18 March 2016

Input on human rights and preventing and countering violent extremism

Introduction

European Digital Rights (EDRi) is an umbrella organisation that represents civil rights organisations from 19 European countries in the European Union.

EDRi welcomes the UN High Commissioner on Human Right's efforts to map the interaction between human rights and counter-extremism measures in his forthcoming report, and his preparedness to receive input from civil society.

On 4th February 2016, EDRi joined efforts with other civil society organisations by co-signing a joint submission to the UN Human Rights Council[1] and sent an open letter[2] as input to your public consultation on this topic. In this separate submission, EDRi would like to share more specific experiences in this area, which relate primarily to counter-extremism in the European digital environment.

While EDRi obviously acknowledges the importance of fighting terrorism and violent extremism, we are concerned by the disproportionate and misguided responses by certain UN countries in pursuit of this aim.

First, we outline our approach regarding the terms 'extremism' and 'terrorism' for the purpose of this response, and the problems inherent in over-reliance on these terms.

Secondly, this contribution identifies some of the risks for the human right to privacy and the fundamental right to data protection and freedom of expression.

Thirdly, we describe the worrying 'privatisation' of counter-extremist law enforcement, shifting from government authorities to online companies and undermining human rights safeguards and the rule of law.

Finally, EDRi makes a set of recommendations regarding the adoption of best practices, in line with those of Article 19, that is one of our member organisation.

1 https://www.article19.org/data/files/Joint_Written_Submission_PVE_HRC31.pdf
2 https://www.article19.org/data/files/Joint_Letter_to_High_Commissioner_PVE.pdf

18 March 2016

On 'extremism' and 'terrorism'

As mentioned in our joint letter and joint submission, the terms 'violent extremism' and 'counter-extremism' lack clear, uniform definitions. What makes the recent focus on 'violent extremism' particularly troubling, is that this concept is even *broader* than that of terrorism, as acknowledged by the Secretary General in its Plan of Action to Prevent Violent Extremism:

> *'Violent extremism encompasses a wider category of manifestations [than terrorism] and there is a risk that a conflation of the two terms may lead to the justification of an overly broad application of counter-terrorism measures, including against forms of conduct that should not qualify as terrorist acts'. Accordingly, the threat to legal certainty and foreseeability might be even greater than we already have seen with the notion of 'terrorism'.*

As the concept of counter-extremism appears to subsume that of counter-terrorism, we will include counter-terrorist measures in our analysis of potential threats to fundamental rights below. We consider these examples relevant since we fear that the measures which have previously been advocated for under the frame of counter-terrorism, might potentially also be advocated for under the broader frame of counter-extremism.

Privacy and data protection

In response to terrorism and violent extremism, European states have introduced surveillance powers of an unprecedented scope. Regrettably, these measures often involve untargeted, indiscriminate forms of surveillance which affect the entire population and can therefore create disproportionate restrictions on the rights to privacy and data protection. Furthermore, there is little or no evidence to confirm that these measures are in any way effective, let alone efficient, in fighting terrorism and violent extremism.

Perhaps the most extreme example of disproportionate mass surveillance at the European Union level was the Data Retention Directive introduced in 2006, which forced telecommunications operators throughout Europe to retain all communications data for a minimum of 6 months and up to 24 months.[3] This instrument remained in force for almost 6 years, until the Court of Justice of the European Union (CJEU) invalidated the Directive for breaching the fundamental rights to privacy and data protection.[4] In these six years of indiscriminate mass surveillance, affecting almost every citizen in Europe, this measure did not contribute to any documented examples of prevention or prosecuting terrorism or violent extremism. Nevertheless, despite the significant negative impact on the right to privacy - as clearly confirmed in the CJEU's ruling - and despite the lack of demonstrable results, many European national governments have continued to require

3 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

4 Case C-293/12, *Digital Rights Ireland* Court of Justice of the European Union 2014, ECLI:EU:C:2014:238.

untargeted data retention[5], and in some have even introduced new proposals to this end.[6] EDRi has serious concerns regarding the compatibility of these measures with human rights.

