

"The representative, director or agent of a legal entity, in case any of the crimes set forth in the present Decree Law is committed, with his knowledge, by any employee of said entity acting in its name or to its interest, shall be sentenced to the same penalties prescribed for the committed crime. The legal entity shall be held jointly liable to settle any pecuniary penalties or compensation as ruled thereof."	United Arab Emirates
The French legal system establishes criminal liability for legal persons. Under article 121-2 of the Criminal Code, "legal persons, with the exception of the State, are criminally liable for the offences committed on their account by their organs or representatives."	France
Article 48 - Offences by corporations, societies, etc. (Newspaper Act 1976) reads: "Where any offence under this Act or any subsidiary legislation made hereunder is committed by a company or other body corporate, or by a society, association or body of persons then, as well as the company or other body corporate, or the society, association or body of persons, every person who, at the time of the commission of the offence, was concerned, as a director or an officer, with the management of the affairs or activities of such company or other body corporate, or society, association or body of persons, commits the offence and be liable to be proceeded against and punished accordingly, unless he proves to the satisfaction of the court that he had no knowledge, and could not by the exercise of reasonable diligence have had knowledge of the commission of the offence."	Tanzania
Russia has established administrative liability for legal persons, not criminal liability.	Russia
(4) 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?	**STATES**
It follows from section of the Danish Criminal Code, that offences are not punished if they have become barred by limitations under sections 93-94. • Section 93: (1) The limitation periods are - i. two years where the maximum penalty prescribed for the offence is imprisonment for one year; ii. five years where the maximum penalty prescribed is imprisonment for four years; iii. ten years where the maximum penalty prescribed is imprisonment for ten years; and iv. fifteen years where the maximum penalty prescribed is imprisonment for a determinate period. (2) The limitation period is in no case less than five years for - i. violation of sections 296(3), 297(2) and 302(2) of this Code; and ii. violation of the legislation on taxes, customs, duties or subsidies, where an unlawful gain is or can be made. (3) The limitation period for violation of section 223(1) or section 225, cf. section 223(1), of this Code is in no case less than ten years. (4) If a person has committed several offences by the same act and different limitation periods apply under subsections (1)-(3), the longest of those periods will apply to all offences. • Section 93 a): (1) Where an offence falls within an international convention to which Denmark has acceded, and the criminal liability is not subject to any limitation period according to such convention, the offence will never become barred by limitation. • Section 93 b): (1) Where an offence falls within section 157a of this Code, the offence will never become barred by limitation. • Section 94: (1) The limitation period is reckoned from the date when the criminal act or omission ceased. (2) Where criminality depends on or is influenced by a current consequence or other subsequent event, the limitation period is reckoned only from the date when the consequence or event occurred.	Denmark

(3) Where the offence was committed on board a Danish ship outside the territory of the Danish state, the limitation period is reckoned from the date when the ship called at a Danish port. The commencement of the limitation period cannot be postponed by more than one year under this provision. (4) For violation of section 210, sections 216-224, section 225, cf. sections 216-224, section 226, section 227(1), section 245a, section 246, cf. section 245a, section 260(2) or section 262a(2) committed against a person under 18 (i) years of age, or of section 232 committed against a child under 15 years of age, the limitation period is reckoned from the date when the victim attains the age of 21 years at the earliest. The same applies to violation of section 244, 245 or 246 by termination of a pregnancy, foetal reduction or sterilisation without consent committed against a person under 18 years of age. If the offender has coerced the victim to refrain from reporting the offence to the police by the use of violence, duress under section 260 or otherwise by a criminal act, the limitation period is reckoned from the date when such coercion ceased at the earliest. (5) The limitation period is suspended when the relevant person is notified of the provisional charge, or when the Prosecution Service requests legal proceedings by which the relevant person is provisionally charged with the offence. The limitation period of the liability of a legal person can be suspended by notification to a person authorised to accept service on behalf of the legal person under section 157a of the Administration of Justice Act (retsplejeloven). (6) Where prosecution is abandoned and such decision is not reversed by a superior prosecutor within the statutory period of reversal, the limitation period will continue to run as had no prosecution been pursued. This also applies where prosecution is suspended indefinitely. If prosecution is suspended because the person provisionally charged has evaded prosecution, the period of prosecution is not included in the calculation of the limitation period.	
Under the Terrorism Act law enforcement can order website operators or intermediaries to remove material they believe to be "unlawfully terrorism-related" and find those that fail to comply with the notice within two working days without a "reasonable excuse" liable for endorsing that material. “Very little can be done to take down websites that are extreme: because they are rarely hosted in the UK. The alternative to takedown is censorship, which is both ineffective and hands a propaganda victory to the targets of that censorship,” Killock said. "Furthermore, the committee should not be advocating "codes of conduct" but examining what the law says. If the UK really wants censorship, the minimum should be that it takes place through the courts." (...) The Government should help UK internet service providers (ISPs) draw up new rules requiring them to proactively remove radical extremist content posted online, a committee of MPs has said (07 Feb 2012). (...) The Home Affairs Committee said that the internet was one of the main “drivers of radicalisation” and that it was more likely that individuals become “radicalized” on the basis of what they read online than their experiences at university, prison or “religious institutions”.	United Kingdom
Basis rules on statute of limitations provided by the Criminal Code apply to radicalizing content.	Tunisia
No.	Albania
Yes, regarding the criminal offences listed under Question 1.b. above (which can be regarded as radicalisation), sections 26-28 of the CC provides the rules for statute of limitation. The basic rule is, that the statute of limitation equals to the maximum penalty for the criminal offence but at least five years. • Section 27 of the CC regulates the starting date of the statute of limitation: “Start of the period of limitation a) in case of a consummated offence, the day when the crime is actually committed; b) in case of attempt or preparation, the day when the act resulting in consequences is carried out; c) in case of an act that is considered a crime only if it relates to a breach of duty, the last day when the offender could discharge his or her duty without the consequences set out in this Act of Law; d) in the case of crimes which manifest in the maintenance of an unlawful state, the day when this state ceases to exist.	Hungary

There are also additional rules, the most important ones are perhaps that if certain crimes were committed against a minor, then the statute of limitation only starts when the victim reaches the age of 18 years, as well as there is no statute of limitation for crimes punishable by life imprisonment."	
Given that India does not have specific legal provisions on liability for radicalization of content, the question of application of special statute of limitation does not arise.	India
As noted above, there is no primary offence for radicalisation per se under the Criminal Code. For the related offences of urging violence or advocating terrorism, there is no statute of limitations for prosecution of an individual. Where a person aids, abets, counsels or procures the commission of offences, including genocide (see 'complicity and common purpose' referred to above), section 15B of the Crimes Act 1914 provides that prosecutions must commence any time within one year after the commission of the offence by the individual.	Australia
There is no specific statute of limitation for radicalizing content. Thus the general rules for limitation apply. The rules on limitation are laid down in Sections 78 et seq. of the Criminal Code. The limitation period for a specific offence depends on the maximum sentence which can be imposed for that offence.	Germany
Generally, there is no limitation on penal liability for felonies. Internet content/electronic documents, would be used as evidence.	Seychelles
There is no specific statute of limitation for radicalization content offences. However, Article 9 of the Criminal Procedure Law [Consolidated Version 5742 – 1982] provides that the statute of limitation applied to felonies (an offence which is punishable with a period of imprisonment exceeding three years) is 10 years. The statute of limitation for a misdemeanor (an offence which is punishable with a period of imprisonment between three months and three years) is 5 years. The time period begins on the date of the commission of the crime. When an investigation is being conducted, the time period will begin on the date of the last investigation action, or on the date on which an indictment was filed or on the date of the last court proceeding, whichever is the latest of these dates. With regard to crimes related to radicalization content, the offence of publication is a continuing crime. The offence begins when the content is first published and ends with its removal. Therefore, the statute of limitation will begin on the date of the removal of the content.	Israel
There is no specific legislation that would serve as the legal content for limitation on penal liability.	Slovakia
There is no specific statute of limitations for crimes related to the dissemination of content suitable for radicalization through the Internet. The period of limitation of the particular offence committed will be applied. In any case, under Article 132.1ºCP, the limitation period will start counting from the day the unlawful situation was removed or the illicit behavior ceased (in the case examined in the questionnaire since the radicalizing content is removed) and not the first day that such content was published.	Spain
Sweden does not have a specific statute of limitation on criminal liability regarding internet radicalization. The Swedish Penal Code includes general rules on limitations of sanctions. According to these rules no sanction may be imposed unless the suspect has been remanded in custody or received notice of prosecution for the crime within certain time limits. The specified times shall be reckoned from the date when the crime was committed.	Sweden
No.	Iraq
The Criminal Code, generally, does not have a statute of limitations for terrorism, hate propaganda or defamatory libel offences.	Canada

Singapore does not have a specific limitation period on penal liability for radicalising content on the Internet. However, under the Sedition Act, there is a limitation period of 6 months after an offence of sedition is committed for prosecutions to be brought.	Singapore
No.	Norway
No. General statute of limitations rules apply.	Belgium
It appears that Kenya does not have a specific statute of limitations for radicalizing content.	Kenya
It appears that Japan does not have a specific statute of limitations for radicalizing content. Article 32 of the Criminal Code provides for the Statute of Limitations for filing a criminal action for defamation which shall prescribe in ten (10) years. As expressly stated under Article 724 of the Civil Code, the right to demand compensation for damages in tort shall be extinguished by prescription if it is not exercised by the victim within three years from the time of the knowledge of the damage and the identity of the victim.	Japan
It appears that Egypt does not have a specific statute of limitations for radicalizing content.	Egypt
It appears that Brazil does not have a specific statute of limitations for radicalizing content.	Brazil
It appears that Poland does not have a specific statute of limitations for radicalizing content.	Poland
It appears that the United states of America does not have a specific statute of limitations for radicalizing content.	United States of America
It appears that New Zealand does not have a specific statute of limitations for radicalizing content.	New Zealand
It appears that China does not have a specific statute of limitations for radicalizing content.	China
It appears that Argentina does not have a specific statute of limitations for radicalizing content.	Argentina
No.	Nigeria
It appears that the United Arab Emirates does not have a specific statute of limitations for radicalizing content.	United Arab Emirates
It appears that France does not have a specific statute of limitations for radicalizing content.	France
It appears that Tanzania does not have a specific statute of limitations for radicalizing content.	Tanzania

It appears that Russia does not have a specific statute of limitations for radicalizing content. However, it should be noted that pursuant to Article 83 of the Criminal Code of the Russian Federation, the periods of limitation shall not apply to persons convicted for the commission of crimes against the peace and security of mankind provided for by the Criminal Code of the Russian Federation.	Russia
(5) 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, right of response, rerouting, denial of access and defensive hacking, refusal of access, suspension of ISP license, other.	**STATES**
Other: The police can, with a courts approval, impound a web site.	Denmark
Take down notices and filtering.	United Kingdom
Each of the measures is being enforced.	Tunisia
N/A.	Albania
Blocking and other: With regard to hate crimes committed on the internet, the amendment of the Criminal Code that entered into force on 1 July 2013 must be highlighted, since this introduced a new measure, namely rendering electronic data that realises a crime permanently inaccessible. The main purpose of rendering data inaccessible is to remove the illegal content (delete it from the storage server which can be done by the web hosting provider), if this is does not bring any successful result, then the court orders the temporary prevention of access to electronic data ("blocking" by the internet providers).	Hungary
Taking down notices, blocking, suspension of ISP license	India
Take down notices and filtering: Illegal and offensive online content is regulated through the Online Content Scheme under Schedule 5 and 7 of the Broadcasting Services Act 1992 through a complaints-based mechanism. The Scheme is designed to protect consumers, particularly children, from exposure to inappropriate or harmful material. Australian hosted extremist material can be removed if it is found to be: • advocating terrorist acts • offending the standards of morality, decency and propriety • promotion, incitement or instruction in matters of crime or violence. Where content is hosted in Australia and is found by the Children's eSafety Commissioner (the Commissioner) to be prohibited, the Commissioner has the authority to direct the relevant content service provider to remove the content from their service. Where content is not hosted in Australia and is prohibited, the Commissioner will notify the content to the suppliers of approved filters, so that access to the content using such filters is blocked. The Commissioner will also notify material found to advocate terrorist acts to the Australian Federal Police. Blocking: Section 313 of the Telecommunications Act 1997 enables Commonwealth, State and Territory government agencies to request Internet Service Providers (ISPs) to provide such help as is reasonably necessary to disrupt	Australia

the operation of illegal online services by blocking access to websites. This could allow agencies to block access to a website containing terrorist propaganda.	
Take down notices, blocking, right of response (where hate speech appears in a journalistic article the persons affected have a right to reply. If necessary, they can prosecute the operator before civil courts), Suspension of ISP license in extreme cases (Under the Trade Regulation Act, the competent authority can order an enterprise to terminate operations under certain conditions.)	Germany
Other: Interception of communication, confiscation of devices.	Seychelles
N/A.	Israel
Other: In Slovak national law there is possibility of dismiss the web site according to court order. In Act no 46/1993 Coll. about Slovak information service, section 16a there is stated: ,,Legal or natural person who is intermediary of a website, or who provides domain name is required according to a court order which is issued on the proposal of Slovak information service in accordance with paragraph 3 to prevent service of the web site or access to a domain name if the use of such web site or the domain name occurs supporting the dissemination of ideas that support or promote terrorism, political or religious extremism, extremism manifested in a violent manner or harmful sectarian groupings." Code of Criminal Procedure is used as a supporting legislation dealing with general aspects.	Slovakia
Take down notices, blocking, refusal of access, other: link deletion.	Spain
In media protected by the Fundamental Law on Freedom of Expression, inter alia part of the internet, the public administration as a whole is prohibited from intervening against abuses of the freedom of expression in other manners than prescribed in the fundamental law. The remedies listed are not mentioned in the Fundamental Law on Freedom of Expression. Judges or law enforcement agencies cannot act in preventively. In order to act there must be an ongoing criminal investigation regarding a particular crime. The coercive measures available to the law enforcement agencies are seizure and search warrant. Such measures, however, cannot be taken against a particular homepage, but is used primarily to seize hard drives, servers and other materials to get access to electronically stored information	Sweden
Take down notices, filtering and blocking.	Irak
Take Down Notices/Refusal of Access (on author, host or user). Under section 83.223 of the Criminal Code, a judge who is satisfied by information on oath that there are reasonable grounds to believe that there is material — that is terrorist propaganda or computer data that makes terrorist propaganda available — stored on and made available to the public through a computer system that is within the court's jurisdiction, may order the computer system's custodian to ensure that the material is no longer stored on and made available through the computer system. "Terrorist propaganda" is defined to mean material that counsels the commission of a terrorism offence or that advocates or promotes the commission of terrorism offences in general.	Canada
The following laws are relevant to take-down notices: • Under section 10 of the Sedition Act, the court may, on the application of the Public Prosecutor, make an order prohibiting the issuing and circulation of seditious publications.	Singapore

