Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Parere n. 2014-3 sull'articolo 9 del progetto di legge mirante al rafforzamento delle disposizioni relative alla lotta contro il terrorismo

Consiglio nazionale per il digitale
15 luglio 2014

CNNum
Conseil National du Numérique

http://www.cnnumerique.fr/terrorisme

Premessa

Il Consiglio nazionale per il digitale è stato interpellato riguardo all'articolo 9 del progetto di legge mirante a rafforzare le disposizioni relative alla lotta contro il terrorismo. Tali disposizioni modificano l'articolo 6 della Legge del 21 giugno 2004 intesa a promuovere la fiducia nell'economia digitale (LCEN), prevedendo il blocco da parte dell'autorità amministrativa dei siti responsabili della diffusione di frasi o immagini che incitano a commettere atti di terrorismo o ne fanno l'apologia. Esse ampliano altresì il campo degli strumenti di notifica imposti ai provider.

Nell'intento di esprimere un parere il più possibile informato, il Consiglio nazionale per il digitale ha proceduto ad una quindicina di audizioni che hanno riunito esperti di terrorismo (sociologi, giornalisti, rappresentanti di associazioni), magistrati e avvocati specializzati nel settore, rappresentanti della società civile, membri dei servizi di informazione e professionisti dell'ambito digitale (l'elenco completo è disponibile in allegato).

Le disposizioni sottoposte alla valutazione del Consiglio s'inseriscono in un contesto che vede il moltiplicarsi delle partenze di cittadini francesi per la Siria – dato che il conflitto in corso in tale zona esercita un'attrattiva senza precedenti, in particolare sui giovani.

Il dispositivo proposto è parte di un piano governativo mirante a rafforzare la legislazione antiterrorismo. Esso si prefigge l'obiettivo di lottare contro il reclutamento di terroristi prevedendo la possibilità, da parte dell'autorità amministrativa, di bloccare direttamente l'accesso a determinati siti o contenuti.

Tale disposizione risponde ad una situazione concreta : un gran numero di contenuti che circolano in Rete sotto forma di testi, video, immagini e suoni, inscenano atti di terrorismo o mostrano vittime di conflitti allo scopo di provocare l'adesione e l'empatia degli internauti. I più motivati tra questi ultimi vengono orientati verso un numero più esiguo di siti di reclutamento, a partire dai quali sono poi selezionati per essere destinati ai teatri di operazioni terroristiche. Alcuni di essi rientrano a volte con l'intenzione di commettere azioni violente in Francia. Queste due fasi, di diffusione di contenuti e di reclutamento, non possono essere assimilate.

Il Consiglio nazionale per il digitale ha già avuto l'occasione di fornire il proprio parere riguardo ad argomenti affini[1]. Senza necessariamente opporsi al blocco o al filtro di contenuti in caso di illiceità degli stessi, il consiglio consigliava in casi simili di non derogare mai al principio del ricorso ad un'autorità giudiziaria prima di instaurare un dispositivo di sorveglianza, filtro o blocco di contenuti su Internet. Il dispositivo si propone invece di non tener conto di tale principio di controllo giudiziario preliminare per ragioni di efficienza, intervenendo a monte del reclutamento dei candidati in maniera da impedire loro di accedere a contenuti di tipo propagandistico e a siti di reclutamento. Esso non distingue tra l'efficacia di un'azione di contrasto al reclutamento di terroristi e la comunicazione a fronte alla propaganda terroristica. Queste due problematiche richiedono, tuttavia, risposte di natura diversa.

Stando alle chiarificazioni ricevute riguardo a tale progetto di legge, il dispositivo proposto mira più specificatamente a fornire alle autorità amministrative strumenti per agire rapidamente a fronte della grande viralità di siti e contenuti, là dove oggi, per bloccare ogni riproduzione di contenuti, è richiesta una decisione giudiziaria.

[1] Cfr. il parere n. 2013-4 sulla proposta di legge per il rafforzamento della lotta contro il sistema prostitutivo ((http://www.cnnumerique.fr/avis-prostitution/), il parere n. 2013-6 del 17 dicembre 2013 riguardo ai contenuti e ai comportamenti illeciti on line ((http://www.cnnumerique.fr/contenus-illicites/) e il parere n. 2013-5 del 6 dicembre 2013 sulle libertà digitali (http://www.cnnumerique.fr/libertes-numeriques/).

