Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Opinion No. 2014-3
on Article 9 of the bill on scaling up counter-terrorism provisions

French Digital Council

15 July 2014

CNNum
Conseil National du Numérique

Foreword

The French Digital Council has been given a mandate to examine Article 9 of the bill on scaling up counter-terrorism provisions. These provisions amend Article 6 of the Act of 21 June 2004 on confidence in the digital economy (LCEN) by providing for the administration to block websites containing speech and/or images constituting incitement to terrorism or in defence of terrorism. They also extend the scope of the notification tools that technical service providers are bound to use.

The French Digital Council has held fifteen interviews with terrorism experts (sociologists, journalists and association representatives), specialised lawyers and judges, civil society representatives, intelligence agency members and digital professionals (full list available in the appendix) to be able to deliver as fully informed an opinion as possible.

The provisions submitted for the Council's appraisal come at a time when a growing number of French nationals are leaving France for Syria – the conflict in Syria is unprecedented in its power of attraction, especially to young people.

The proposed measure is part of the government plan to scale up anti-terrorist legislation. It is designed to counter the recruitment of terrorists by providing for the possibility for the administrative authorities to directly block access to certain websites and content.

This proposal comes in response to a real situation: a large volume of content circulating on the Internet in the form of text, videos, pictures and sound recordings presents acts of terrorism and victims of conflicts with the aim of arousing Internet users' support and empathy. The more motivated of these Internet users are then directed to a smaller number of recruitment websites where they are picked out to join terrorist theatres of operations. Some return with the intention of committing acts in France. These two phases – content dissemination and recruitment – cannot be treated as if they were one.

The French Digital Council has already given its opinion on related subjects.[1] Although it is not against blocking or filtering content when such content is illegal, it has recommended, in these cases, always observing the principle of applying to a judicial authority before setting up an Internet content surveillance, filtering or blocking mechanism. The proposed measure intends, for reasons of effectiveness, to override this principle of advance legal oversight by taking steps upstream of the recruitment of candidates to prevent them from accessing propaganda content and recruitment websites. It makes no distinction between effectiveness in countering terrorist recruitment and the communication of terrorist propaganda. Yet these two aspects call for different kinds of responses.

The explanations the Council has obtained regarding the bill state that the proposed measure is designed more especially to give the administration the means to take urgent action when content and websites go viral, whereas a court ruling is currently required to block each replication of content.

However, other interviews pointed up the need for a distinction between recruitment and activation and also the fact that the attraction processes are slow and gradual. Targets generally go through many phases of indoctrination and integration before being encouraged to commit a terrorist act or join a group. A number of counter-terrorism professionals believe these recruitment websites to be few and far between and that the decision to block them should be weighed against what can be gained from their surveillance.

[1] See Opinion No. 2013-4 on the bill strengthening the fight against the system of prostitution (http://www.cnnumerique.fr/avis-prostitution/), Opinion No. 2013-6 of 17 December 2013 on illegal online content and behaviour (http://www.cnnumerique.fr/contenus-illicites/) and Opinion No. 2013-5 of 6 December 2013 on digital freedoms (http://www.cnnumerique.fr/libertes-numeriques/).

Lastly, content is highly diverse and complex by nature. It calls for careful supervision and assessments to determine what constitutes incitement to terrorism and what constitutes opinion. It is mainly disseminated during the sensitisation phases that precede recruitment. It is exchanged far from the hub of activist communities, not on websites as such, but on platforms and in forums where legal content appears alongside illegal content. If a blocking mechanism is to be effective, it has to be able to analyse the very content of these personal exchanges in fine detail. Such in-depth inspection techniques would constitute not only censorship, but an invasion of privacy and violation of the freedom of thought. As such, they would be unacceptable.

The Council is of the opinion that:

1. The proposed blocking mechanism is technically inefficient

- Recruiters and Internet users alike can easily circumvent Internet service provider blocking mechanisms, because they cannot delete content at source.[2]

- The proposed measure could prompt terrorist networks to increase the complexity of their underground techniques by adding further layers of encryption and moving to less visible areas of the Internet, which would make the investigators' job that much harder. Some of these techniques are very easy to use and the recruiters' target age brackets are already adept at them, being familiar as they are with the use of virtual private networks (VPNs), Peer-to-Peer (P2P) and Tor.