• The Maintenance of Religious Harmony Act gives the Minister for Home Affairs the power to make restraining orders against persons, including religious leaders, whose conduct causes "feelings of enmity, hatred, ill-will or hostility between different religious groups," or who carry out" subversive activities under the guise of propagating or practising any religious belief." • For convictions under section 298 (uttering words etc., with deliberate intent to wound the racial or religious feelings of any person) of the Penal Code, the court may issue take down orders against the offending material. This could also apply to section 298A of the Penal Code. In addition, please see answers to Q1 on the powers of the MDA under the Broadcasting Act. MDA requires ISPs to inform and offer optional Internet filtering services to their subscribers at the point of subscription or renewal of their residential fixed-line and mobile Internet access subscriptions. It should be noted that such filters are principally intended to protect the young from content containing sexually explicit material, violence and gore, and not specifically content pertaining to online radicalisation.	
Please see the answer to question 7.	Norway
Filtering, Take-down notices, blocking,	Belgium
Filtering: In Japan, filtering is conducted by ISPs on a voluntarily basis (and mostly for the protection of juveniles).	Japan
Blocking: The new Anti-Terrorism Law gives the Director of the Internal Security Agency authority to order the immediate blocking of specific websites with no prior judicial authorization. After a five-day period, a court must confirm that the ISA's order to block a website was justified.	Poland
Denial of service (attacks in 2008 by the Pentagon's Joint Functional Component Command Network Warfare in Fort Meade).	United States of America
Filtering and blocking are measures taken by the authorities but only with regards to digital child exploitation. ISPs voluntarily adopt the system.	New Zealand
Blocking of content on the basis of a judicial decision.	Argentina
Take down notices, Blocking, Refusal of access (on author, host and user) and Others. Take-down notices; Under Article 12 of the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission pursuant to Section 70(2) of the Nigerian Communications Act of 2003, "ISPs must have in place a procedure for receiving and promptly responding to content related complaints, including any notice to withdraw or disable access to identified content issued by the Commission or other legal authority ("takedown notices")".	Nigeria
Filtering, take down notices, blocking of content and other: Article 41 of the Federal Decree-law no. (5) of 2012 on Combating Cybercrimes reads: "Without prejudice to the right of bona fide third-party, shall be ordered, in all instances, the confiscation of devices, programs or means used in the commission of any of the crimes specified in this Decree-Law or the	United Arab Emirates

money accrued thereof, or deletion of the information and statements or their killing, as to the closure of the domain or site in which any of these crimes is committed whether permanent closure or for a specified period as determined by court."	
Blocking of content: The Decree No. 2015-125 of 5 February 2015 allows the French government to block websites accused of promoting terrorism and publishing child pornography, without seeking a court order. Internet service providers (ISPs) must take down offending websites within 24 hours of receiving a government order.	France
Blocking of content and other: The Russian telecommunications regulator Roskomnadzor has the authority to request content to be taken down, if it considers an online article or post to be extremist in nature, offensive to religious believers or to call into question the integrity of Russian territory. Blocking of content is also conducted. In 2013, Russia's blacklist law was amended to include extremist content. The federal list contains details of court decisions that identify any online information materials as extremist. As of February 2013, the list included 1,704 items, compared to 1,066 as of January 2012 (http://minjust.ru/ru/extremist-materials?search).	Russia
(6) Please provide statistics on take downs and similar remedies in your country.	**STATES**
N/A.	Denmark
The government's Counter Terrorism Internet Referral Unit (CTIRU), set up in 2010, has removed more than 49,000 pieces of content that "encourages or glorifies acts of terrorism", 30,000 of which were removed since December 2013. London police take down over 1,000 extremist web pages every week, London's police chief has said (300,000 pages have been removed in the past 18 months). ... Now most of that is to do with terrorist type posting but its not only that. Its also extremes on both sides. There are also right wing sites.	United Kingdom
N/A.	Tunisia
N/A.	Albania
No answer given by the State.	Hungary
N/A.	India
N/A.	Australia
The State media supervisory authorities examined ca. 30,250 internet offers in 2015. Of those, 935 were considered illegal on the grounds of incitement to hatred or using symbols of unconstitutional organisations (e.g. swastika).). The measures taken differed. As the vast majority of offers was hosted on servers outside Germany the most important step was to notify the operators of the services (e.g. Facebook) through their privileged communication channels. In 2014, jugendschutz.net achieved removal of 58% of all hate speech offences. 95% of the successful cases were obtained by notifying the provider.	Germany

N/A.	Seychelles
N/A.	Israel
N/A.	Slovakia
N/A.	Spain
N/A.	Sweden
N/A.	Irak
Since the coming into force of Bill C-51, the Government of Canada is not aware of section 83.223 of the Criminal Code being used formally.	Canada
Take-down notices have been used sparingly. The MDA has issued 27 take-down notices since 1996 but none was for content pertaining to online radicalisation. Most were for pornographic content or advertisements that solicited for sex. A small number of the notices were for religiously sensitive material.	Singapore
N/A.	Norway
After the creation of IRU at Europol in 2015, State members have been invited to create a national contact. Belgium has established the "Single Point Of Contact" in the beginning of 2016. Belgium has reported 3 websites to Europol. After the terrorist attack of 22 March, all the relevant services have enable the identification of numerous websites and accounts and the removal of the latter. The removals have essentially been undertaken directly by the service providers, which have applied strictly their Terms of Service.	Belgium
The Federal Communications Commission said in 2015 that it had no jurisdiction to shut down websites used by the Islamic State and other terrorist groups.	United States of America
The Telecommunications Regulatory Authority has issued st atistics regarding blocking of content. In 2016, amongst the content blocked, 2% was blocked because of it contained material which expresses hate to religions.	United Arab Emirates
According to the nonprofit project RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2015: 773 sites for extremism and calls for protests (by orders from the Prosecutor General's Office).	Russia
No statistics available. The Cybercrime (Prohibition and Prevention) Act 2015 is a new legislation and offences are yet to be prosecuted under it.	Nigeria

(7) Has your country put in place user platforms where radicalization content may be reported by the internet community?	**STATES**
No.	Denmark
ttps://www.gov.uk/report-terrorism (administered by The Counter Terrorism Internet Referral Unit). You can report material such as: articles, images, speeches or videos that promote terrorism or encourage violence content encouraging people to commit acts of terrorism, websites made by terrorist or extremist organisations, videos of terrorist attacks) http://content.met.police.uk/Site/terrorism You can also call the confidential Anti-Terrorist Hotline 0800 789 321.	United Kingdom
Yes, in civil society.	Tunisia
No.	Albania
[No answer given by the State].	Hungary
No.	India
The Australian Government's operates Report Online Extremism, an online tool that encourages the public to report violent extremist material and terrorist propaganda so that action can be taken to remove it if it breaches legal standards. If the content is assessed as being reasonably likely to break a companies' terms of use, the material may be referred to the appropriate company. The tool is available at https://www.reportextremism.livingsafetogether.gov.au/.	Australia
Yes. Users may report radicalized content, e.g. to • jugendschutz.net, a public body tasked with systematic examination of internet offers with respect to youth protection (which includes protection against incitement to hatred and using of symbols such as the swastika) • Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) (Association for Voluntary Self-Regulation of Digital Media service providers), a state-approved self-regulatory body of the electronic media industry which advises its members on youth protection issues and assesses complaints about alleged violations of youth protection regulations • Internet Complaint Office (internet-beschwerdestelle.de), provided by eco, the largest Internet association in Europe, and FSM.	Germany
No.	Seychelles
The Israeli Ministry of Justice provides a "hot-line" to the public, allowing internet users to submit complaints on inciting, racist and discriminating content on the internet.	Israel
Private based initiative: www.Stopline.sk serves as platform where users can report illegal content of web sites.	Slovakia

Spain launched in December 2015 a project known as "STOPS RADICALIMOS" (STOP RADICALIMS) which provides citizens with different tools: - The website www.stop_radicalismos.es, and the email address stopradicalismos@interior.es. Citizens can communicate any information they deem interesting or useful in an anonymous way. - The free hotline 900 822 066, which can receive both national and international calls operative 24/7. - A gateway in the mobile application called “ALERTCOPS”, where by pressing the specific button “STOP RADICALISMOS”, citizens can connect with the members of CITCO.	Spain
No.	Sweden
There isn't a specific platform but any agency and NGO can interact with CMC based on guidelines published from CMC	Irak
Canada has not specifically implemented a "user platform" for reporting internet-based radicalization, however there are ways that the public may report such content. The public may contact the Internet Service Provider (ISP) or the national ISP association to report online material containing radical or extremist messages, particularly ones advocating or promoting violence. Many ISPs have acceptable use policies that place restrictions around certain types of content, and the Canadian Association of Internet Provider’s Code of Conduct states that members will not host illegal content. Violent extremist material can also be reported to local law enforcement agencies. Many local police forces have computer crime units that are able to quickly take effective steps to get such material removed from the internet. The Royal Canadian Mounted Police will investigate security and terrorism offences. The public can report suspicious activity that may portend terrorist actions or violent extremism, including radicalizing online material, by calling the National Security Information Line at 1-800-420-5805 or e-mailing nsin_risn@rcmp-grc.gc.ca. Concerned members of the public may also contact their local police force. The province of Quebec has introduced a Centre for Preventing Radicalization. Assistance can be obtained through their website at: https://info-radical.org; to submit a form individuals can visit the website: https://info-radical.org/fr/demande-dassistance/ Some provinces and local communities also have resources for citizens who wish to report (by telephone or online) criminal activity. For example, in Quebec, Crime Stoppers and the Central criminal information of the Sûreté du Québec are also available to Internet users wanting to denounce radical content. It should be noted however that these platforms are not specifically dedicated to radicalization.	Canada
Members of the public may write in to MDA or other government agencies to report online radicalisation content.	Singapore
The National Criminal Investigation Service (NCIS) has established an online platform for tip-offs related to radicalization and violent extremism. Through this, one can choose to identify him/herself or be anonymous when giving information to the police. This is somewhat of a unique model which works well in Norway due to the high level of trust the Norwegian police has in the Norwegian population. Thus, the Norwegian approach when it comes to its online measures, is not countering per se, but based on help from the public and a preventive approach. As part of the Norwegian online model, the NCIS' Facebook page is also an important tool when it comes to noticing persons that might be in a radicalization process. Through the page, the Norwegian population can give the police information in an easy way (3,3 million of Norway's 5 million population is on Facebook). It is also a platform which allows for one-to-one communication as well as one-to-many communication. This allows the	Norway

NCIS to not only communicate privately with people who want to get in touch with the police, but also to give guidance to followers - whether that is regarding radicalization and violent extremism or other important topics related to the Internet.	
It does not seem that such a platform exists. However, there is a general platform that enables reports of all sorts of criminal behavior. Belgium incites people to report radicalization in its Social Action Public Centers or to its Youth Help Unit.	Belgium
The Department of Internal Affairs has put in place a complaint form on its website for objectionable content in general: https://www.dia.govt.nz/Censorship-Make-a-Complaint	New Zealand
France has put in place a website on which any individual can report extremist content or behavior https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action	France
Citizens can file complaints regarding illegal content on the state UNIFIED REGISTER of the domain names, website references and network addresses that allow identifying websites containing information circulation of which is forbidden in the Russian Federation. http://eais.rkn.gov.ru/en/	Russia
Yes.	Nigeria
(8) 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.**	**STATES**
No.	Denmark
In practice ISPs are not monitoring information but are waiting until they receive a take down notice. This has led a Home Office Committee to recommend that a code of conduct be produced requiring ISPs to proactively remove radical extreme content posted online, which would necessitate that material is monitored. The Investigatory Powers Bill answers this issue partly (next stage is the Committee stage: House of Lords | 05.09.2016). A Bill to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes. There is also the Preventing Extremism in London Programme which was released in Dec 2015, and commented that "at the moment, some public services have questions about the Government's Prevent Strategy—designed to deter individuals from engaging in extremism—and some communities continue to view the Strategy with suspicion." https://www.london.gov.uk/sites/default/files/preventing_extremism_in_london_report.pdf	United Kingdom
	Tunisia

Yes: The Decree No. 412-20145 of 16 January 2014 establishing the requirements and procedures relating to the granting of authorization to exercise the activity of virtual telecommunications operator. - The powers of the « Instance nationale de télécommunication », national telecommunications agency, an agency specialized and created by the Law of 2011 inserted in the Code of Communications. - ATI (l'agence tunisienne de l'internet), the Tunisien Internet Agency - The national agency for cyber security	
No.	Albania
[No answer given by the State].	Hungary
No.	India
Illegal and offensive online content is regulated through the Online Content Scheme under Schedule 5 and 7 of the Broadcasting Services Act 1992 through a complaints-based mechanism. The Scheme is designed to protect consumers, particularly children, from exposure to inappropriate or harmful material. Australian hosted extremist material can be removed if it is found to be: • advocating terrorist acts • offending the standards of morality, decency and propriety • promotion, incitement or instruction in matters of crime or violence. Where content is hosted in Australia and is found by the Children's eSafety Commissioner (the Commissioner) to be prohibited, the Commissioner has the authority to direct the relevant content service provider to remove the content from their service. Section 313 of the Telecommunications Act 1997 enables Commonwealth, State and Territory government agencies to request Internet Service Providers (ISPs) to provide such help as is reasonably necessary to disrupt the operation of illegal online services by blocking access to websites. This could allow agencies to block access to a website containing terrorist propaganda.	Australia
Yes. The Minister of Justice and Consumer Protection established a task force in 2015 composed of representatives from government, civil society and the IT companies Google (acting for Youtube), Facebook and Twitter. In December 2015, the task force agreed on a document entitled "Together against hate speech". In that document the IT companies committed themselves inter alia • to providing user friendly mechanisms for submission of removal requests, • to enforcing their terms and conditions by reviewing specific reports of hateful content and incitement to violence against their community guidelines and German law, in particular section 130 of the German Criminal Code (incitement to hatred), once notified, • to reviewing requests for removal of content in a timely manner, with dedicated teams; the majority of notified content has to be reviewed in less than 24 hours and removed or blocked for users in Germany, if necessary.	Germany
No legal obligations or guidelines in place. However, information held with service providers can be obtained through court warrants.	Seychelles
No.	Israel