Dalle altre audizioni emerge invece che occorre operare una distinzione ben precisa tra il reclutamento e il passaggio a vie di fatto, e che i processi di attrazione sono lenti e progressivi. I soggetti prescelti passano il più delle volte attraverso parecchie fasi di indottrinamento e integrazione, prima di essere spinti a passare all'azione o ad unirsi a un determinato gruppo. Stando al parere di numerosi professionisti dell'antiterrorismo, i siti di reclutamento non sono molto numerosi e la decisione di bloccarli deve essere valutata in rapporto all'interesse di poterli sorvegliare.

Infine, i contenuti presenti in Rete sono di natura estremamente varia e complessa e richiedono un know how e degli strumenti di controllo molto sofisticati per riuscire a distinguere ciò che attiene all'incitamento al terrorismo da ciò che rientra nell'ambito dell'opinione. Tali contenuti vengono diffusi soprattutto durante le fasi di sensibilizzazione che precedono il reclutamento vero e proprio. Essi sono scambiati a margine delle comunità di attivisti, e non su dei siti in senso proprio, bensì su piattaforme o forum nei quali coesistono contenuti leciti ed illeciti. Per essere efficace, un dispositivo di blocco dovrebbe essere in grado di analizzare in maniera sottile il contenuto stesso di questi scambi a livello personale. Tali tecniche di indagine profonda non solamente si configurerebbero come censura, ma violerebbero la privacy e la libertà di coscienza, e in quanto tali sarebbero inammissibili.

Il Consiglio ritiene che:

1. Il dispositivo di blocco proposto sia inefficace dal punto di visto tecnico

- I dispositivi di blocco presso gli ISP (Internet Service Provider) sono facilmente aggirabili dai responsabili del reclutamento così come dagli internauti, posto che non consentono di eliminare il contenuto alla fonte.[2]

- Il dispositivo proposto corre il rischio di spingere le reti terroristiche a rendere più complesse le proprie tecniche per rimanere in clandestinità, moltiplicando i livelli di criptaggio e orientandosi verso spazi meno visibili della Rete, rendendo così più difficile il lavoro degli investigatori. Alcune di queste tecniche sono di facile uso e sono già ampiamente utilizzate dagli utenti appartenenti a fasce d'età prese di mira dai responsabili del reclutamento, i quali sono abituati ad utilizzare le Reti Private Virtuali (VPN), il modello Peer-to–Peer (P2P) o la rete TOR.

- Il dispositivo proposto rischia dunque di essere controproducente in termini sia pedagogici sia di immagine. Essendo facilmente aggirabile, esso potrebbe infatti far pensare che le autorità siano in ritardo nella guerra tecnologica, finendo col suscitare sentimenti di orgoglio e impunità.

- Come mostra bene il rapporto stilato dalle deputate Corinne Erhel e Laure de la Raudière sulla situazione delle tecniche attualmente disponibili, i dispositivi di blocco all'accesso presentano rischi di blocco eccessivo o insufficiente. Le esperienze negative registrate in paesi come il Regno Unito,[3] gli Stati Uniti[4] o l'Australia confermano la presenza di tali rischi. Dato che uno stesso server può ospitare numerosi siti o contenuti perfettamente legali, il loro blocco collaterale costituisce una chiara violazione della libertà d'espressione e di comunicazione. L'unica soluzione sarebbe quella di ispezionare direttamente e massicciamente il contenuto degli scambi di informazioni tra internauti[5], incorrendo così in gravi rischi in materia di rispetto della privacy e di libertà di coscienza.

2. Il dispositivo proposto non sia adatto a raccogliere le sfide della lotta contro il reclutamento dei terroristi

- ***Il principio del ricorso preliminare all'autorità giudiziaria continua ad essere indispensabile :***

    - Le consultazioni condotte dal Consiglio hanno evidenziato che il numero di siti dediti al reclutamento è limitato a un numero compreso tra dieci e cento, stando al parere degli esperti. Rispetto a questi numeri, il rischio - a volte evocato - di sovraccarico dei tribunali non è evidente e non sembra dunque ragionevole creare un dispositivo ad hoc che aggiri l'autorità giudiziaria in favore di quella amministrativa.