Another troubling legislative development at European level is the proposed Passenger Name Record Directive, which, if adopted, would force airline companies to retain detailed accounts of their passengers' travel behaviour for access by law enforcement authorities for five years.[7] First proposed by the European Commission in 2011, this dossier was initially rejected by the European Parliament's Civil Liberties Committee for disproportionately affecting the right to privacy. Nevertheless, an updated proposal is now being pushed through the legislative process, although EDRi expects that - as a form of untargeted mass surveillance - this law is likely to be invalidated if challenged before the CJEU.[8] The EU also has bilateral arrangements with the US (15 years of data storage) and Australia (5 and a half years of data storage),

At national level, counter-terrorist legislation in Europe has been so extensive over the past decade that we cannot give a comprehensive overview in this submission. Repeatedly, courts have determined such measures to be in violation of human rights. For example, in 2016, the European Court of Human Rights in *Vissy v. Hungary* determined that the Hungarian surveillance powers introduced in their revised Police Act of 2010 were in breach the fundamental right to privacy.[9] In the same year, the London Court of Appeal ruled the UK Terrorism Act to be incompatible with the European Convention on Human Rights (ECHR).[10] However, many more laws have so far gone unchallenged. Counter-terrorism laws from various Member States. such as France and Spain, as well as recent proposals from states such as the Netherlands, have been subject to severe criticism from civil society for their interference with human rights.[11]

---

5 E.g., Sweden, the United Kingdom.

6 E.g. Germany, Belgium. See also: EDRi, 'Data retention: German government tries again'. (03.06.2015) https://edri.org/data-retention-german-government-tries-again/ http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf

7 Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

8 For more information: EDRi, 'FAQ: Passenger Name Record' (09.12.2015) https://edri.org/faq-pnr/

9 *Case of Szabo and Vissy v.* Hungary, app. no. 37138/14, ECHR 2016.

10 Terrorism Act incompatible with human rights, court rules in David Miranda case', *The Guardian* (19.01.2016) http://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case

11 Amnesty, 'Spain: new counter-terrorism proposal would infringe basic human rights'. (10.02.2015) https://www.amnesty.org/en/latest/news/2015/02/spain-new-counter-terrorism-proposals-would-infringe-basic-human-rights/+&cd=1&hl=en&ct=clnk&gl=be
Human Rights Watch, 'France: New Emergency Powers Threaten Rights' (24.11.2015) https://www.hrw.org/news/2015/11/24/france-new-emergency-powers-threaten-rights
EDRi, 'Dutch Minister reveals plans for dragnet surveillance' (15.07.2015) https://edri.org/dutch-minister-reveals-plans-for-dragnet-surveillance/

Another misguided and damaging effort intended to combat terrorism has been the move by states in Europe and abroad to undermine encryption technologies. Encryption technologies allow digital communications to be conducted in a secure and confidential manner, and are therefore crucial for all citizens and industries and for the activities of journalists, lawyers and whistleblowers.[12] However, governments including those of France and the United Kingdom have suggested banning strong encryption out of fear that terrorists might use it.[13] In addition, various intelligence agencies including the US NSA and the UK GCHQ have attempted to create 'backdoors' which can potentially also be exploited by third parties.[14] These measures were claimed to be justified on the basis that terrorists might use encryption to evade surveillance. Yet again, however, these claims lack evidential basis. On the contrary, the available evidence indicates, for example, that the Paris attackers of November 2015 didn't use encrypted communications.[15] Governments' quixotic push against encryption is yet another example of the extreme, misguided measures which counter-terrorism has inspired.

Freedom of Expression

In various European anti-terrorist measures, EDRi also identifies grave threats to the freedom of expression. The most extreme examples come from France, where the government has criminalised 'terrorist apologia'.[16] The satirist comedian Dieudonné M'bala M'bala received a two-month sentence under this law for a statement on Facebook. Since the Charlie Hebdo attacks, over 257 similar investigations have been opened into speech which allegedly condones or glorifies terrorism, leading to at least 18 prison sentences.[17] In addition to criminalising speech acts under the broad and ill-defined remit of 'terrorist apologia', France has also introduced powers to block such messages via Internet Service Providers. Under their 'state of emergency' powers, France's Minister of the Interior can order websites to be blocked instantly for 'promoting terrorism or inciting terrorist acts'.[18]