No.	Slovakia
In cases of terrorism or exaltation of terrorism and other serious crimes - which also includes those crimes committed on social media, such as Facebook or Twitter, as it has been the case until now -, the new Penal Code has provided judges with the necessary tools to order the withdrawal of certain contents when the crime has been committed on-line or through other communication channels. In addition, they now have the possibility of ordering service providers to withdraw any illegal material, search engines to eliminate any links leading to them, and communication companies to block access to those contents. Therefore, the role of social media platforms, service providers and search engines in the legislative sphere, when it comes to open litigated investigations, is clear. However, for investigations out of the scope of judicial warrants, the collaboration and support provided by those platforms, ensuring the most scrupulous respect for current legislation and fundamental rights, is very satisfactory. LEAs maintain excellent relations with companies such as Google, Facebook or Twitter, whose implication and collaboration in the fight against on-line radicalization is very satisfying.	Spain
No.	Sweden
Still cybercrime law and ISP license is under review but there are security related articles for ISP and major communication companies' contracts for using Infrastructure.	Irak
No, Canada does not currently have legal obligations or "soft law" obligations in this area.	Canada
Under the Broadcasting Act, licensees are required to exercise judgement and use their "best efforts" to ensure that their services do not contain "prohibited material" as set out in the ICOP: "Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws."	Singapore
In the field of collecting information / evidence from ISP's with no infrastructure within Norwegian boundaries, Norwegian police has no jurisdiction. Nevertheless, we do get such information on the basis of cooperation with the ISPs and on the basis of Letters rogatory. It's worth mentioning that there is an ongoing process in the Council of Europe and its Cloud Evidence Group where the goal is to make it easier for the Police to collect such evidence. Further information on this is to be found in the recent published report: "Criminal justice access to electronic evidence in the cloud": Recommendations for consideration by the T-CY: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e	Norway
Yes. Belgium has signed the Budapest Convention on 23 November 2001. The ratification has been made in 2012 and the text has been published on 1 December 2012. Belgium has also signed the preventive approach Protocol binding it to Europol's IRU. The objectives are the screening and removal of online terrorist, extremist or violent propaganda. The Belgian Law from 1 March 2003 incorporates the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. However, it has a specificity: the ISP must inform the Attorney-General ("*procureur du Roi*").	Belgium
Individuals or police instruct ISPs to administratively delete contested or illegal content.	Japan

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern takedown requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement.	
Pursuant to Article 64 of the Egypt Telecommunication Regulation Law of 2003 in "consideration to inviolability of citizens' private life as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law. The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State."	Egypt
In Brazil, judges regularly block access to the "Whatsapp" application when its staff refuses to deliver private data on users involved in drug-related investigations. However, the Supreme Court nullifies these blockings.	Brazil
In the White House's fact sheet on working to counter online radicalization to Violence in the United States, the Government expresses its wishes to collaborate with the industry: "The Federal Government will collaborate with industry to explore how we might counter online violent extremism while protecting lawful Internet use and the civil liberties and privacy of individual users. Many companies have developed voluntary measures to promote Internet safety (such as fraud warnings, identity protection, and Internet safety tips), and we look forward to hearing their views about how we might apply similar measures to counter online radicalization to violence." https://www.whitehouse.gov/sites/default/files/docs/fact_sheet-countering_online_radicalization_-_final1.pdf	United States of America
According to Article 18 of the Counter-Terrorism Law of 2015, "Telecommunications operators and internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law." Further, Article 19 of the same law provides that "Telecommunications operators and internet service providers shall, according to provisions of law and administrative regulations, put into practice network security systems and information content monitoring systems, technical prevention and safety measures, to avoid the dissemination of information with terrorist or extremist content. Where information with terrorist or extremist content is discovered, its dissemination shall immediately be halted, relevant records shall be saved, and the relevant information deleted, and a report made to public security organs or to relevant departments. Network communications, telecommunications, public security, state security and other such departments discovering information with terrorist or extremist content shall promptly order to the relevant units to stop their transmission and delete relevant information, or close relevant websites, and terminate relevant services. Relevant units shall immediately enforce [such orders] save relevant records, and assist in conducting investigations. Departments for network communications shall adopt technical measures to interrupt transmission of information with terrorist or extremist content that crosses borders online."	China
Yes. 1) Administration of Criminal Justice Act 2015. 2) Cybercrime (Prohibition and Prevention) Act 2015. 3) Terrorism (Prevention) (Amendment) Act 2013. 4) Nigeria Communications Commission (NCC) Code of Corporate Governance. Pursuant to Section 29 of the Terrorism Act of 2013, the relevant law enforcement agency with the approval of the Attorney General of the Federation and the approval of the Coordinator on National Security can apply ex-	Nigeria

parte to a judge for an interception of communication order. The judge may make the order to (a) require a communication service provider to intercept and retain a specified communication or communications of a specified description received or transmitted or about to be received or transmitted by that communications service provider; (b) authorize the relevant law enforcement agency to enter any premises and to install in such premises, any device for the interception and retention of a communication or communications of specified description and to remove and retain such a device for the purpose of intelligence gathering; and (c) authorize the relevant law enforcement agency to execute covert operations in relation to an identified or suspected terrorist group or persons for the purpose of gathering intelligence. Further, according to 5 of the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission pursuant to Section 70(2) of the Nigerian Communications Act of 2003 "ISPs must ensure that users are informed of any statements of cybercrime prevention or acceptable Internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution, including with respect to: (a) unlawful access or fraudulent use of a computer; (b) identity theft, impersonation or unauthorized disclosure of access codes; (c) unlawful interception, or any form of system interference; (d) violation of intellectual property rights; (e) any other use for unlawful purposes, including terrorism, promoting racial, religious or other hatred or any unlawful sexual purposes." In accordance with Article 6, "(a) ISPs must generally cooperate with all law enforcement and regulatory agencies investigating cybercrime or other illegal activity. (b) ISPs must provide contact details for the ISP representative(s) responsible for addressing cybercrime issues. The contact information must include one or more means of contacting the identified individual(s) outside of normal business hours. (c) ISPs must provide any service related information requested by the Commission or other legal authority, including information regarding particular users and the content of their communications, subject to any other applicable laws of Nigeria. (d) ISPs must contact the Commission, and any other legal or regulatory authority identified by the Commission from time to time, in the event they become aware of any complaint or activity indicating Internet use for the commission of an offence." Under Article 12, "ISPs must have in place a procedure for receiving and promptly responding to content related complaints, including any notice to withdraw or disable access to identified content issued by the Commission or other legal authority ("takedown notices")".	
The Telecommunications Regulatory Authority is responsible for producing the Internet Access Management (IAM) policy, which outlines prohibited online content categories for ISPs. These categories include: Internet tools for bypassing blocked content; content for learning criminal skills and illegal drugs; content containing pornography and nudity; gambling sites; sites for hacking and malicious codes; content offensive to religions, phishing Internet sites; Internet content that downloads spyware; Web sites providing unlicensed voice over Internet protocol (VoIP) service; terrorism content; and prohibited top level domain, apparently a reference to the top level domain of Israel (.il), which is blocked in the UAE. https://opennet.net/research/profiles/united-arab-emirates	United Arab Emirates
Law no. 2014-1353 of 13 November 2014 inserted in Article 421-2-5 of the Criminal Code the offence of "incitement to commit acts of terrorism and their glorification" as well as to the list of contents being particularly serious for which hosting providers are required to set up easily accessible and visible measures enabling anyone to report such content. Hosting providers must also promptly inform public authorities of any unlawful activities that are reported to them. The administrative authority can now request that editors or hosting providers withdraw unlawful content as described above. In the absence of withdrawal within 24 hours, the administrative authority may request Internet service providers to prevent access to the concerned websites. It may also request search engines and electronic directories to dereference these websites. Furthermore, under some conditions, it is provided that the administrative authority may directly request that the concerned websites be blocked, without having requested the withdrawal of the unlawful contents beforehand to editors or hosting providers. In this case, blocking the	France

website would thus no longer be only a subsidiary measure, used when editors or hosting providers do not withdraw the unlawful content promptly enough, but a main measure.	
According to Article 30 of the Prevention of Terrorism Act 2002, "(1) The Minister may, for the purposes of the prevention or gathering detection of offences of terrorism or for the purposes of prosecution of offenders under this Act, give such directions as may appear to him to be necessary to; (a) communication service providers generally; (b) communication service providers of a specified description; (c) any particular communication service provider. (2) Before giving a direction under this section, the Minister may consult any communication service provider he deems fit to consult, (3) A direction under this section shall specify the maximum period for which a communication service provider may be required to retain Communications data. (4) In this section "communication service provider" means a person who provides postal, information, or communication, including telecommunications and internet service providers; "data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose. (5) In the event of resistance, the court may, on application by the Attorney General, issue an order directing the communication service provider to comply with the direction of the Minister." Further, pursuant to Article 31 of the Prevention of Terrorism Act 2002: "(1) Subject to subsection (2), a police officer may, for the purpose of obtaining evidence of the commission of an offence under this Act, apply, exparte, to the Court, for an interception of communications order. (2) A police officer may make an application under subsection (1) only with the prior written consent of the Attorney General. (3) A Court to whom an application is made under subsection (1), may make an order (a) requiring a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communication service provider; (b) authorizing the police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communications of a specified description and to remove and retain such device, if the Court is satisfied that the written consent of the Attorney General has been obtained as required by subsection (2) and that there are reasonable grounds to believe that material information relating to (i) the commission of an offence under this Act, or (ii) the whereabouts of the person suspected by the police officer to have committed the offence, is contained in that communication or communications of that description. (4) Any information contained in a communication (a) intercepted and retained pursuant to an order under subsection (3) ; (b) intercepted and retained in a foreign state in accordance with the law of that foreign state and certified by a Court of that foreign state to have been so intercepted and retained, shall be admissible in proceedings for an offence under this Act, as evidence of the truth of its contents notwithstanding the fact that it contains hearsay."	Tanzania
According to recent changes to the Civil Code of Russia and the Law on Information, operators and ISPs are obliged to block "black listed" domains, as well as websites containing unauthorised IP content and/or personal data. • Article 51.1. The Special Features of the Rendering of Communication Services to Meet the Needs of the Defence of the Country, the Security of the State and the Protection of Law and Order: "1. The federal executive body in the sphere of communication, by agreement with the federal executive bodies in charge of the networks of special designation, intended for the needs of the defence of the country, the security of the State and the protection of law and order, shall have the right to make additional requirements for communication network, which are a part of the network of communication for public use and are used for rendering communication services to meet the needs of the defence of the country, the security of the State and the protection of law and order. If the Government of the Russian Federation vests the communication operator with the duty of rendering such communication services in accordance with the legislation of the Russian Federation for placing orders in the deliveries of goods, the performance of works and the rendering services to	Russia

meet state and municipal needs, the said requirements shall be fulfilled during the time fixed by the respective government contract to render communication services for the needs of the defence of the country, the security of the State and the protection of law and order." • Article 64. Duties of Communications Operators and Restriction of the Rights of the Users of Communications Services in Carrying Out Operational-Search Measures, Measures for Ensuring the Security of the Russian Federation and in Performing Investigatory Actions: "1. Communications operators are obliged to supply to the authorized state bodies performing operational-search activity or ensuring the security of the Russian Federation, information on the users of communications services and the communications services rendered to them, as well as other information necessary for carrying out the tasks imposed upon these bodies, in the cases established in federal laws. 2. Communications operators are obliged to provide for the satisfaction of the requirements applicable to communication networks and facilities established by the federal executive power body in the sphere of communications in agreement with the authorized state bodies engaged in operational search activity or ensuring the security of the Russian Federation, for the purpose of these bodies' implementing in the cases established by federal laws measures in order to fulfil the tasks vested therein, and to take measures aimed at precluding the revelation of the organizational and tactical methods applied in carrying out these measures. 3. Rendering communications services to legal and natural persons is suspended by communications operators on the grounds of a motivated written decision of one of the managers of the body performing operative investigation activity or ensuring the security of the Russian Federation in the cases established by federal laws. Communications operators are obliged to resume rendering communications services on the grounds of a court decision or of the motivated written decision of one of the managers of the body engaged in operational-search activity or ensuring the security of the Russian Federation who has adopted the decision on the suspension of rendering communications services. 4. The procedure for the communications operators' interaction with the authorized state bodies carrying out operational-search activity or ensuring the security of the Russian Federation shall be established by the Government of the Russian Federation. 5. When the authorized state bodies are carrying out investigatory actions, communications operators are obliged to render assistance to these bodies in conformity with the demands of the criminal procedural legislation."	
(9) 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?	**STATES**
No. However, The Ministry of Justice can inform you that legislative initiatives countering internet radicalization will be launched in autumn 2016.	Denmark
CONTEST, The Prevent Strategy (2011) ... https://www.gov.uk/government/publications/2010-to-2015-government-policy-counter-terrorism/2010-to-2015-government-policy-counter-terrorism	United Kingdom
Yes. Law 26/2015 on the countering of terrorism and repression of money laundering as well as the national strategy's mechanisms in the tackling of extremism and terrorism established on 12 February 2015.	Tunisia
On 18th of November 2015, Albania adopted the National Strategy on CVE 2016-2020, which states that: « It will reduce the influence of propaganda and violent extremism online recruitment, utilizing social media to design and convey alternative positive messages ». It further stresses that: « The Government of Albania intends to oppose the message of violent extremism, particularly through its conductive materials and Internet messaging campaigns. Regarding this key area, the National Strategy represents a two-track approach discrediting and weakening the influence of extremist propaganda ». An interagency work is under way, to draft the National Strategy on Countering Terrorism for 2016-2020, where the recruitment and radicalization through internet platforms is not mentioned.	Albania

[No answer given by the State].	Hungary
No.	India
In February 2015, the Australian Government launched a new $21.7 million program to challenge terrorist propaganda in Australia, especially online. The program is focused on working with communities, civil society, academia and international counterparts across three areas of effort: 1. Building greater understanding of terrorist propaganda and an evidence base on how to counter its effect 2. Limiting access to extremist propaganda online through content removal and digital advertising 3. Undermining the appeal of extremist messages through leadership messaging and community-led counter-narrative activity	Australia
The government has recently adopted a comprehensive strategy on preventing extremism and promoting democracy (Strategie der Bundesregierung zur Extremismusprävention und Demokratieförderung). Media and the internet is one of the key areas of action. In that regard, the government aims to strengthen media literacy of children and young people and to better protect them against harmful content. Furthermore, it aims to raise awareness with all internet users for the strategies used by extremists for distributing propaganda. Lastly the government supports counter-narratives on the internet and in social media in particular. Examples of projects: • "No Hate Speech Movement", a project supported by the Council of Europe, which is a campaign for human rights online and the promotion of counter speech • The project "Research – Report – Remove: Countering Cyber Hate Phenomena" (2016-2017), funded by the European Commission Directorate-General for Justice and Consumers, developed by the International Network Against Cyber Hate (INACH), aims at providing a solid basis to draw sound conclusions on the concept of cyber hate. Besides project partners from Austria, Belgium, France, the Netherlands and Spain, jugendschutz.net from Germany is participating. • Web-site "Police for You" (German: "Polizei für dich") targeted at children and young people which provides information and raises awareness on extremism of all kinds (www.polizeifürdich.de) • Through the www.jugendschutz.net centre systematic research of extremist web-sites, developing of counter-strategies and providing information to the public • Social media competition to promote counter-narratives to islamist internet propaganda • Monitoring of the implementation of the commitments agreed upon by the IT companies in the task force mentioned above.	Germany
No.	Seychelles
In order to counter internet radicalization, the prosecutorial authorities in Israel have significantly enhanced enforcement with respect to related offences, such as incitement to violence or to racism. This policy reflects in the increasing numbers of indictments filed with respect to these offences and in the severity of the punishments imposed, including imprisonment sentences.	Israel
Slovak republic did not adopt any own strategy, but support policy created at European Union. Concretely there is Radicalization Awareness Network (RAN) which aim is fighting terrorism and violent extremism. For further information about RAN check the web site: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm	Slovakia
The National Strategic Plan against Violent Radicalization has a cyber space sphere where LEAs will be aware of everything circulating in the net that affects the aforementioned phenomenon, including both authors and contents. Functional areas are differentiated according to the situation at the national level. Thus, in the	Spain