---

[2] Numerose tecniche consentono di sfuggire al filtro su Internet: proxy servers, tunnels, cambio di host o rotazione di URL, Botnets, cambio di DNS…

[3] In Gran Bretagna, dove gli ISP applicano ormai un filtro automatico su richiesta del governo, quasi il 20 % dei siti più popolari vengono bloccati da almeno un operatore di telecomunicazioni, di cui solamente il 4% sono siti pornografici.

[4] Negli Stati Uniti, il blocco di 10 siti pedopornografici da parte delle autorità americane aveva provocato il blocco di 84 000 siti legali che condividevano lo stesso provider DNS.

[5] Gli operatori effettuano il blocco solo a livello del nome a dominio (DNS), ed eventualmente di sottodominio. Qualunque blocco più sofisticato (in particolare tramite l'URL) richiederebbe tecnologie più avanzate e dovrebbe ricorrere a tecniche di *deep packet inspection* (DPI), in netto contrasto con la riservatezza della corrispondenza.

- Il dispositivo proposto comporta un notevole rischio di conflitto tra l'attività dell' autorità amministrativa e quella dei servizi giudiziari. Ad esempio, la chiusura non ponderata di un sito o di un contenuto da parte delle autorità amministrative potrebbe allertare i terroristi della sorveglianza giudiziaria di cui sono oggetto.

- Il dispositivo proposto non tiene conto delle ricadute negative e dei rischi messi in luce da esperienze simili all'estero, in particolare dalla lotta al terrorismo negli Stati Uniti. Basti pensare alle rivelazioni di Edward Snowden a tale proposito e al rischio di perdita di fiducia dei consumatori nei confronti dell'ecosistema digitale.

- ***I dispositivi di blocco non costituiscono una risposta efficace alla lotta per l'attenzione e l'influenza sulle popolazioni prese di mira dalla filiera terroristica, specialmente tra i giovani :***

  - E' illusorio affrontare dinamiche di diffusione di immagini e contenuti tipiche di Internet e dei social network con misure tecnicamente aggirabili. A tale riguardo, l'unica ipotesi in cui il dispositivo potrebbe avere una qualche efficacia implicherebbe la sua utilizzazione massiccia e sistematica, in netto contrasto con i principi di uno Stato di diritto.

  - In un contesto di lotta alle strategie di diffusione di ideologie radicali, il ricorso al blocco può avere un effetto controproducente, istillando il desiderio di consultare contenuti bloccati.

Raccomandazione – I soggetti consultati mettono in luce la necessità di potenziare la ricerca per meglio comprendere la dimensione sociale del radicalismo e l'esatto ruolo di Internet in tale processo. Numerosi fattori possono concorrere al passaggio di determinati individui all'azione violenta, fattori che sono totalmente estranei all'incitamento diretto ad atti di terrorismo o alla loro apologia. I contatti con ideologie estremiste può, infatti, avvenire in Rete così come al di fuori degli spazi digitali. Studi e ricerche su tali argomenti meritano di essere potenziati per poter servire da base a qualunque futura decisione.

Raccomandazione **-** In un'ottica di prevenzione, gli stessi esperti sottolineano in particolare l'importanza che riveste, nel salvaguardare i soggetti presi di mira, l'educazione e lo sviluppo di capacità di lettura critica dei diversi messaggi diffusi in ambiente digitale e non.

3. Il dispositivo proposto non offra sufficienti garanzie in materia di libertà fondamentali

- Per poter preservare la partecipazione dell'autorità giudiziaria all'interno di tale processo, il dispositivo proposto prevede la nomina, da parte del Ministro della Giustizia, di un magistrato appartenente alla magistratura ordinaria, il cui controllo verterebbe sulla regolarità delle condizioni di creazione, aggiornamento, comunicazione e utilizzo dell'elenco degli indirizzi elettronici relativi ai servizi di comunicazione al pubblico on line.

- Tali misure sono insufficienti, e ciò per due motivi:

    - Il magistrato in questione non è incaricato del controllo sull'opportunità del blocco stesso;
    - Essendo nominato dal governo, questi non presenta le garanzie di indipendenza offerte dalla procedura giudiziaria.