- The proposed measure could be counterproductive in terms of image and education. The ease with which it can be circumvented could give the impression that the authorities are lagging behind in the technological war, hence creating a feeling of pride and impunity.

- As shown by the report by French MPs Corinne Erhel and Laure de la Raudière, access blocking measures currently present overblocking and underblocking risks. The failed experiments in countries such as the United Kingdom,[3] the United States[4] and Australia confirm this risk. Given that one and the same server can host other perfectly legal websites and content, collaterally blocking them constitutes a direct violation of the freedom of expression and communication. The only solution would be to directly and massively inspect the content of Internet users' communications.[5] This would raise serious privacy and freedom of thought risks.

[2] Many techniques are available to get round Internet filtering: proxy servers, tunnel filter breakers, hosting change or rotation of URLs, Botnets, change of DNS, etc.

[3] In the United Kingdom, where Internet service providers now apply default filtering at the government's request, nearly 20% of the most popular websites are blocked by at least one telecommunications operators. Only 4% of these websites are pornographic.

[4] In the United States, the blocking of ten child pornography websites by the American authorities caused the blocking of 84,000 legal websites sharing the same DNS provider.

[5] Operators block solely at domain name (DNS) level or sometimes at sub-domain level. More finely targeted blocking (especially by URL) would call for more advanced technological developments and the use of deep packet inspection (DPI) techniques, which especially violate privacy of correspondence.

2. The proposed measure is unsuited to the challenges of countering terrorist recruitment

- ***The principle of obtaining advance court authorisation remains vital:***

    - The Council's consultations found that the number of recruitment websites is estimated by the experts to be between ten and one hundred. These figures suggest that there is no reason to believe that the courts will be overloaded, as is sometimes mentioned, and that there is no reason to create a special mechanism to bypass the court to go straight to the administrative authority.

    - The proposed mechanism bears a considerable risk of concertinaing between administrative authorities and courts. For example, the administration's untimely closure of a site or content could alert terrorists to the fact that they are subject to legal surveillance.

    - The proposed measure disregards the negative returns on and risks raised by similar experiences in other countries, especially with respect to counter-terrorism action in the United States, Edward Snowden's revelations on the subject and the risk of the loss of consumer confidence in the digital ecosystem.

- ***Blocking mechanisms are no answer to competition for the attention of and influence over population groups targeted by terrorist channels, especially young people:***

    - It is unrealistic to address the image and content propagation dynamics specific to the Internet and social networks with measures that can be technically circumvented. The only scenario in which the mechanism might be effective would be in the case of a massive, automated application, which would be in blatant breach of the principles of the rule of law.

    - Blocking could be counterproductive to action to prevent strategies spreading radical ideologies in that it might fuel interest in viewing the blocked content.

Recommendation – The stakeholders consulted point to the need to develop research to improve our understanding of the social aspect of radicalisation and to define precisely the Internet's role in this process. There may be many factors involved in individuals' decisions to take the path of violence, which may have nothing to do with direct incitement to terrorism or the defence of terrorism. Contact with extremist ideologies can occur both online and offline. More research will be needed on these subjects to inform any future decisions.

Recommendation – With respect to prevention, the same experts point out the particular importance of education and capacity building to be able to interpret the different messages – online and offline – with a critical eye.

3. The proposed measure does not provide sufficient guarantees in terms of freedoms

- In a move to keep the courts involved in the process, the proposed measure provides for the Minister of Justice to appoint a "magistrate" to check that the list of websites and content accessible to the general public is drawn up, updated, communicated and used in a lawful manner.

- These measures are inadequate for two reasons:

  - The magistrate is not tasked with checking the advisability of the blocking operation itself;
  - Being appointed by the government, this magistrate does not benefit from the guarantees of independence provided by the judicial process.

- The Constitutional Council has ruled that blocking a website constitutes a serious breach of the freedom of expression and communication.[6] Any violation of freedoms, irrespective of whether it is justified by national security considerations, must be commensurate with and necessary for the objective sought. Yet the proposed mechanism introduces an extraordinary administrative blocking procedure without this being justified by conditions such as an imminent emergency or the absence of any other possible solution.