Prevention area, the State will suggest initiatives against radicalization; in the Surveillance area, executive measures will be adopted in order to shut down websites with malicious content. In the field of action, authors might be arrested. With regards to the field of counter-narrative, as it has been the case with other initiatives, within the framework of the Spanish plan, a working group of experts has been formed in order to design and elaborate of a national counter-narrative that can challenge the radical messages coming from Jihadi terrorist organizations and networks. At present day, this group is elaborating the basic guidelines of action on this subject.	
The Government has a national strategy against terrorism (Prevent, preempt and protect – the Swedish counter-terrorism strategy) that will form the basis of Sweden's long-term work in this area, both nationally and internationally. The aim is to create a clear structure for the work needed to combat terrorist crime. The strategy emphasises the importance of cooperation and a clear follow-up of the work carried out. The goal of all counter-terrorism activities is to keep terrorist attacks from being carried out. This work is divided into three areas: Prevent, Preempt and Protect. Particular focus is given to the area Prevent. Measures in this area are intended to counteract radicalisation and recruitment to extremist and terrorist groups, and to influence the intent of individuals to commit or support terrorist crime. In this way, the recruitment base for terrorism can be reduced. The area Preempt deals with counteracting and reducing the capabilities and opportunities to commit terrorist attacks, while Protect deals with creating and maintaining protection for individuals and reducing society's vulnerability to terrorist attacks. If a terrorist attack is nevertheless carried out, society must also be able to manage the resulting consequences. One important premise for the Government is that fundamental rights and freedoms and the principles of the rule of law must be ensured in all actions to combat terrorism. Terrorism is an extreme form of violent extremism. To counter terrorism it is essential to work with the factors underlying extremism and terrorism, to prevent and counter its push factors and to identify individuals in the risk zone. Crime prevention work strives to systematically counter the causes of crime, based on factual knowledge, and to limit opportunities to commit crime. The preventive area of the strategy seeks to counter radicalisation and influence people's intention to commit crime. The focus is thus on measures that seek to reduce the recruitment base for terrorism. One issue on which attention should particularly be focused is the use of the internet and social media by extremist and terrorist groups to spread propaganda and other material that glorifies and encourages violence, violent ideologies and terrorism. This leads to groups growing stronger and more people being radicalised and recruited. The Swedish Media Council was previously commissioned by the Government to produce digital training material with the aim of increasing media awareness among children and young people, thereby increasing their ability to question anti-democratic and violent messages on the internet and in social media that encourage threats and violence for an ideological cause. The Swedish Media Council has recently been commissioned to expand and extend the No Hate Speech Movement to also include initiatives to safeguard democracy against violent extremism by increasing media awareness among children and young people. The campaign shall particularly be focused on strengthening the ability of children and young people to use their freedom of expression and respect human rights, increase their participation in democracy and stimulate source criticism and individual critical thought in relation to the media. However, there is a need for further knowledge to understand, analyze and tackle the violent propaganda on the internet and in social media, and the role which social media plays in radicalization and recruitment to violent extremism and terrorism. Therefore, the Swedish Defence University have surveyed violent extremism in social media. The survey also included a description on how other countries in Europe use social media in their preventive work.	Sweden
NSC endorsed Policy for ICT Security and established Higher Committee of ICT security to overlook the issue and there is a small committee to follow the internet content.	Irak
The Government of Canada has not adopted a strategy/policy specific to internet radicalization, however in December 2015, the Government of Canada published the "Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy" to protect Canada and the safety and security of Canadians at home and abroad. The Strategy operates through four mutually reinforcing elements: Prevent, Detect, Deny and Respond. All Government activity is directed towards one or more of these elements. The Strategy is available online at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/rslnc-gnst-trrrsm-eng.pdf The Anti-Terrorism Act, 2015 received Royal Assent on June 18, 2015. The Anti-Terrorism Act, 2015 was introduced, in part, to encourage and facilitate information sharing between Government of Canada institutions	Canada

in order to protect Canada against activities that undermine the security of Canada. Through the Anti-Terrorism Act, 2015 as discussed in response to question 5, section 83.223 of the Criminal Code provides for terrorist propaganda to be deleted from a computer system pursuant to a judicial order. The Government of Canada has committed to launching an Office for community outreach and countering radicalization to violence (the Office). The Office will contribute to a safe and resilient Canada by providing leadership on Canada's response to radicalization to violence, coordinating talent and expertise, mobilizing and supporting community outreach and enhancing research in the area. As a centre of excellence, the Office will undertake broad consultations to help inform national priorities, including the development of a national countering radicalization to violence strategy. It should be noted that some provincial governments have also adopted strategies to counter radicalization. For example, on June 10, 2015, the Quebec government unveiled the Government Action Plan 2015-2018 entitled "*La radicalisation au Québec: agir, prévenir, détecter et vivre ensemble*" which now includes 61 measures under the responsibility of 9 departments and two agencies. This action plan, which aims to prevent radicalization to violence, has measures to combat radicalization on the Internet. To this end, measure 2.5 aims to "educate young people about the use of ethical and responsible information technology and communications by providing schools with the awareness and prevention tools necessary." Moreover, measure 3.1 aims through a partnership between the Sûreté du Québec and other police forces to increase the ability to detect and anticipate threats on social media. Finally, the action plan also has measures that provide for the conduct of studies on radicalization leading to violence, some of which should address the issue of radicalization on the Internet.	
Under the Broadcasting Act, licensees are required to exercise judgement and use their "best efforts" to ensure that their services do not contain "prohibited material" as set out in the ICOP: "Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws."	Singapore
Through Norway's Action Plan against Radicalization and Violent Extremism, a group was put together in order to strengthening the presence of the police on the Internet. The group was placed at the NCIS. In addition to executing the tasks as described above (question 7), the group contributes with strengthening the competence regarding radicalization and violent extremism to other Norwegian law enforcement agencies/local police through seminar and lectures.	Norway
The countering of radicalism constitutes one of the priorities of the Security Framework 2016-2019 and of the government's National Security Plan 2016-2019. The "National plan for the countering of radicalism of 2005" has been amended and approved on 14 December 2015 by the National Security Council. It is a plan aiming, through collaboration of multiple public services, to reduce radicalism and extremism in our society. With this regard, the Radicalism Action Plan has to objectives: (1) set up a map of individuals and groups that have a racializing effect on their environment and (2) reduce the vectors of radicalization. Its goal is the early detection of radicalizing actors, in order to take necessary measures in time. The objectives and the development of the Plan form part of a common and integrated approach, under the form of a national taskforce and different work groups. The objective is to arrive, both at national and local level to: - The creation of an exchange of information forum between different services; - The processing of information in consultation; - The consensual proposition of appropriate measures.	Belgium
Kenya has a CVE strategy. The government through the National Counter Terrorism Centre (NCTC), which is the agency responsible for coordinating implementation of the strategy, is currently working with various partners in implementing parts of the strategy. In particular the government has collaborated with the European Union and the Government of Denmark in programs involving training of law enforcement officers and Prisons and Probation Services Officers to identify radicalization cases and equip them with the proper intervention tools and techniques. While	Kenya

the government CVE Programs continue to be effective, Al Shabaab has enhanced its radicalization efforts by increasing its penetration of communities for recruitment to join its radical movement. There is urgent need to strengthen community resilience among the affected groups to curb the growing radicalization and recruitment. The government therefore wishes to embark on a program to build capacity for youth and women groups to counter violent extremism in their communities. The State is currently developing a Community Policing Initiative and a community security system dubbed 'Nyumba Kumi' based on a ten-household's interactive security model premised on the idea that a small community as a unit can be accountable to each other, keep watch over the activities that happen within their neighborhood. • « Article 40A. of the Prevention of Terrorism Act (2012) (1) There is established a National Counter-Terrorism Centre, hereinafter referred to as the "Centre" which shall be an inter-agency body. […] » • « Article 40B. of the Prevention of Terrorism Act (2012) (1) The Centre shall be responsible for the co-ordination of national counterterrorism efforts in order to detect, deter and disrupt terrorism acts. (2) Without prejudice to the provisions of subsection (1) the Centre shall (a) establish a database to assist law enforcement agencies; (b) conduct public awareness on prevention of terrorism; (c) develop strategies such as counter and de-radicalization (d) facilitate capacity building for counter-terrorism stakeholders […] »	
Japan is implementing a variety of measures under the "3-Pillar Foreign Policy" which was formulated in 2015 in response to the terrorist incident regarding the murder of Japanese citizens. This consists of 1) Strengthening counter-terrorism measures, 2) Enhancing diplomacy towards stability and prosperity in the Middle East and 3) Assistance in creating societies resilient to radicalization. Regarding Assistance in Creating Societies Resilient to Radicalization, following measures are implemented: putting "The best way is to go in the Middle" concept into practice (realization of a vibrant and stable society); expanding people to people exhanges (including inviting religious leaders); coordination with ASEAN (promoting moderation, etc.).	Japan
The Ministry of Islamic Endowments (Awqaf) is legally responsible for issuing guidance to which all imams throughout Egypt are required to adhere, including weekly instructions on a provided theme that aims to prevent extremist language in sermons. The Ministry is also required to license all mosques in Egypt; however, many continued to operate without licenses. The government has the authority to appoint and monitor the imams who lead prayers in licensed mosques, and the government pays their salaries. Egypt's Dar Al-Iftaa (Egypt's official body for drafting religious edicts) has increased its efforts to counter violent extremism and extremist religious rhetoric, particularly online, where it has millions of followers on social media. Dar Al-Iftaa's countering violent extremism activities included sending scholars to remote areas of the country to engage communities considered vulnerable to violent extremist messaging; organizing international outreach and speaking tours throughout Muslim majority countries and the West; publishing books and pamphlets to undermine the alleged religious foundations of violent extremist ideology; running rehabilitation sessions for former violent extremists; and confronting violent extremists in cyber space.	Egypt
http://www.refworld.org/docid/5587c75915.html Countering Radicalization to Violence and Violent Extremism: Brazil's DPF Anti-Terrorism Division was created specifically to address threats of radicalization and to counter violent extremism.	Brazil
The United States' have a countering violent extremism strategy:	

In 2011, the United States issued its Strategy to Empower Local Partners to Prevent Violent Extremism in the United States. On December 18, 2015, Congress passed the Department of Homeland Security Appropriations Act, 2016 (Public Law 114-113). Section 543 of the Act and the accompanying Joint Explanatory Statement provide $10 million for "a countering violent extremism (CVE) initiative to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism." According to a Statement from January 2016 on the Department of Homeland Security website: The CVE Task Force (permanent interagency task force hosted by the Department of Homeland Security with averall leadership provided by the Department of Homeland Security and the Department of Justice with additional staffing provided by representatives from the FBI) will organize federal efforts into several areas, including: • Research and Analysis. The Task Force will coordinate federal support for ongoing and future CVE research and establish feedback mechanisms for CVE findings, thus cultivating CVE programming that incorporates sound results. • Engagements and Technical Assistance. The Task Force will synchronize Federal Government outreach to and engagement with CVE stakeholders and will coordinate technical assistance to CVE practitioners. • Communications. The Task Force will manage CVE communications, including media inquiries, and leverage digital technologies to engage, empower, and connect CVE stakeholders. • Interventions. The Task Force will work with CVE stakeholders to develop multidisciplinary intervention programs. https://www.dhs.gov/news/2016/01/08/countering-violent-extremism-task-force The FBI has launched a website "Don't be a puppet" aiming at preventing the youth from embracing violent ideologies.	United States of America
New Zealand's counter-terrorism efforts are reinforced by its engagement in interfaith and inter-cultural initiatives aimed at countering radicalization and terrorist recruitment. New Zealand (with Australia, Indonesia and the Philippines) co-sponsors the Asia-Pacific Regional Interfaith Dialogue. The Dialogue involves religious and community leaders from 15 countries from South East Asia and the Pacific and aims to foster tolerance, reinforce moderate religious views and isolate religious extremism. https://wikileaks.org/plusd/cables/08WELLINGTON424_a.html. The government also contributed to the development of 'Know Your Neighbors,' a regional education resource aimed at high school students in Southeast Asia and Australasia that sought to build greater understanding and respect of different cultures and religions, thereby helping to bridge some of the divides between societies around the region http://www.state.gov/j/ct/rls/crt/2010/170255.htm.	New Zealand
China does not appear to have an official strategy or program with regards to the countering of radicalization. However, pursuant to Article 17 of the Counter-Terrorism Law of 2015, "People's governments and relevant departments at all levels shall organize the initiation of counter-terrorism publicity and education, raising citizens' counter-terrorism awareness. Administrative management departments for education and human resources, schools and relevant vocational training institutions shall include knowledge of prevention and response to terrorist activities within their teaching, studies and training content. Relevant units such as for news, radio, television, culture, religion and the internet shall conduct pertinent counter-terrorism publicity and education aimed at the public. Villagers ' committees and residents ' committees shall assist people's governments and related departments in strengthening counter-terrorism publicity and education."	China
No. Legislations stated in Question 1a) are relied on. In an effort to better equip local communities with the means to prevent and counter violent extremism, Nigeria agreed to serve as an initial pilot country for the Global Community Engagement and Resilience Fund (GCERF). GCERF requires beneficiary countries to establish a multi-stakeholder "country support mechanism" that brings	Nigeria