- La Corte costituzionale ha ricordato che il blocco di un sito Internet costituisce una grave violazione della libertà d'espressione e di comunicazione[6]. Qualunque violazione delle libertà fondamentali, anche se giustificata da considerazioni riguardanti la sicurezza nazionale, deve essere proporzionata e necessaria rispetto all'obiettivo che ci si prefigge. In questo caso, il dispositivo proposto istituisce una procedura eccezionale - mirante al blocco su decisione dall'autorità amministrativa - senza che questa sia giustificata dalla presenza di condizioni di assoluta urgenza o di assenza di soluzioni alternative.

- A differenza delle disposizioni relative alla pedopornografia, dalle consultazioni effettuate da parte del Consiglio è emerso che la definizione di concetti come il perpetrare atti di terrorismo o farne l'apologia si presta ad interpretazioni di tipo soggettivo e comporta dunque un reale rischio di deriva verso il semplice reato d'opinione.

Raccomandazione – Il moltiplicarsi del ricorso a regimi di eccezione, che mirano a fare del digitale un settore "a parte", concorre a sminuire la coerenza del sistema giuridico. Il Consiglio raccomanda in questo senso di instaurare una moratoria sull'insieme dei progetti di disposizioni miranti ad istituire misure di blocco o di filtro su Internet. Il bilanciamento tra gli imperativi della sicurezza e della libertà dovrebbe avvenire all'insegna della prudenza e al riparo da pressioni contingenti.

Il moltiplicarsi, a partire dal 2004, di questo tipo di dispositivi impone che ne **venga stilato il bilancio e analizzata l'efficacia.** A tale proposito, ancor più che su altri argomenti di ambito digitale, il Consiglio incoraggia la messa a punto di valutazioni di bisogni e di impatto basate su dati concreti, con riferimento a quantità, tempi, costi, rischi, conseguenze per i professionisti del settore ecc., e persino di simulazioni.

Raccomandazione – In senso generale, un simile dispositivo dovrebbe offrire strumenti suscettibili di misurarne l'efficacia, ad esempio degli indicatori o delle date limite, che consentano di riesaminare le misure disposte.

[6] Decisione n. 2011-625 del 10 marzo 2011
http://www.cnnumerique.fr/terrorisme

4. Si possano utilizzare alternative più efficaci e suscettibili di offrire maggiore tutela rispetto al blocco amministrativo presso gli ISP

- Altri settori offrono esempi di meccanismi ibridi che permettono di collegare efficacemente tra loro le autorità amministrativa e giudiziaria, fornendo al contempo le necessarie garanzie. Il sistema di segnalazione dell'ARJEL,[7] ad esempio, consente al suo Presidente di sottoporre delle liste di siti da bloccare al Presidente del Tribunale di Grande Istanza, il quale le esamina a intervalli regolari. Ciò consente di preservare il ruolo di un giudice specializzato nel processo decisionale. L'azione congiunta delle due autorità risulta in tal modo coordinata e la regolarità delle udienze permette di intervenire in tempi sufficientemente rapidi.

Raccomandazione – Si potrebbe mettere a punto un dispositivo dello stesso tipo che instauri un collegamento tra le autorità amministrative e le autorità giudiziarie preposte all'antiterrorismo. Un dispositivo del genere potrebbe ad esempio consentire alle autorità amministrative di presentare a date stabilite delle serie di siti e di contenuti all'autorità giudiziaria per chiederne il blocco, utilizzando al contempo una specifica procedura d'urgenza o delle misure cautelative in situazioni di emergenza.

- Esistono anche altre soluzioni per ovviare agli intralci insiti nella necessità di ottenere una decisione giudiziale ad ogni nuova comparsa di un sito « specchio ». Il rapporto interministeriale sulla lotta alla cybercriminalità[8] raccomanda ad esempio di preservare il ruolo dell'autorità giudiziaria, ma di accompagnare alla decisione del giudice uno specifico obbligo di sorveglianza, limitato nel tempo e a carico dell'operatore di rete, volto a prevenire, finché è possibile, le procedure di aggiramento e la duplicazione di siti o contenuti illeciti.