- Unlike the child pornography provisions, the Council's consultations found that determining notions of acts of terrorism and defence of terrorism is open to subjective interpretation and bears a real risk of ending up as a mere offence for holding certain views.

Recommendation – Growth in the use of extraordinary measures to isolate the digital sphere is undermining legislative cohesion. The Council hence recommends introducing a moratorium on all plans for provisions to introduce blocking or filtering measures on the Internet. The trade-off between the imperatives of security and freedom should be made with care in an environment free of the pressures of current events.

The proliferation of these measures since 2004 calls for **a review and an analysis of their effectiveness**. On this subject, even more than on the other digital subjects, the Council encourages the production of quantified needs and impact studies covering volume, timeframes, costs, risks, repercussions for sector professionals, etc., if not simulations.

Recommendation – Generally speaking, such a mechanism should include tools to be able to measure its effectiveness, such as indicators and cut-off dates for the re-evaluation of the measures put in place.

[6] Decision No. 2011-625 of 10 March 2011.

4. There are more effective and protective alternatives to the administrative blocking vis-à-vis Internet service providers

- Other sectors offer examples of hybrid mechanisms that effectively interface administrative and judicial authorities while providing the necessary safeguards. The President of the French Online Gambling Regulatory Authority (ARJEL),[7] for example, uses the authority's notification system to submit series of websites for blocking to the President of the Court of First Instance, who examines them regularly. This system keeps a specialised judge involved in the decision-making process. The action of the two authorities is coordinated and the regular hearings keep timeframes sufficiently short.

Recommendation – A similar measure could be studied for the administrative and judicial anti-terrorist authorities. The administrative authorities could, for example, regularly present series of websites and content for blocking to the judicial authority, with a special summary proceedings procedure or precautionary measures in situations of extreme urgency.

- There are also other ways of cutting through the red tape inherent in the need to obtain a court ruling every time a "mirror" site appears. The Interministerial Report on Countering Cybercrime[8] recommends, for example, maintaining the judicial authority's role, but attaching to the judge's ruling a specific short-term surveillance obligation assigned to the operator to prevent circumvention and the duplication of illegal websites and content.

Recommendation – In a manner more in keeping with the spirit of the digital economy, a fast-track judicial procedure could also be set up for simple replications of content already banned.

- In addition, the proposed measure creates an extraordinary procedure that could slow down the development of international cooperation in this area. This measure merely shifts the problem abroad and prompts a "Splinternet" phenomenon, which could enable recruiters to juggle between different countries to protect themselves against local technical blocks.

Recommendation – For a digital action to be effective, it has to be internationally coordinated with the best possible level of guarantees and the development of concrete tools such as an international equivalent of PHAROS – a voluntary notification centralisation tool -, a European and/or OECD ad-hoc unit and technical working groups at standardisation body level to prevent a Splinternet phenomenon.

[7] In particular, the possibility for the French Online Gambling Regulatory Authority (ARJEL) to directly apply to the President of the Court of First Instance (TGI) to order hosts or, if not, Internet service providers to block websites and institute systematic case investigations and hearings.

[8] http://www.economie.gouv.fr/remise-du-rapport-sur-la-cybercriminalité

5. Other solutions could be considered to extend the scope of notification tools

The Council recommends refraining from the sole solution of waiver scenarios for notification so as to prevent the proliferation of extraordinary measures that restrict the scope of ordinary law. There should never be any waiver of the principle of an advance court ruling before a mechanism is set up for the surveillance, deletion or blocking of content on the Internet.

***Recommendation* – Foster innovation in the supervision of illegal behaviour and content instead of relying on *a priori* notification and eradication:**

- Standardise the information and response mechanisms and procedures: improve their processing timeframes and effectiveness, make them easier for Internet users to recognise, and develop a unique pictogram that is identical from one platform to the next;
- Improve website terms and conditions to make sure that they are clear and that their users really understand their rights and responsibilities, with the introduction of more respect for cultural, linguistic and social norms;
- Improve mediation with users: help people contact appointed, accredited associations for assistance with the widespread display of visible contact links;
- Encourage good practices and facilitate dialogue among all digital stakeholders, anti-discrimination associations and Internet users to determine what is a matter of best practices, what is a matter of legislation and what is a matter of regulation, if not a form of accreditation.