together government agencies, civil society organizations, and the private sector to enable communities to develop localized CVE responses. Nigeria also agreed to serve as a pilot country for the Global Counterterrorism Forum-endorsed International CT/CVE Clearinghouse Mechanism, which is being developed as a means to help countries and donors optimize civilian counterterrorism and CVE capacity-building programs. CVE efforts continued to be hindered by the security forces' harsh treatment of civilians, lack of trust between security services and communities, and lack of economic opportunities in the northeast. An English language program to promote leadership, tolerance, and civic engagement was implemented to provide training of trainers – teachers and students – in Kano and Jos. English language clubs were also used to expand the teaching and themes of the program to youth in these states. Dandal Kura, a shortwave radio program targeting northeastern Nigeria, continued to provide access to credible information for its listeners. Dandal Kura, which also uses a combination of high-tech and low-tech tools – including SMS, e-mail, Facebook, Twitter, and a website – to reach and interact with its audience, has developed a tremendous following since it went live in January 2015 http://m.state.gov/md257514.htm	
The UAE government continued to support Hedayah, the International Center of Excellence for Countering Violent Extremism (CVE), which it hosts in Abu Dhabi. In June, Hedayah conducted a workshop bringing together CVE practitioners and former foreign terrorist fighters to discuss the foreign terrorist fighter threat and counter-messaging approaches to address it. Hedayah participated in the Madrid+10: Stop Violent Extremism conference in Spain in October, where it also organized a two-day workshop on the Role of Women in Countering Radicalization and Violent Extremism. Hedayah hosted a follow-up International CVE Research Conference in December in coordination with Edith Cowan University and New York University Abu Dhabi Institute. In addition to supporting Hedayah, the UAE government in July partnered with the U.S. government to launch the Sawab Center in Abu Dhabi, a new social media platform focused on countering ISIL's radical narratives and online propaganda. The UAE was also host to the Forum for Promoting Peace in Muslim Societies. To prevent violent extremist preaching in UAE mosques, the General Authority of Islamic Affairs and Endowments provided guidelines for all Friday sermons and monitored mosques' compliance, excluding those in Dubai, which has its own system under the supervision of Islamic Affairs and Charitable Activities Department. Abroad, the General Authority continued providing training to cohorts of Afghan imams on preaching messages of non-violence and tolerance. During key periods of Muslim religious observance, especially the fasting month of Ramadan, the UAE government aired commercials on television warning Muslim citizens and residents to refrain from donating money at mosques, as the funds could unknowingly support terrorist causes. The UAE also worked to keep its education system free of violent extremist influences, emphasizing social tolerance. In November, the UAE government announced its plan to open in Al Ain a branch of Egypt's Al-Azhar University, a premier institution of Islamic learning, as a way to promote the teaching of moderate Islam in the Gulf region. The Government of the UAE also received training on social media analysis to enhance its ability to combat ISIL's use of the internet to spread propaganda and increase recruitment. The United Arab Emirates has subjected all media forms to monitoring, and is using them, including TV channels, to teach the “right Islam” and rebut distorted violent ideology.	United Arab Emirates
The French Government has established an information platform on the risks related to Islamic radicalization via the electronic communication networks: « Stop-djihadisme.gouv.fr ». The Governemnt has also launched a line dedicated for the reporting of radicalization. As the campaign’s government-run website boasts, France has instituted counter-jihadism measures to its education (by presenting 11 measures to prevent radicalization and promote secular, republican values within France’s school system) and prison systems (by segregating extremist inmates), allocate additional resources to its counterterrorism agencies, and enforce the country’s November 2014 anti-terror law. In September 2016, France’s first de-radicalization center opened. Thirteen other centers will open.	France
The interagency unit called NCTC's (composed of officers from the Intelligence, Police, Defense, Immigration, and Prison sectors) is in charge of the countering violent extremism strategy.	Tanzania

It has launched a community policing program. Through this initiative, which has been active in many perceived radicalization hot spots for several years, officials believe they are building better relations with key communities and have been better able to detect threats tied to radicalization. In addition, police enforced laws against spreading messages advocating violence by confiscating cassettes containing violent extremist messaging that are sold on the streets. Finally, Tanzania has outreached religious leaders to encourage moderate voices and to discourage guest preachers who might seek to spread extremist ideologies in houses of worship. http://www.refworld.org/docid/57518d812f.html	
Federal Law No 35-FZ, supplemented by a new official approach to countering terrorism in 2009, redistributed responsibilities among state agencies by creating a National Antiterrorism Committee (NAK) tasked with coordinating counterterrorism policies and operations, and a Federal Operational Coordination Centre (FOCC) within it. The director of the Federal Security Service (FSB) acts as chairman of the NAK, and decides on the execution of counter-terrorism activities. The Ministry of Defence plays an important role in coordinating efforts to prevent terrorist attacks on nuclear sites and attacks involving weapons of mass destruction, and in organising special operations to eliminate illegal armed groups and block illegal traffic of arms, ammunition and fissile and highly toxic materials.A presidentialdecree inDecember 2015 established counter-terrorism operational headquarters in five of Russia's coastal cities: Kaspiysk, Murmansk, Petropavlovsk-Kamchatsky, Simferopol and Yuzhno-Sakhalinsk. The centres are tasked with organising the use of force and managingcounterterrorism operations in Russian waters.	Russia
(10) Does your country allow extradition of authors and accomplices charged with internet radicalization in other countries?	**STATES**
As a starting point Denmark would allow extradition, if internet radicalization is defined as a criminal offence.	Denmark
Extradition to the UK Outgoing extradition requests to countries other than those which operate the EAW system (ie category 1 territories) fall outside the scope of the 2003 act and are made under the royal prerogative. ICU at the Home Office forwards extradition requests that have been prepared by the prosecuting authorities in England and Wales and Northern Ireland (eg CPS, Serious Fraud Office or Public Prosecution Service Northern Ireland) to the requested state through the diplomatic route. The COPFS deals with Scottish outgoing extradition requests, these are also transmitted to the requested State through diplomatic channels. An outgoing request can either be: a full order request (ie a request which fully complies within the requirements of the relevant treaty or other international arrangement with the requested state) a request for provisional arrest - this is made when someone is known to be in a particular country but where there is insufficient time to prepare a full request, because the person is deemed to be a flight risk Where a request for provisional arrest is accepted, the person will usually be arrested in the requested state before extradition papers are formally submitted. When someone is provisionally arrested there is a deadline within which the papers must be submitted. This deadline is set out in the treaty or other arrangements governing extradition arrangements with that state. ICU liaises with the relevant prosecuting authority to make sure the papers are delivered in enough time for ICU to dispatch them. Bringing a requested person back to the UK Once a requested person is available for surrender, ICU will be notified by the British Embassy or High Commission, or the police will be notified by Interpol. The police (usually from the force where the original arrest warrant was issued) then collect and escort the requested person back to the UK. ICU will forward the officers' travel arrangements to the relevant British Embassy or High Commission and can provide a letter of introduction for officers, which will allow them to bring the requested person back.	United Kingdom
The general extradition rules provided by the Code of Penal Procedure are applied. Article 12 of the law against terrorism provides that the Tribunal expulses any convicted foreigner.	Tunisia

N/A	Albania
Hungary allows extradition if the following conditions are met: Section 11 (2) of the Hungarian Act XXXVIII of 1996 on mutual legal assistance in criminal matters provides that extradition for the purpose of conducting criminal proceedings shall be granted where the act for which extradition is requested is punishable under both the law of Hungary and the law of the Requesting State by imprisonment of at least one year. This requirement is deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that the offence regardless of its denomination is punishable under the laws of both countries by imprisonment of at least one year. Section 12 of this Act provides that extradition shall be refused, if • the offence or penalty for which extradition is requested has become barred by lapse of time under the law of either the Requesting State or Hungary, • the person claimed has been granted a pardon or amnesty in respect of the offence or punishment, • in the Requesting State the private bill of indictment or other motion having equivalent effect, or the consent required for the institution of criminal proceedings has not been submitted or granted, • a Hungarian court has already finally adjudicated the offence for which extradition is requested. Section 13 of the Act provides furthermore that the extradition of a Hungarian national shall not be granted unless the person claimed is simultaneously a national of another state and is not resident in Hungary.	Hungary
No.	India
The terrorism offences Division 102 of Part 5.3 of the Criminal Code have extraterritorial application. In other words, the offences apply whether the conduct which is the subject of the offence occurs within or outside Australia.	Australia
German law allows for an extradition if the offence is an unlawful act under German law or unless mutatis mutandis the offence would also constitute an offence under German law and is punishable under German law by a maximum penalty of imprisonment of no less than one year, or, in the case of an extradition for the purpose of enforcement of a sentence, a custodial penalty still to be served is not less than four months.	Germany
Internet radicalization has not been defined as an offence, and is therefore not an extraditable offence. However, if the Internet is used as a medium to commit an extraditable offence, then the offender would be extradited for that offence.	Seychelles
According to Section 2 of the Extradition Law 5714-1954, a person may be extradited for offences punishable with at least one year imprisonment. In this respect, the requirement of double criminality was interpreted broadly by the Israeli courts. Thus, extradition based on charges related to internet incitement could be possible.	Israel
According to Code of Criminal Procedure which has special part (in concreto Part five) that deals with extradition in connection with third countries and also there is European Arrest Warrant which deals with extradition at the European Union level.	Slovakia
Spanish Law on passive Extradition (Law 4/1985) allows the extradition of persons accused of radicalization, to be tried where the crime in question has “not less than one year of deprivation of freedom in its maximum degree or a more serious penalty or where the claim was entered for the enforcement of a sentence to a penalty or security measure not less than four months' imprisonment for acts also punishable under Spanish law”.	Spain

Sweden will, in general, allow extradition of persons charged with acts related to internet radicalization provided that the act also constitutes a crime according to Swedish law (see question 1).	Sweden
No, unless there is a bilateral agreement for such an issue.	Irak
Extradition from Canada is only available if the requirement for dual criminality provided for in paragraph 3(b) of the Extradition Act is met. More specifically, paragraph 3(b) only allows for extradition if the conduct for which the person is sought, had it occurred in Canada, would have constituted an offence punishable in Canada. The replies to questions 1-3 of this questionnaire provide guidance concerning what Canadian criminal offences might address conduct characterized in this questionnaire as "radicalization on the internet".	Canada
Singapore law does not at present allow the extradition of persons on the basis that they are charged with internet radicalization in other countries.	Singapore
As mentioned, internet radicalization is not criminalized as such in Norway. Whether or not extradition is allowed for other offences, varies. Firstly: Norwegian citizens cannot be extradited according to the Norwegian Act on Extradition s. 2. For citizens of other countries who are currently staying in Norway, extradition can only be allowed under certain conditions. Most important is that for extradition to be allowed, the person has to have committed a crime that can be punished after Norwegian law with at least 1-year imprisonment (s. 3,1). If the person is already convicted in Norway for this crime, the punishment must have been at least 4 months' detention. There are exceptions from this if there is an agreement with another state on beforehand deciding a shorter period of detention/imprisonment is accepted (s. 3,2). For crimes that are viewed as 'political', extradition is not allowed (s. 5,1).	Norway
Yes. However, in practice, the Belgian justice system has yet to be seized with an extradition request for such facts.	Belgium
There no specific provision with regards to the offence of internet radicalization. However, according to Article 26(A) of the Criminal Code, "Where a person who is not a citizen of Kenya is convicted of an offence punishable with imprisonment for a term not exceeding twelve months the court by which he is convicted, or any court to which his case is brought by way of appeal against conviction or sentence may, by directions to the Commissioner of Police and the Commissioner of Prisons (including directions on how the order shall be carried out) order that the person be removed from and remain out of Kenya either immediately or on completion of any sentence of imprisonment imposed; but where the offence for which the person is convicted is punishable with imprisonment for a term exceeding twelve months, the court shall, where it is satisfied that the person may be removed from Kenya, recommend to the Minister for the time being responsible for immigration that an order for removal from Kenya be made in accordance with section 8 of the Immigration Act."	Kenya
There no specific provision with regards to the offence of internet radicalization. According to Article 37 of the Anti-Terrorism Law of 2015, in relation to any terrorist crime, and in addition to imposing the prescribed penalty, the court may impose, amongst other measures, the deportation of foreigners.	Egypt
There no specific provision with regards to the offence of internet radicalization. Regarding extradition in general, according to Article 5(LI) of the Brazilian Constitution, "no Brazilian may be extradited except for a naturalized Brazilian, if extradition is requested for a common crime committed prior to naturalization or for proven involvement in unlawful traffic in narcotics and similar drugs, as provided by law."	Brazil

There is no specific provision with regards to the offence of internet radicalization. As a general principle, and according to Article 602 of the Code of Criminal Procedure "If an authority of a foreign State requests the extradition of a prosecuted person in order to conduct criminal proceedings against him, or to execute a penalty or a preventive measure previously imposed, the state prosecutor shall examine this person and, if necessary, secure the material evidence in this country, whereupon he shall file the case with a Voivodship Court having territorial jurisdiction over the case." Pursuant to Article 604 of the Code of Criminal Procedure: "§ 1. The extradition is inadmissible if: 1) the person to whom such a motion refers, is a Polish citizen or has been granted the right of asylum in the Republic of Poland, 2) the act does not have the features of a prohibited act, or if law stipulates that the act does constitute an offence, or that a perpetrator of the act does not commit an offence or is not subject to penalty, 3) the period of limitation has lapsed, 4) the criminal proceedings have been validly concluded concerning the same act committed by the same person, 5) the extradition would contravene Polish law § 2. In particular, extradition may be refused, if: 1) the person to whom such a motion refers has permanent residence in Poland, 2) the criminal offence was committed on the territory of the Republic of Poland, or on board a Polish vessel or aircraft, 3) a criminal proceeding is pending concerning the same act committed by the same person, 4) the offence is subject to prosecution on a private charge, 5) pursuant to the law of the State which has moved for extradition, the offence committed is subject to the penalty of deprivation of liberty for a term not exceeding one year, or to a lesser penalty or such a penalty has been actually imposed, 6) the nature of the offence with which the motion for extradition is connected is political, military or fiscal, or 7) the State which has moved for extradition, does not guarantee reciprocity in this matter. § 3. In the event indicated in § 1 subsection (4) and § 2 subsection (3), the resolution of the motion for extradition may be adjourned, until the criminal proceedings pending against the same person in the Republic of Poland are concluded, or until he has served the sentence imposed or has been granted remission of the penalty."	Poland
There is no specific provision with regards to the offence of internet radicalization.	United States of America
There is no specific provision with regards to the offence of internet radicalization. Regarding extradition in general, Article 8 of the Extradition Act of 1999 relating to Discretionary restrictions on surrender provides that: "(1) A discretionary restriction on surrender exists if, because of- (a) the trivial nature of the case; or (b) if the person is accused of an offence, the fact that the accusation against the person was not made in good faith in the interests of justice; or (c) the amount of time that has passed since the offence is alleged to have been committed or was committed, and having regard to all the circumstances of the case, it would be unjust or oppressive to surrender the person. (2) A discretionary restriction on surrender exists if the person has been accused of an offence within the jurisdiction of New Zealand (other than an offence for which his or her surrender is sought), and the proceedings against the person have not been disposed of."	New Zealand
There no specific provision with regards to the offence of internet radicalization. Regarding extradition in general, pursuant to Article 7 of the Extradition Law of 2000, a "request for extradition made by a foreign state to the People's Republic of China may be granted only when it meets the following conditions:	China