Raccomandazione – In uno spirito più rispettoso dell'economia digitale, si potrebbe inoltre approntare una procedura giudiziaria accelerata per quanto concerne le semplici repliche di contenuti già condannati.

- D'altronde, il dispositivo proposto crea un regime d'eccezione che può rallentare lo sviluppo della cooperazione internazionale su questi temi. Tale dispositivo non fa che spostare il problema all'estero, provocando così una balcanizzazione di Internet che potrebbe consentire agli addetti al reclutamento di giostrare tra paesi diversi per difendersi dai blocchi tecnici introdotti a livello locale.

Raccomandazione – Per poter essere efficace, ogni azione in campo digitale va coordinata a livello internazionale, integrando il livello più alto possibile di garanzie e sviluppando strumenti d'intervento concreti, come ad esempio un equivalente internazionale del francese PHAROS – uno strumento per centralizzare le segnalazioni spontanee, una cellula *ad hoc* a livello europeo e/o dell'OCSE, e dei gruppi di lavoro tecnici a livello di organismi di standardizzazione a livello tecnico e giuridico per evitare fenomeni di balcanizzazione di Internet.

[7] In particolare la possibilità, da parte dell'*Autorité de régulation des jeux en ligne* (ARJEL) (Autorità francese di regolamentazione dei giochi on line) di rivolgersi direttamente al Presidente del tribunale di Grande Istanza (TGI) per ordinare agli host, e in mancanza di questi, agli Internet Service Provider (ISP) il blocco dei siti e l'introduzione di procedure sistematiche in fase istruttoria e di trattazione dei casi in esame.

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

5. Riguardo all'estensione del campo degli strumenti di notifica, siano ipotizzabili soluzioni di tipo diverso

Il Consiglio invita a non basarsi unicamente su ipotesi derogatorie delle procedure di segnalazione per evitare il moltiplicarsi di regimi d'eccezione che limitano il campo di applicazione del diritto comune. Non si deve mai derogare al principio del ricorso preliminare all'autorità giudiziaria prima di instaurare un dispositivo di sorveglianza, cancellazione o blocco di contenuti su Internet.

Raccomandazione – Favorire l'innovazione nel controllo di comportamenti e contenuti illeciti piuttosto che limitarsi alla loro segnalazione e cancellazione a priori :

- Introdurre dispositivi e procedure standard di informazione e reazione : migliorarne i tempi di intervento e l'efficacia, facilitarne l'individuazione da parte degli internauti, sviluppare un identico pittogramma su tutte le piattaforme;

- Migliorare le condizioni generali d'utilizzo per verificare la loro leggibilità e la reale conoscenza dei propri diritti e doveri da parte degli utenti, introducendo un maggiore rispetto di norme culturali, linguistiche e sociali ;

- Migliorare la capacità di mediazione nei confronti degli utenti : favorire i contatti delle persone con le associazioni specificamente designate e abilitate a seguirle, generalizzando la presenza di link ben visibili ;

- Promuovere le migliori prassi e facilitare il dialogo tra l'insieme dei soggetti parte in causa del settore digitale, le associazioni per la lotta contro le discriminazioni e gli utenti di Internet, per poter stabilire con chiarezza ciò che dipende dalle migliori prassi, dalla legislazione vigente, dalla normativa o da forme di "labellizzazione".

Raccomandazione – Sistematizzare gli interventi e gli strumenti relativi all'accompagnamento, all'educazione, al senso civico e all'alfabetizzazione : la responsabilizzazione degli internauti tramite campagne educative e di informazione è il presupposto di qualsiasi dispositivo di controllo :

- Gli strumenti offerti da Internet possono fungere da supporto a strategie di sensibilizzazione e di comunicazione rivolte ad ogni tipo di pubblico, per esempio facendo richiesta ai motori di ricerca o ai social network di evidenziare contenuti espressi dalle associazioni delle vittime o offrendo a queste ultime dei mezzi di comunicazione.

- Allo stesso modo, la piattaforma PHAROS, che consente di segnalare contenuti illeciti è, ad esempio, troppo poco conosciuta e potrebbe essere oggetto di una migliore comunicazione[9].