---

12 For more information, please consult EDRi's position paper on encryption: https://www.edri.org/files/20160125-edri-crypto-position-paper.pdf

13 'France mulls encryption backdoors', *The Register* (16.01.2016). http://www.theregister.co.uk/2016/01/12/new_french_law_to_require_backdoors/
'David Cameron pledges anti-terror law for internet after Paris attacks', *The Guardian* (12.01.2015). www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg

14 'NSA director defends plan to maintain 'backdoors' into technology companies' *The Guardian* (23.02.2015) http://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies
'GCHQ-developed phone security 'open to surveillance' *BBC* (23.01.2016) http://www.bbc.com/news/technology-35372545

15 'Signs Point to Unencrypted Communications Between Terror Suspects', *The Intercept* (18.11.2015) https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects/

16 Art. 421-2-5, Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

17 'French dissenters jailed after crackdown on speech that glorifies terrorism', *The Guardian* (30.01.2015) http://www.theguardian.com/world/2015/jan/30/french-jailed-crackdown-speech-glorifies-terrorism

18 La Quadrature du Net, 'A Police State to Avoid Any Critical Evaluation?'

It should be noted that the harmful consequences of blocking measures and (threats of) criminal prosecution go beyond those targeted directly. By punishing and stigmatising certain forms of expression, these measures also lead to self-censorship by others - a phenomenon also known as the 'chilling effect'. As 'terrorism' and especially 'violent extremism' are such broad concepts, the risk of self-censorship is particularly high, since citizens may find it difficult to foresee the limits of what authorities deems acceptable. Therefore, the free speech impact of certain anti-terrorist measures, even those which do not amount to direct punishment or prohibition, should not be underestimated. For instance, the Dutch police has been directly and without prior caution visiting the homes of perceived extremist Twitter uses to discuss their online behaviour.[19] This method does not involve any direct censorship but can nevertheless chill speech and make users feel less free to voice their true opinions online. We also recall the case of David Miranda, who, while carrying sensitive, confidential information provided by whistleblower Edward Snowden, was detained for over eight hours by UK law enforcement under the UK Terrorism Act.[20] This case is not merely an incident but part of a larger trend: other high-profile whistleblowers including Julien Assange and Edward Snowden have also been described as terrorists by senior government officials.[21] As these case shows, allegations of terrorism can be, and have been, misdirected at those pursuing a legitimate public interest. Such allegations, and the harsh treatment which they can trigger, can obstruct legitimate forms of expression. Moreover, these accusations are highly stigmatising and intimidating, and can potentially discourage future acts of expression.

Privatised enforcement

The above has focused on direct state interventions affecting the rights to privacy, data protection and free speech. However, anti-terrorist measures are increasingly carried out by private companies rather than public authorities, especially in the digital environment. For example, the blocking of online hate speech is increasingly achieved not through binding orders from law enforcement agencies, but rather through 'voluntary' measures decided on by Internet service providers and online intermediaries such as Facebook, Google and Twitter. Government officials throughout the EU have exercised pressure over intermediaries including social media platforms to "do more". At the World Economic Forum of 2015, President François Hollande said:

> *"The big operators, and we know who they are, can no longer close their eyes if they are considered accomplices of what they host. We must act at the European and international level to define a legal framework so that Internet platforms which manage social media be considered responsible, and that sanctions can be taken."*

---

https://www.laquadrature.net/en/police-state-in-france

19 'U twittert wel heel veel, zei de politie', *NRC* (20.01.2016) http://www.nrc.nl/next/2016/01/20/u-twittert-wel-heel-veel-zei-de-politie-1578392

20 'Terrorism Act incompatible with human rights, court rules in David Miranda case', *The Guardian* (19.01.2016) http://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case

21 'Biden makes the case for Assange as a high-tech terrorist', *Huffington Post* (19.12.2010). http://www.huffingtonpost.com/2010/12/19/joe-biden-wikileaks-assange-high-tech-terrorist_n_798838.html
'George Pataki calls for Twitter to ban Edward Snowden', *CNN* (09.30.2015) http://edition.cnn.com/2015/09/29/politics/george-pataki-edward-snowden-twitter/

In the same year, the EU Ministers of Interior issued a joint statement stating that *"the partnership of the major Internet providers is essential to create the conditions of a swift reporting of material that aims to incite hatred and terror and the condition of its removing, where appropriate/possible*."