(1) the conduct indicated in the request for extradition constitutes an offence according to the laws of both the People's Republic of China and the Requesting State; and (2) where the request for extradition is made for the purpose of instituting criminal proceedings, the offence indicated in the request for extradition is, under the laws of both the People's Republic of China and the Requesting State, punishable by a fixed term of imprisonment for one year or more or by any other heavier criminal penalty; where the request for extradition is made for the purpose of executing a criminal penalty, the period of sentence that remains to be served by the person sought is at least six months at the time when the request is made. If the request for extradition concerns miscellaneous offences which conform to the provisions of Subparagraph (1) of the preceding paragraph, as long as one of the offences conforms to the provisions of Subparagraph (2) of the preceding paragraph, extradition may be granted for all of those offences." However, the request for extradition made by a foreign state to the People's Republic of China shall be rejected if, for example the person sought is a national of the People's Republic of China under the laws of the People's Republic of China or if, at the time the request is received, the judicial organ of the People's Republic of China has rendered an effective judgement or terminated the criminal proceedings in respect of the offence indicated in the request for extradition or again if the request for extradition is made for a political offence, or the People's Republic of China has granted asylum to the person sought.	
There is no specific provision with regards to the offence of internet radicalization. As regards to extradition rules in general, Article 12 of the International Cooperation in Criminal Matters and Extradition Law No. 24767 of 18 December 1996 provides that extradition of nationals is allowed but the suspect has the right to choose to be tried by Argentine courts; if that option is chosen, extradition is denied.	Argentina
No. Pursuant to Section 22 on the Extradition (Terrorism Act of 2011), "Offences under section 1, 2, 3, 4, 5, 6, 10, 11, 13 and 14 of this Act Extradition, are considered to be an extradition crime for which extradition may be requested, granted or obtained under the Extradition Act."	Nigeria
There is no specific provision with regards to the offence of internet radicalization. However, regarding general rules of extradition, Article 38 of the Constitution of 1971 provides that "the extradition of citizens and of political refugees shall be prohibited". In addition, individuals can be deported: • Pursuant to Article 46 of Federal Law No. (7) of 2014 On Combating Terrorism Offences, "Every ruling of conviction for terrorist offence issued against a foreigner shall necessitate expulsion of the convict outside the country after the lapse of the penalty ruled." • Pursuant to Article 42 of the Federal Decree-law no. (5) of 2012 on Combating Cybercrimes, "The court may decide deportation of a foreigner who is condemned in any of the crimes specified in this DecreeLaw upon execution of the punishment adjudged." • Pursuant to Article 18 of the Federal Decree Law No. 2 of 2015 On Combating Discrimination and Hatred, "[…] The court shall order the expulsion of a foreigner from the country after the execution of the penalty charged thereof."	United Arab Emirates
There is no specific provision with regards to the offence of internet radicalization. Extradition in general is provided by Article 692-2 of the Criminal Code: "The French government may hand over any person who does not have French nationality and who is the subject of a prosecution initiated in the name of the requesting state or of a conviction imposed by its courts, to foreign governments, at their request, where this person is found on French national territory. However, extradition is only granted if the offence for which the application has been made was committed: - either on the territory of the requesting state by a national of this state or by a foreigner;	France

- or outside the territory of the requesting state by a national from that state; - or outside the territory of the requesting state by a foreigner, where the offence features among those for which French law authorises prosecution in France, even if they are committed by a foreigner abroad. [...]"	
There is no specific provision with regards to the offence of internet radicalization. The general rules of extradition can be found in the Extradition Act of 1965: Part II – The Surrender of fugitive criminals "5.-(1) A requisition for the surrender of a fugitive criminal of any country who is in or suspected of being in Tanzania shall be made to the Minister by a diplomatic representative or consular officer of that country and, upon receipt of such requisition, the Minister may, by order under his hand, signify to a magistrate that a requisition has been made and require the magistrate to issue his warrant for the arrest and detention of the fugitive criminal. (2) If the Minister is of the opinion that the offence is one of a political character he may refuse to make an order and may also at any time order a fugitive criminal accused or convicted of such offence to be discharged from custody."	Tanzania
There no specific provision with regards to the offence of internet radicalization. Regarding extradition in general, Article 464 of Criminal-procedure Code of the Russian Federation prohibits the extradition of nationals of the Russian Federation.	Russia
(11) For the purposes of countering online radicalization has your country introduced specific: **(a) 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).** **(b) Specific tribunals/administrative bodies with oversight authority including the application of the remedies listed under point 5 above?**	**STATES**
a) There are no special enforcement tools under the Danish legal system. **b)** There are no specific tribunals or authorities set up.	Denmark
a) https://cst.org.uk/docs/countering_online_radicalisation1.pdf **b)** The Investigatory Powers Tribunal (IPT) investigates complaints that law enforcement and the security and intelligence agencies have used their covert investigative techniques unlawfully or claims that the intelligence or law enforcement agencies have breached human rights legislation. It is an independent Tribunal comprised of judges and senior members of the legal profession. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf	United Kingdom
a) Specific procedures exist in the Anti-Terrorism Law. **b)** The judiciary Anti-Terrorism Unit created following the Anti-Terrorism Law.	Tunisia
a) In Albania according to constitutional rights the service provider is obliged to stop or prevent a violation, if required by court or by the responsible authorities, in accordance with legislation in force.	Albania

These limitations may not infringe the essence of the rights and freedoms and in no case may exceed for in the European Convention on Human Rights. **b)** There are no specific tribunals or authorities set up.	
[No answer given by the State].	Hungary
a) 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). **b)** There are no specific tribunals or authorities set up.	India
a) Australia has not introduced specific enforcement tools for the purposes of countering online radicalization. However, there are generally-available powers that can address this issue. There are powers under the Telecommunications (Interception and Access) Act 1979 (the TIA Act) that allow law enforcement and security agencies to investigate online terrorist propaganda and incidents of radicalization. For such purposes, agencies can obtain telecommunications interception warrants, stored communications warrants and access telecommunications data. Each power is only available for certain offences that meet the offence thresholds. For example, agencies can obtain telecommunications interception warrants for 'serious offences' (these are offences that generally carry a penalty of imprisonment of 7 years or more). This definition includes the Commonwealth Criminal Code offences of advocating terrorism and urging violence against members of groups. A telecommunications interception warrant could allow agencies to determine and identify the source of terrorist propaganda. The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 amended the TIA Act to require service providers in Australia to retain certain telecommunications data for a period of two years. Although service providers are not required to retain the source or destination IP address of a communication, agencies can often obtain this information (e.g. which IP address was a post uploaded from) from social media providers. In such circumstances, the requirement to keep a record of IP/Port address assignations will allow agencies to attribute such posts back to a particular user. **b)** There are no specific tribunals or authorities set up.	Australia
a) There are no rules specifically applicable to online radicalization. Instead, the general rules for prosecution apply. **b)** Under the Code of Criminal Procedure and relevant administrative law measures taken for the purpose of investigation or enforcement may be subject to judicial review or, in some cases, judicial approval beforehand. This includes the measures mentioned under Q5 above. The conditions for the review/approval and the courts responsible for that depend on the individual measure. As an example, complaints against an action in the course of prosecution are dealt with by the competent criminal courts while complaints against orders by the media supervisory authorities are dealt with by the administrative courts.	Germany
a) Seychelles has not encountered the issue of internet radicalization within the scope of the above question, requiring specific measures as described. Law enforcement agencies can intercept any online transaction, propaganda, incitement, communication, etc. by an application to the court for an order to intercept, for investigation purposes. **b)** There are no specific tribunals or authorities set up.	Seychelles
a) There are no special enforcement tools available under the Israeli legal system.	Israel

b) There are no specific tribunals or authorities set up.	
a) In Slovak national law we don´t have specific enforcement tools oriented to the area of the internet radicalization. We think that it is interesting to mention enforcement tools at the European Union level, in connection with already mentioned RAN. Those are not really legislative tools but might be very helpful in order to prevent and reduce negative impacts of internet radicalization. These tools are mostly Education (RAN EDU) which is about equipping and empowering teachers and the education sector to deal with radicalization, EXIT (RAN EXIT) – focused on de-radicalization and disengagement programs that help individuals to move from a radicalized and violent mind-set towards mainstream society, HELP FOR VICTIMS and many more (list is available on RAN web site). **b)** Nowadays we have one specific tribunal so called Specialized criminal court. This court has authority only for proceedings where there are crimes of terrorism, but just for now. In our national law there was imposed proposal according to which also crimes of extremism will be held by this Specialized criminal court.	Slovakia
a) Any measure of research to combat radicalization as an offence is subject to judicial authorisation and supervision in our legal system. Likewise, this judicial authorization is subject to the principles of specialty, suitability, exceptionality, necessity and proportionality. **b)** Ordinary judges and courts are responsible for authorizing or supervising the measures referred to in question 5.	Spain
a) There are no special enforcement tools under the Swedish legal system. **b)** There are no specific tribunals or authorities set up.	Sweden
a) CMC charining committee consisted of security agencies and has administrative authority for such a purpose. **b)** There is a publish and media court which looks into such cases and works based above mentioned laws.	Irak
a) The Criminal Code has two unique tools: the recognizance with conditions, which is designed to prevent terrorist activity, and the terrorism peace bond, which is designed to prevent a terrorism offence. The Recognizance with Conditions Under section 83.3 of the Criminal Code, a peace officer can apply to a judge to have a recognizance with conditions imposed on a person where the peace officer believes on reasonable grounds that a terrorist activity may be committed and suspects on reasonable grounds that imposing the recognizance on the person is likely to prevent the carrying out of a terrorist activity. There is a limited power for the police to arrest the person without a warrant in order to bring him or her before a judge for a hearing to decide on whether to impose the recognizance -- for example, in the case of exigent circumstances. However, if a judge is available within 24 hours of arrest, the police must bring the person before the judge without unreasonable delay or, if a judge is not available within that time frame, as soon as feasible. Once the person is brought before the judge, the judge must release the person pending the hearing unless the peace officer shows cause why the person should continue to be detained. The grounds of detention are set out in subsection 83.3(7) of the Criminal Code, such as the likelihood that, if the person is released from custody, a terrorist activity will be carried out. A judge may order detention for 48 hours for three consecutive 48 hour periods before the hearing takes place, for a maximum of six days of judicially-ordered detention. However, after the first 48-hour period, the judge must not only be satisfied that a ground for detention continues to be satisfied, but also that the investigation in relation to which the person is detained is being conducted diligently and expeditiously. At the hearing, where satisfied by the evidence that the police officer has the requisite reasonable grounds set out previously, a judge may order that the person enter into a recognizance with conditions. The recognizance	Canada

lasts for one year unless the person has a previous conviction for a terrorism offence in which case it may last for two years. If the person refuses to enter into the recognizance, he or she may be imprisoned for up to one year. While the judge may impose any reasonable condition, the judge must consider, for example, whether to order the person to surrender their passport(s) or other travel document or to remain within a specific geographic area. The recognizance with conditions has numerous safeguards, including the prior consent of the appropriate Attorney General, a process that allows the conditions imposed to be varied, and annual reporting on its use. The Terrorism Peace Bond Under section 810.011 of the Criminal Code, anyone can apply for peace bond to be imposed on a person where the applicant fears on reasonable grounds that the person may commit a terrorism offence. If the judge is satisfied that the applicant has reasonable grounds for the fear, the judge may order the person to enter into the peace bond for up to one year, unless the person has been previously convicted of a terrorism offence, in which case the recognizance may be imposed for up to five years. As is the case for the recognizance with conditions, the judge must consider, for example, whether to impose a geographical restrictions condition on the person and whether to require the person to surrender their passport(s) or other travel documents. The prior consent of the appropriate Attorney General is also required. Other Measures The Criminal Code allows a judge to order the seizure and forfeiture of terrorist propaganda material that is in printed form or is in the form of audio recordings (section 83.222). A judge may also order the removal of terrorist propaganda when it is in electronic form and is made available to the public through a Canadian Internet service provider (ISP) (section 83.223). Terrorist propaganda is defined in subsection 83.222(8) to mean "any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general — other than an offence under subsection 83.221(1) [i.e., the offence of advocating or promoting the commission of terrorism offences in general] — or counsels the commission of a terrorism offence." As well, terrorist propaganda has been added to the Customs Tariff so as to prevent the importation of such material into Canada. Provincial Approaches Some provinces have their own measures, for example, the Sûreté du Québec has been monitoring the web by its permanent lookout social media team to detect radicalization and risky behavior on the Internet. **b)** See the response to Question 11a.	
a) The Internal Security Act introduces key enforcement tools, e.g. detention orders, police supervisory orders, that can serve to counter online radicalization, amongst other acts that threaten our national security. Relevant procedures and safeguards, including the establishment of independent Advisory Boards are provided within the Act.	Singapore
a) No. **b)** No.	Norway
a) There is no specific procedure applicable in the matter. **b)** There are no specialized tribunals. Attorney generals and judges exercise their judicial control on such measures.	Belgium
a) The Countering Terrorist Fighters Legislation Bill (2014) gives the Security Intelligence Service (SIS) greater surveillance powers and the Minister of Internal Affairs greater powers to suspend and cancel passports. It can now conduct surveillance for up to 24 hours on terrorist suspects without a warrant, conduct video surveillance	New Zealand

on private property in relation to suspected terrorism, and gain access to Customs data in relation to suspected terrorism. The Minister of Internal Affairs can now suspend passports for up to 10 working days and cancel them for up to three years. **b)** New Zealand does not appear to have created specific bodies.	
a) France is actually under a state of emergency which extends the powers of the administrative authority. The decree gives the police power to carry out searches without the approval of a judge as well as place suspects under house arrest without prior judicial authorization. Law enforcement can also dismantle groups Regarding tools to counter illicit content online, see question 5. **b)** A specific unit called "Pôle antiterroriste du parquet de Paris" in Paris is composed of judges and is dedicated to countering terrorist offences and has national jurisdiction on terrorist matters. Further, the « Groupe d'Intervention de la Gendarmie Nationale" (GIGN) is the law enforcement division that conducts counter-terrorist operations.	France
a) Roskomnadzor carries out orders issued by the Prosecutor General's Office to block content that is extremist or contains calls for participation in unsanctioned public actions. **b)** Roskomnadzor, and the Prosecutor General's Office.	Russia
a) Yes. **b)** Federal High Court.	Nigeria
(12) 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.)?	**STATES**
A judicial decision may have extraterritorial effect if Denmark has criminal jurisdiction. The Criminal Code section 6 – 9 a regard jurisdiction: **Section 6:** (1) Acts falling within Danish criminal jurisdiction are acts committed - i. within the Danish state; ii. on board a Danish vessel or aircraft located within the territory of another state by a person belonging to or travelling on the vessel or aircraft; or iii. on board a Danish vessel or aircraft located outside the territory of any state. **Section 7:** (1) Acts committed within the territory of another state by a person who was a Danish national or has his abode or similar habitual residence within the Danish state at the date of the provisional charge are subject to Danish criminal jurisdiction, if - i. the act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality); or ii. the offender had the aforesaid attachment to Denmark when committing the act and such act – a. comprises sexual abuse of children, human trafficking or female circumcision; or b. is aimed at someone having the aforesaid attachment to Denmark when the act was	Denmark

committed.
(2) Acts committed outside the territory of any state by a person having such attachment to Denmark as referred to in subsection (1) at the date of the provisional charge are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term exceeding four months.
(3) Subsections (1)(i) and (2) apply, with the necessary modifications, to acts committed by a person who is a national of or has his abode in Finland, Iceland, Norway or Sweden at the date of the provisional charge, and who is staying in Denmark.