[9] Come nei dispositivi introdotti all'interno dei motori di ricerca per migliorare la visibilità dei servizi in materia di pianificazione familiare.

Raccomandazione – Utilizzare gli strumenti già presenti all'interno dei motori di ricerca, dei social network o dei siti di video sharing. Tali strumenti offrono, infatti, possibilità d'intervenire in maniera molto più duttile e mirata rispetto a blocco. Ad esempio, gli Amministratori potrebbero procedere a semplici richieste di dereferenziazione di contenuti illeciti, o richiedere alle piattaforme che ancora non lo fanno di informare PHAROS dei contenuti che vengono loro segnalati.

***Raccomandazione* – Incoraggiare le piattaforme ad adottare nelle proprie condizioni generali d'utilizzo dispositivi più equilibrati,** come l'avvertimento, la sospensione temporanea o l'introduzione di procedure interne di arbitrato, traendo ispirazione dai dispositivi già utilizzati nelle comunità collaborative on line. Per quanto concerne le piattaforme attive contemporaneamente in Francia e all'estero, l'autorità amministrativa deve sviluppare contatti regolari con esse; va inoltre chiarito quale sia il regime giuridico applicabile nei loro confronti.

Allegati

Personalità sentite nel corso delle audizioni

ARTIGUELONG Maryse, Membro del Comitato centrale della *Ligue des droits de l'Homme* (Lega per i diritti umani*),* rappresentante dell'*Observatoire des libertés et du numérique* (Osservatorio sulle libertà digitali)

BAUER Alain, Professore di criminologia, consulente su questioni di sicurezza

BOCCIARELLI Eric, Segretario generale del *Syndicat de la Magistrature* (Sindacato della Magistratura) rappresentante dell'*Observatoire des libertés et du numérique*

CHARMET-ALIX Adrienne, Coordinatrice generale dell'associazione *Quadrature du Net,* rappresentante dell'*Observatoire des libertés et du numérique*

DELETANG Agnès, Magistrato, consigliere presso il Consiglio Nazionale dei Servizi di Informazione

FERAL-SCHUHL Christiane, ex Presidente dell'Ordine degli Avvocati di Parigi, Copresidente della Commissione per il digitale della Camera dei deputati

GEORGES Marie, Rappresentante dell'*Observatoire des libertés et du numérique*

GHIBELLINI Julie, Funzionaria della Camera dei Deputati

GUERCHOUN Frédéric, Responsabile giuridico dell'*Autorité de régulation des jeux en ligne* – ARJEL (Autorità francese di regolamentazione dei giochi on line)

LACOMBE Stéphane, Responsabile di progetto e consulente dell'Associazione francese delle vittime del terrorismo

MANACH Jean-Marc, Giornalista investigativo

MOURTON Mathieu, Funzionario della Camera dei Deputati

RABENOU Jérôme, Vice direttore generale con delega al controllo e ai sistemi d'informazione dell'*Autorité de régulation des jeux en ligne* (ARJEL)

TRÉVIDIC Marc, Giudice istruttore presso il Tribunale di Grande Istanza di Parigi, settore antiterrorismo

WARUSFEL Bertrand, Avvocato, specialista del settore

WIEVORKA Michel, Sociologo, specialista di terrorismo

ZABULON Alain, Coordinatore nazionale dei Servizi di Informazione

Risorse documentali

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

Relazione informativa n. 3336 del 13 aprile 2011 di Corinne Erhel e Laure de la Raudière sulla neutralità delle Rete e dei social networks
Reperibile al link : http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

Rapporto n. 2000 del 4 giugno 2014 di Guillaume Larrivé, Eric Ciotti, Philippe Goujon e Olivier Marleix sulla proposta di legge n.1907, tesa a rafforzare la lotta contro l'apologia del terrorismo in Rete
Reperibile al link: 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 :
Reperibile al link : 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 (Irlanda), Marco Gercke (Germania), Estelle De Marco (Francia), Hein Dries-Ziekenheiner (Olanda), October 2009
Reperibile al link : http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf
Sintesi in lingua francese :
http://www.laquadrature.net/files/Filtrage_d_Internet_et_d%C3%A9mocratie%20-%20R%C3%A9sum%C3%A9%20Principal_1.pdf