Through declarations such as these, political pressure has steadily been piling onto intermediaries to monitor and prevent (often misperceived) threats of terrorism and (undefined) extremism in their online communities with no due process and outside the rule of law.

The move towards 'privatised enforcement' threatens freedom of expression and the rule of law. After all, online intermediaries can and do remove content on the basis of their Terms of Service and Community Guidelines, which generally to go further than the law would require and do so in a way which is far less predictable. Simply put, they frequently censor content which is legal. Since these intermediaries are private companies, they do so without the levels of predictability, transparency and due process. While a law prohibiting terrorist apologia might be challenged before constitutional courts in light of requirements such as necessity and proportionality, online services are free to ban such content at their own discretion.[22] In terms of predictability, terms of service frequently include broad, ambiguous removal grounds.[23] In terms of transparency, although most intermediaries tend to publish general (but incomplete) statistics on content censorship, they rarely publish information regarding individual removal decisions. In short, since private intermediaries are not subject to the same standard and human rights obligations as government authorities and since their decisions have no democratic legitimacy, their increased involvement in the regulation of online discourse can result in unnecessary or arbitrary censorship, thereby jeopardising the right to freedom of expression and the rule of law. In addition, companies do not have an incentive to solve public interest issues. It is dangerous to leave public interest issues to companies.

European authorities have been keen to exploit the unaccountable removal powers of online intermediaries. Europol recently launched an 'Internet Referral Unit (IRU)' which refers terrorist and extremist content to online platforms so that they might remove it. Member States have also been called upon to establish such bodies at national level, such as the UK's Counter-Terrorism Internet Referral Unit (CTIRU). The authorities in charge have consistently emphasised that content removal is to be decided on and carried out *voluntarily* by intermediaries themselves, based on their own Terms of Service.[24] In the words of the EU's anti-terrorism coordinator Gilles de Kerchove: ' Member States should consider establishing similar units to the UK CTIRU and replicate relationships with the main social media companies to refer terrorist and extremist content which breaches the platforms' own terms and conditions (and not necessarily national

22 'Facebook revamps its takedown guidelines', *BBC* (16.03.2015) http://www.bbc.com/news/technology-31890521

23 UNESCO, 'Fostering Freedom Online: The Role of Internet Intermediaries' (19.01.2015(http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

24 This however, raises counterproductive effects: http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/white-paper-the-role-of-prevent-in-countering-online-extremism.pdf

legislation)'.[25] These public-private collaborations allow states to regulate and stifle online speech indirectly, while deferring responsibility for the outcomes to unaccountable private corporations. Thus, the methods currently being adopted to take down extremist content online in Europe - an aim which has not necessarily been proven an effective method of combating such movements and has however counterproductive effects[26] - are undermining the rule of law and jeopardises our freedom of expression.

Recommendations

In light of the above and EDRi's previous contributions, EDRi fully endorses the recommendations made by our member Article 19, i.e.:

"to proactively seek the input of civil society to the report as a primary stakeholder;
to explore the various meanings given to "violent extremism" and related concepts, and the potential impact of ambiguity in this area on the promotion and protection of human rights, drawing upon lessons learned through parallel Human Rights Council initiatives on promoting and protecting human rights while countering terrorism.[27]

For more information or clarification, please contact

Joe McNamee (joe.mcnamee@edri.org) **and**

Maryant Fernández (maryant.fernandez-perez@edri.org)

Tel. +32 22742570

25 DS 1035/15, EU Counter-terrorism Coordinator input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, Council of the European Union 17 January 2015. Available online at: http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf

26 Hussain, G. and Saltman, E.M., Jihad Trending. A Comprehensive Analysis of Online Extremism and How to Counter it, Quilliam Foundation, available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf

27 https://www.article19.org/resources.php/resource/38133/en/un-hrc:-resolution-on-%E2%80%9Cviolent-extremism%E2%80%9D-undermines-clarity (08.10.2016)