Section 7 a:
(1) Acts committed within the territory of another state and aimed at a person who was a Danish national or had his abode or similar habitual residence within the Danish state when the act was committed are subject to Danish criminal jurisdiction if any such act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality) and may carry a sentence under Danish legislation of imprisonment for at least six years.
(2) Danish criminal jurisdiction under subsection (1) only applies to the acts of -
i. murder;
ii. aggravated assault, deprivation of liberty or robbery;
iii. offences likely to endanger life or cause serious injury to property;
iv. sexual offences or incest; or
v. female circumcision.
(3) Acts committed outside the territory of any state, but aimed at someone having such attachment to Denmark as referred to in subsection (1) when the act was committed are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term exceeding four months.

Section 7 b:
(1) Where the application of Danish criminal jurisdiction to a legal person is subject to dual criminality, the criminal liability of legal persons need not be prescribed by the legislation of the country in which the act was committed.

Section 8:
(1) Acts committed outside the Danish state are subject to Danish criminal jurisdiction, irrespective of the home country of the offender, where -
i. the act violates the autonomy, security, Constitution or public authorities of the Danish state, or official duties to the state;
ii. the act infringes interests which are given legal protection in the Danish state on the condition of particular attachment to the country;
iii. the act breaches an obligation which the offender is required by law to observe abroad;
iv. the act breaches an official duty incumbent on the offender to a Danish vessel or aircraft;
v. the act falls within an international instrument obliging Denmark to have criminal jurisdiction; or
vi. extradition for the purpose of prosecution in another country of a person provisionally charged is refused, and the act, provided that it was committed within the territory of another state, is a criminal offence under the legislation of the country in which the act was committed (dual criminality), and the act may carry a sentence under Danish legislation of at least one year in prison.

Section 8 a:
(1) Acts committed outside the Danish state are subject to Danish criminal jurisdiction where acts of the kind described fall within the Statute of the International Criminal Court, provided that any such act was committed by a person who, at the date of the provisional charge -
i. was a Danish national or had his abode or similar habitual residence in Denmark; or
ii. was staying in Denmark.

Section 8 b:
(1) Acts committed outside the Danish state are subject to Danish criminal jurisdiction where any such act falls within section 183a and the act was committed by a person who, at the date of the provisional charge -
i. was a Danish national or had his abode or similar habitual residence in Denmark; or

ii. was staying in Denmark. (2) The prosecution of acts falling within subsection (1) may also include violations of sections 237 and 244-248 committed in conjunction with a violation of section 183a. **Section 9:** (1) Acts are deemed to have been committed at the place where the offender was when the act was committed. As regards legal persons, acts are deemed to have been committed at the place where the act(s) implying the liability of the relevant legal person were committed. (2) If the criminality of an act depends on or is influenced by an actual or intended consequence, the act is also deemed to have been committed at the place where the effect occurred, or where the offender intended the effect to occur. (3) Attempts or acts of complicity are deemed to have been committed within the Danish state if the offender was in Denmark when the act was committed, irrespective of whether the offence was completed or intended to be completed outside the Danish state. (4) Where part of an offence was committed within the Danish state, the full offence is deemed to have been committed in Denmark. **Section 9 a:** (1) An offence relating to text, sound or image data, etc., made generally available in Denmark through the Internet or a similar system for dissemination of information by acts committed abroad is deemed to have been committed within the Danish state if the data is related specifically, to Denmark. Enforcing a Danish judicial decision abroad can be difficult depending on which country the decision regards. [On the other issues, no answer was given by the State].	
See Sections 3 and 4 of the Terrorism Act of 2006.	United Kingdom
Tunisia follows international standards on that issue. Specific jurisdiction is given to the ATI (Agence Tunisienne de l'Internet) and to the ANS (Agence Nationale de la Sécurité informatique)	Tunisia
No.	Albania
The territorial and personal scope of the CC is provided by section 3 of the CC. According to this Hungarian criminal law shall apply: - if the criminal offence is committed in the territory of Hungary; - if the criminal offence is committed on board of a Hungarian watercraft or a Hungarian aircraft situated outside the territory of Hungary, - to any act committed by a Hungarian national abroad, which considered to be a criminal offence in accordance with Hungarian law. Hungarian criminal law shall, furthermore, apply: - to any act committed by a non-Hungarian national abroad, if: ad. a. it is a criminal offence under Hungarian law and it is punishable as well in accordance with the law of the country where it was committed, ad. b. it is a criminal offence against the State, excluding espionage against allied armed forces and espionage against the institutions of the European Union, regardless of the fact whether it is punishable in accordance with the law of the country where it was committed or not, ad. c. it is a criminal offence under Chapter XIII or XIV or any other criminal offence which is to be prosecuted under an international treaty proclaimed by an act of Parliament, - to any act committed by a non-Hungarian national abroad against a Hungarian national, a legal person and other legal entity without legal personality established under Hungarian law, which is punishable under Hungarian law.	Hungary

The main purpose of rendering data inaccessible (section 77 of the CC, in a criminal case is to remove the illegal content (delete it from the storage server which can be done by the web hosting provider), if this is does not bring any successful result, then the court orders the temporary prevention of access to electronic data ("blocking" by the internet providers). If such content is in the possession of a foreign service provider, it is possible to initiate the removal of the illegal content within the framework of international legal assistance. If such request fails to bring about successful results within 30 days, then the court orders the blocking of the illegal content, and as a result the illegal content will not be accessible for users of Hungarian internet service providers. It can also be mentioned that in order to be able to prevent the injurious situation to continue, it is possible to render online content (electronic data) temporarily inaccessible [section 158/B-158/D. § of Act XIX of 1998 on the Criminal Procedure Code] during the criminal procedure in Hungary as a coercive measure ordered by the court.	
India has provided for extra-territorial jurisdiction under the Indian Information Technology Act, 2000. Thus, even if the legal entity violating the law may be located outside the territorial boundaries of India but its contents are available on computers, computer systems, computer networks, computer resources and communication devices located in India, the provisions of the Indian Information Technology Act, 2000 are made applicable to the said legal entity by virtue of Section 1 of the Indian Information Technology Act, 2000. Though as provided for statutory jurisdiction, there is no specific manner of how this extra-territorial jurisdiction can be enforced.	India
Section 313 of the Telecommunications Act 1997 and take-down notices issued under the Broadcasting Services Act 1992 (the BSA Act) do not have extraterritorial effect. The jurisdiction criterion is determined by the location of the host of the online content. For example, the Office of the Children's E-Safety Commissioner can only direct an Australian content service provider (an internet content host who hosts internet content in Australia) to prevent access to prohibited content under the BSA Act. There is no provision for such enforcement tools to be enforced against the subsidiaries of internet service providers headquartered in other jurisdictions. Nevertheless, agencies can seek their assistance (either domestically or otherwise) on a voluntary basis.	Australia
In the field of criminal law judicial measures in principle only have territorial effects. If there is a need for extraterritorial measures a mutual legal assistance request to the relevant state will be issued. Such requests directed to Germany could be executed according to German law and applicable international treaties	Germany
There is no extra-territorial effect for judicial and or administrative decisions made in Seychelles. Seychelles does not subscribe to criminal jurisdiction based on nationality	Seychelles
No.	Israel
Our national law is in these questions affected mostly by the law of the European Union. That means that we have generally free movement of judicial decisions, which consists of recognition and enforcement of judgements. Another legislative tool is already mentioned European Arrest Warrant.	Slovakia
Our legislation on services of the information society, follows not only the criterion of the place of establishment, but also the so-called "business link" so that providers offering services specifically to Spanish territory shall be subject to Spanish law. In addition, and for the specific case of radicalization leading to the commission of terrorist offences, the PC establishes a rule of jurisdiction and that under Article 575.2 second paragraph in fine, "The activity shall be considered to have been committed in Spain when access is gained to the content from Spanish territory."	Spain
	Sweden

No.	
It depends on bilateral agreements with countries or international treaties and not contradicting with Iraqi regulations and laws.	Iraq
Under section 83.223 of the Criminal Code, "terrorist propaganda" – defined in section 83.222(8) as "any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general — other than an offence under subsection 83.221(1) — or counsels the commission of a terrorism offence" – can be ordered deleted from a computer system pursuant to a judicial order where the material is "stored on and made available to the public through a computer system that is within the court's jurisdiction". As well, "hate propaganda" – defined in subsection 320(8) of the Criminal Code as "any writing, sign or visible representation that advocates or promotes genocide or the communication of which by any person would constitute an offence under section 319" – may also be ordered deleted from a computer system pursuant to a judicial order in the same circumstances.	Canada
The current Broadcasting Act does not give MDA extra-territorial powers. However, MDA's directions to ISPs to block sites are not limited to sites with Singapore domain names.	Singapore
A judicial or administrative decision to delist a domain name will only apply to Norwegian domain names, which means it does not have extraterritorial effect. The second question has no clear answer since Norway only through other criminal offences has criminalized online radicalization. Regarding the third question it depends on the circumstances in the specific case – it's not possible to give a general answer.	Norway
N/A	Belgium
Yes. This is subject to proper registration of such decision or orders in compliance with national laws.	Nigeria
(13) 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?	**STATES**
Denmark complies with obligations, statues and international conventions in regard to the Criminal Code and criminal procedure. E.g. An accused has the right to an attorney; the attorney can have the accused case reviewed by the courts (judicial review) and appeal the case to a higher court. This is to ensure the accused's right to a fair trial.	Denmark
No clearcut answer but perhaps some helpful links: https://cst.org.uk/docs/countering_online_radicalisation1.pdf In the words of Paul Wilkinson: "It is vital to understand that human rights protection is not optional extra in the fight against terrorism; it is an essential weapon or asset in the protection of democracy". See Paul Wilkinson, Terrorism versus Democracy: The Liberal State Response, 2nd ed., (London & New York: Routledge 2006), p. 210. At its core, the policy dilemma is neither new nor unprecedented. Democratic governments must respect and uphold individual rights to freedom of speech and expression even when people's views are distasteful and objectionable. At the same time, if democracy and its freedoms are to survive, governments must protect civil society from political extremists. They must counter ideas and activities that polarise communities, undermine	United Kingdom

the democratic process and lead to violence. The question is: how far can one go in protecting democracy without jeopardising the very liberties one wishes to protect?	
Guaranties figure in: • The Constitution, article 24 "the State protects privacy" • The Law 63/2004 on the protection of personal data • The national institution in charge of protecting personal data	Tunisia
[No answer given by the State].	Albania
[No answer given by the State].	Hungary
Since Indian law has not specifically dealt with radicalization, there are no documented processes and procedures, in the public domain, for investigation and enforcing counter radicalization efforts online. However, lot of work needs to be done in this regard in India.	India
All investigative powers under the Telecommunications (Interception and Access) Act 1979 are subject to strict proportionality tests. To issue a telecommunications interception or stored communications warrant, the independent issuing authority must balance the privacy impact on the individual against the necessity of the information to the investigation. For access to telecommunications data, this test is undertaken by an authorised officer within an agency that makes the authorisation.	Australia
When law enforcement authorities investigate contributions which contain radicalization content they examine carefully whether the contribution or post is in fact of a radicalized nature or if the radicalization content is used in a different way. For example, it may be part of a journalistic article which discusses radicalized content or it may be used as part of a satirical article. In these cases, the activity is either not even an offence under the provisions mentioned at Q1 above or it is covered by freedom of the press or freedom of expression. Even where radicalization content does not fall under the examples mentioned above the law enforcement authorities carry out a thorough analysis as to whether a hateful comment etc. is within the limits of freedom of expression or outside. The assessment depends on all the circumstances of the case, e.g. words, grammar and emoticons used by the author, comments by other users which the author may refer to, etc.	Germany
The process of investigation and prosecution of any offence is strictly subject to the constitutional guarantees and the other laws of Seychelles.	Seychelles
In terms of criminal enforcement, due to potential infringement of human rights, an investigation of related offences can be launched only under the approval of senior officials in the State Attorney's offices. In addition, as mentioned above under question no. 1, indictments over such offences require the approval of the Attorney General.	Israel
Investigating bodies are bind by the Constitution and other statutes, where are stated legal limits of appropriate intervention. In case that there would be any doubts, violated subjects are able to initiate proceedings before the Constitutional court where they can object that their human rights were violated.	Slovakia
Human rights are protected by judicial intervention in order to guarantee the fundamental rights and freedoms when judging and investigating possible crimes. In the particular case of the conduct of radicalization leading to the commission of terrorist offenses (Article 575.2CP) it is required that the prosecutor proves that the access to illicit content is gained in an habitual manner and it is suitable to incite the commission of terrorist offences.	Spain

The fundamental rights and freedoms are protected in the constitution. The constitution also states under which circumstances limitations can be made. Inter alia, limitations can only be imposed to satisfy a purpose acceptable in a democratic society. Generally, the same rules apply online as offline.	Sweden
The Iraqi Constitution of 2005 ensures freedom of speech and freedom of religion and accepting ideologies not contradicting the Constitution and human rights under Iraq's commitment to International declarations of human rights for year 1948 and other international treaties.	Iraq
Canada has a robust constitutional, legislative, and administrative framework to ensure respect for human rights, including freedom of expression, freedom of religion, and right to privacy. This framework ensures that government action and legislation related to counter-radicalization, whether or not in the context of online activities, respects human rights and freedoms. ***Constitutional Protection for Rights and Freedoms*** Rights and freedoms are constitutionally guaranteed in Canada by the Canadian Charter of Rights and Freedoms ("the Charter"). The Charter is Canada's primary vehicle for ensuring that procedures, practices and legislation respect individuals' rights and freedoms. The Charter applies to and places limits on federal, provincial and territorial legislatures and governments to protect and uphold individuals' human rights and fundamental freedoms. It applies to the full range of governmental activities, including administrative practices of officials, acts of the executive branch of government, and enactments of Parliament or the legislatures. Fundamental freedoms are protected under section 2 of the Charter, which provides, in part: "Everyone has the following fundamental freedoms: (a) freedom of conscience and religion; (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication…".; Privacy rights are constitutionally protected through section 8, which guarantees that: "Everyone has the right to be secure against unreasonable search or seizure." The purpose of this right is to protect against unjustified state intrusions on a person's reasonable expectation of privacy. The privacy rights under section 8 extend to reasonable informational privacy interests, including in the context of digital communications and online activities more generally. Section 8 also restricts the sharing of individuals' private information between government officials. Any government action or laws that intrude on Canadians' privacy in relation to counter-radicalization efforts would be subject to section 8. As interpreted by Canada's courts, section 8 of the Charter affords strong privacy protections in Canada, often beyond what is clearly required in international human rights law. ***Statutory Protection for Rights and Freedoms*** Privacy rights are also protected by numerous statutory instruments. The Privacy Act sets out a code of fair practices for the collection, use, disclosure, and retention of personal information held by federal government institutions. The Privacy Act stipulates that collection is to be limited to personal information directly related to operating programs or activities, and must be justified by demonstrable need. It also provides individuals with a right of access to such information and a right to correction of their personal information. More than 250 Government institutions are subject to the Act. At the sub-national level, every Canadian province and territory has public privacy legislation, which governs the collection, use and disclosure of personal information held by government agencies. Part VI of the Criminal Code is one of Canada's primary means for regulating electronic surveillance. Part VI has two main objectives: to protect private communications by prohibiting their interception, and to specify the conditions in which an interception of a private communication may be authorized. At the heart of Part VI are the general prohibitions against willfully intercepting private communications, and against using or disclosing such communications. Subject to certain exceptions, these prohibitions bar third parties (including the police	Canada

and other state actors) from intercepting private communications such as telephone conversations or emails. The key exceptions to the general prohibition on interception are when prior judicial authorization is granted on the basis of a legislative provision, or when one of the parties to the communication is consenting to the interception. These measures supplement existing legal protections to ensure that any counter-radicalization efforts by the government and security agencies are conducted in a manner that upholds and respect human rights.