***Recommendation* – Mainstream actions and assistance, educational, civic and information literacy tools: the precondition for any new supervisory measure must be the empowerment of Internet users through information and education:**

- The tools the Internet offers can be used as information and communication media for all target audiences, for example by asking search engines and social networks to promote content from victim associations and by giving them communication resources.
- At the same time, the PHAROS platform used to notify illegal content has too low a profile with users and could be advertised better.[9]

***Recommendation* – Use the tools already available on the search engines, social networks and video websites**. They offer much more flexible and suitable possibilities than blocking. For example, the administration could simply ask for illegal content to be delisted or require that platforms that do not yet do so inform PHAROS of the content notified to them.

***Recommendation* – Encourage platforms to adopt the use of more balanced measures in their own terms and conditions** such as warnings, temporary suspension and internal arbitration procedures based on measures already put in place by the online collaborative communities. The administration needs to develop regular contacts with platforms operating simultaneously in France and abroad and clarify the arrangements that apply to them.

[9] Like the search engine measures introduced to raise the profile of family planning services.

Appendices

Experts Interviewed

Maryse Artiguelong, Member of the Central Committee of the French Human Rights League (LDH) and representative of the French Digital Freedoms Monitoring Centre

Alain Bauer, Professor of Criminology and Security Consultant

Eric Bocciarelli, Secretary-General of the French Union of the Judiciary (SM) and representative of the French Digital Freedoms Monitoring Centre

Adrienne Charmet-Alix, Coordinator General of the Quadrature du Net and representative of the French Digital Freedoms Monitoring Centre

Agnès Deletang, Consulting Judge for the French National Intelligence Council (CNR)

Christiane Feral-Schuhl, Former President of the Paris Bar and Co-Chair of the National Assembly's Digital Commission

Marie Georges, representative of the French Digital Freedoms Monitoring Centre

Julie Ghibellini, French National Assembly Administrator

Frédéric Guerchoun, Legal Director of the French Online Gambling Regulatory Authority (ARJEL)

Stéphane Lacombe, Project Manager and Consultant for the French Association of Victims of Terrorism (AFVT)

Jean-Marc Manach, Investigative Journalist

Mathieu Mourton, French National Assembly Administrator

Jérôme Rabenou, Assistant to the Director-General for Controls and Information Systems, French Online Gambling Regulatory Authority (ARJEL)

Marc Trévidic, Examining Magistrate, Paris Court of First Instance, Anti-Terrorism Chamber

Bertrand Warusfel, Specialist Lawyer

Michel Wievorka, Sociologist specialised in terrorism

Alain Zabulon, National Intelligence Coordinator

Documentary Resources

Quiliam, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it,* Ghaffar Hussain and Dr. Erin Marie Saltman, May 2014
Available at: http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf
Abstract: http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/djihad-trending-sur-internet.pdf

Information Report No. 3336 of 13 April 2011 on net neutrality and networks by Corine Erhel and Laure de la Raudière (in French)
Available at: http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

Report No. 2000 of 4 June 2014 on Bill No. 1907 on scaling up action to counter the defence of terrorism on the Internet by Messrs Guillaume Larrivé, Eric Ciotti, Philippe Goujon and Olivier Marleix (in French)
Available at: http://www.assemblee-nationale.fr/14/rapports/r2000.asp

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World,* 12 December 2013:
Available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Aconite Internet Solutions, *Internet blocking: balancing cybercrime responses in democratic societies,* Cormac Callanan (Ireland), Marco Gercke (Germany), Estelle De Marco (France), Hein Dries-Ziekenheiner (Netherlands), October 2009
Available at: http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf
Abstract in French: http://www.laquadrature.net/files/Filtrage_d_Internet_et_d%C3%A9mocratie%20-%20R%C3%A9sum%C3%A9%20Principal_1.pdf