Oversight Mechanisms and Remedies for Violations of Rights and Freedoms

The Charter

The Constitution grants Canada's independent and impartial judiciary effective powers to remedy Charter violations. An individual who believes his or her rights have been infringed by a counter-radicalization or terrorism investigation or prosecution can pursue legal proceedings. Where a government action is found to unjustifiably violate the Charter, courts can order an appropriate and just remedy, including an injunction, an order of compensatory damages, or the exclusion of unconstitutionally-obtained evidence from a court proceeding (section 24 of the Charter).

In addition, legislation that is inconsistent with the Charter is, to the extent of the inconsistency, of no force or effect (section 52 of the Constitution Act, 1982). For example, in R. v. Khawaja, the individual was convicted of various terrorism offences. He challenged his conviction by claiming that the Criminal Code definition of "terrorist activity" was contrary to the Charter right of freedom of expression. His claim was rejected by the Supreme Court of Canada in December 2012.

There are also non-judicial complaint mechanisms that help to ensure that allegations of wrong-doing are investigated and, where complaints are upheld, remedied. In addition to the mechanisms described in more detail below, this includes Parliamentary committees, public inquiries, and independent civilian police review mechanisms.

Privacy Commissioner

The federal Office of the Privacy Commissioner is responsible for overseeing compliance of the Privacy Act. The Privacy Commissioner is independent of government, and reports directly to the House of Commons and the Senate. The Commissioner's powers include: investigating complaints, conducting audits, and pursuing court action; publicly reporting on the personal information-handling practices of public and private sector organizations; supporting, undertaking, and publishing research into privacy issues; and promoting public awareness and understanding of privacy issues. At the sub-national level, provincial and territorial oversight is provided through either an independent commissioner or ombudsman authorized to receive and investigate complaints.

Canada's National Security Organizations

Canadian national security organizations conduct their activities according to their legal mandates, with ministerial direction and judicial oversight as appropriate. Each is subject to the scrutiny of the Privacy Commissioner, the Information Commissioner and the Auditor General. In addition, there are independent bodies that scrutinize the activities of certain government agencies.

With respect to the Communications Security Establishment (CSE), Canada's cryptologic agency, all of their activities fully respect the legal parameters and authorities under which they operate in order to protect the privacy of Canadians. Under the National Defence Act, CSE is prohibited from directing its foreign intelligence or information technology security activities at Canadians anywhere in the world or anyone in Canada. The CSE Commissioner, independent of Government and of CSE, pursuant to the Commissioner's legislative mandate, provides a robust review of the activities of CSE to ensure they are in compliance with the law and protects privacy. The CSE Commissioner also has the duty to hear public complaints and has all the powers of a Commissioner under Part II of the Inquires Act, including the power to summon witnesses to give evidence under oath. The CSE Commissioner is required by law to inform the Minister of National Defence and the Attorney General of Canada of any action by CSE which the Commissioner believes may not comply with the law, including the Charter, the National Defence Act, the Privacy Act and the Criminal Code. The Commissioner has never identified any actions of the CSE as being unlawful. The Commissioner's annual

reports to the Minister of National Defence and to Parliament can be found at https://www.ocsec-bccst.gc.ca/s21/s20/eng/2014-2015-annual-report. With respect to the Canadian Security Intelligence Service (CSIS), their activities are conducted according to their legal mandate, under the CSIS Act with ministerial direction and judicial oversight, as appropriate. Moreover, judicial scrutiny is provided via a regime for the issuance of warrants by the Federal Court of Canada. CSIS is also subject to full and independent review by the Security Intelligence Review Committee (SIRC). SIRC is an independent, external review body which reports to the Parliament of Canada on the operations of CSIS to ensure that the powers given to CSIS are used legally and appropriately. SIRC is also mandated by law to report annually to the Minister of Public Safety and Emergency Preparedness who then presents the report to the Parliament of Canada. (SIRC Annual Report for 2013-2014 can be found at https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2013-2014/2013-2014_Public_Report_Inside_ENG.pdf). With respect to the Royal Canadian Mounted Police (RCMP), their powers of interception are governed by Part VI of the Criminal Code, which sets out the procedures to obtain judicial authorization to conduct electronic surveillance of private communications for criminal investigations. These procedures are to be carried out to ensure that the privacy of individuals is appropriately respected during the surveillance. As an additional measure of accountability, section 195 of the Criminal Code requires the Minister of Public Safety and Emergency Preparedness to prepare and present to Parliament an annual report on the use of electronic surveillance under Part VI for offences that may be prosecuted by or on behalf of the Attorney General of Canada. (The latest report available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2013/lctrnc-srvllnc-2013-eng.pdf). Furthermore, enacted in 2013, the Enhancing Royal Canadian Mounted Police Accountability Act bolstered the review of the RCMP through the Civilian Review and Complaints Commission for the RCMP, allowing greater access to RCMP information, enhanced investigative powers, and the ability to undertake policy reviews.	
Fundamental rights such as freedom of speech and religious belief are entrenched in the Constitution of the Republic of Singapore. In creating a framework for individuals to freely exercise these rights, the Singapore Government has an important role - to be vigilant and ensure that Singapore and Singaporeans remain united. The Government has to impose limits to address the competing tension between the exercise of these rights and the interest of maintaining religious harmony in a diverse community. For example, freedom of speech in Singapore does not extend to permitting the burning of religious texts. Nor does it permit denigration of any religion. The Government's policies are designed to ensure equality of opportunities, fairness and a fair stake for all in Singapore. Institutional safeguards are also in place. The most fundamental safeguard is that fundamental liberties, such as the right to life and personal liberty, freedom of speech, assembly and association, and freedom of religion, are protected by Singapore's Constitution and upheld by the Singapore judiciary as the guardians of the Constitution. Notably, Singapore was ranked 3rd globally for Criminal Justice by the World Justice Project Rule of Law Index in 2015. Under the Internal Security Act (ISA), Singapore's key legislation in the fight against terrorism, strict checks and balances are built into the ISA to safeguard the rights of the detainee. The detainee will be informed of the grounds of his detention and the allegations of fact on which his Order of Detention (OD) is based, within 14 days of the OD. He has the right to make his representations against his OD to an independent Advisory Board (AB). The AB comprises a Supreme Court judge and two citizens appointed by the President in consultation with the Chief Justice, under the Constitution of Singapore. The detainee has the right to engage a legal counsel of his choice to make representations before the AB. The Elected President also serves as a check, and where the Government (i.e. the Cabinet, on Minister's recommendation) proposes to further detain a person contrary to the AB's recommendation, the President can exercise his veto power. Detainees' rights are also listed in Rules made pursuant to the ISA.	Singapore
Norway is legally bound by human rights conventions such as the United Nations International Covenant on Civil and Political Rights and the European Convention on Human Rights. These conventions are implemented in Norwegian law. Recently, a number of human rights, including the right to privacy, have also been implemented in the Norwegian Constitution. The protection of human rights is monitored, inter alia, by the courts and by national and international supervisory mechanisms.	Norway

*Additional information regarding the survey: Norwegian law enforcement enjoys a high level of trust in the Norwegian population; trust that has been built throughout the years. Norwegian law enforcement has implemented a model or approach that relies on assistance from the public when it comes to discovering persons that might enter into or already be in a radicalization process through online tools such as social media platforms. We believe that this enhances the trust law enforcement has in the public. Thus, the National Criminal Investigation Service (NCIS), one of the law enforcement agencies that work online, focus on preventing, rather than countering per se; which we consider to be a more "aggressive" approach. Additionally, the NCIS does not wish to decide what opinions the Norwegian public is allowed to have; rather, the NCIS wants to ensure freedom of speech by relying on a somewhat more liberal approach. That is not to say that rebukes are inefficient, but it is a task for other agencies and communities in the Norwegian society, such as civic organizations and religious communities.	
Belgium is very committed to freedom of religion, public worship and the freedom of opinion, enshrined in Articles 19 et 25 of the Constitution. This freedom is necessary for the well-functioning of a democratic society. It is also established in Articles 9 et 10 of the European Convention on the Safeguard of Human Rights. The prohibition of incitement to hatred or violence constitutes a legal restriction to freedom of speech permitted by Article 10 § 2 of the Convention. In Belgium, the legal basis for the tackling of the incitement to hatred or violence is founded in 3 federal laws: 1. The antiracism Act of 30 July 1981 (amended by the Law of 10 May 2007) punished, in its Article 20: "whoever, in any of the circumstances described at Article 444 of the Criminal Code, incites to hatred or violence against a person, group, community or its members on the grounds of one the protected criterion, i.e. nationality, alleged race, skin color, ascendance or national origin or ethnicity, even outside of the fields mentioned in Article 5." 2. The antidiscrimination Act of 10 May 2007 completes the antiracism Act by prohibiting the following criteria of discrimination: age, sexual orientation, civil status, birth, fortune, religious or philosophical conviction, union, language, present or future health state, disability, physical or genetic characteristic or social origin (Article 3). Article 22 prohibits attitudes of incitement to hatred, violence or discrimination. 3. The "gender" Act (10 May 2007) of which Article 27 punished acts of incitement to hatred, violence or discrimination committed against a person on basis of its gender (plus identity or gender expression, added in 2014). These laws cover acts committed under multiple public forms (meaning in the presence or, or directed towards two or more persons), including offences committed by means of computer systems. Considering the increasing importance of digital economy and of the digital world and of the presence of social media in our day-to-day lives, the Belgian government has designated a Secretary of State responsible for the protection of privacy. The government's policy, including in the security field, gives a particular attention to the right to privacy established in Article 22 of the Constitution and in the Law of 8 December 1992 on the protection of privacy towards the processing of personal data. An independent and external supervision is also conducted. Legislative projects that have consequences on the respect of the right to privacy and notably the protection of data are submitted to the Commission on the protection of privacy for advice. In general, this Commission is mandated to monitor the respect of the right to privacy and controls the way a person or an authority uses personal data.	Belgium
The Constitution guarantees that human rights are complied with: Article 25. of the Constitution provides that "Despite any other provision in this Constitution, the following rights and fundamental freedoms shall not be limited– (a) freedom from torture and cruel, inhuman or degrading treatment or punishment; (b) freedom from slavery or servitude; (c) the right to a fair trial; and (d) the right to an order of habeas corpus."	Kenya

The 'principle of proportionality' in investigation is one of the basic principles regulating the methods of investigation and protecting the rights of the suspect and the third party. Another important principle is the 'requirement of warrant'. Art. 35 of the Japanese Constitution provides that "[t]he right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by art. 33. Each search or seizure shall be made upon separate warrant issued by a competent judicial officer." The third principle, stipulated in art. 197 of the Codes of Criminal Procedure, prohibits compulsory dispositions unless special provisions have been established in the Code even if such examination as is necessary to achieve its objective may be conducted. http://www.penal.org/sites/default/files/files/RH-10.pdf	Japan
Brazil's Marco Civil Bill protects the right to free expression online and guarantees network neutrality. However, the Brazilian Constitution explicitly forbids anonymity, which can restrict freedom of speech.	Brazil
Poland is Party to the European Convention on Human Rights which guarantees that Human Rights are not violated However, concerns have been made by organizations regarding the new Anti-Terrorism Law and its impact of freedom of expression especially given the lack of prior judicial intervention in the blocking of content by the Internal Security Agency.	Poland
According to the White House: "It is important that we continue to protect civil liberties and privacy as we implement an Internet safety approach and that we do not restrict speech. Our focus is on providing communities with information for staying safe online from individuals who are trying to encourage others to commit acts of violence. Our concern with protecting civil liberties and privacy informed the development of our policy and will guide the efforts of the Working Group." https://www.whitehouse.gov/sites/default/files/docs/fact_sheet-countering_online_radicalization_-_final1.pdf	United states of America
In its "National Plan to Address Cybercrime" from 2015, the Government stated that "a key part of the New Zealand's government's approach to cyber security policy is to support the creativity, freedom, openness and dynamism that has made the Internet what it is today. New Zealanders should be able to engage online without suffering harm or unlawful interference."	New Zealand
France is Party to the European Convention on Human Rights which guarantees that Human Rights are not violated. Moreover, the universal principles of the right to a due process and fair trial are established in the French Constitution of 1958.	France
According to Freedom House's report for the year 2015, "Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Russia remains a member of the Council of Europe and a party to the European Convention on Human Rights and Fundamental Freedoms, Article 10 of which enshrines the right to freedom of expression. However, over the past few years Russia has adopted a set of laws and other acts that, coupled with repressive law enforcement and judicial systems, have eroded freedom of expression in practice. Courts tend to side with the executive authorities, refusing to apply provisions of the constitution and international treaties that protect the basic rights of journalists and internet users." https://freedomhouse.org/report/freedom-net/2015/russia	Russia

The judicial and justice system of Nigeria allows the protection of Fundamental Human Rights in a Court of Competent Jurisdiction where such rights are violated or about to be violated.	Nigeria