IAIC
Italian Academy of the Internet Code

POSITION PAPER

Cybersecurity e tutela dei cittadini: strumenti normativi, modelli d'intervento e interessi in gioco

Sommario: 1. Introduzione. - 2. Lo stato dell'arte sugli strumenti normativi di sorveglianza pubblica on-line rispetto alla sicurezza dei cittadini: Unione Europea e U.S.A. a confronto. - 3. L'intervento del legislatore italiano, in particolare: il Decreto Legge antiterrorismo. - 4. Il bilanciamento tra diritti individuali e interessi collettivi raggiunto mediante strumenti non normativi. - 5. Conclusioni.

1. Introduzione.

Lo spazio cibernetico riveste un'importanza centrale per la gestione che in esso si esplica della vita politica, sociale ed economica di tutti i Paesi, e l'interconnessione dei relativi sistemi informatici impone a ciascuno di essi di prendere in grande considerazione il tema della sicurezza.

Inizialmente concepito come uno spazio immateriale non soggetto ad alcuna regolamentazione, lo spazio cibernetico si trova oggi sottoposto a confliggenti iniziative regolatorie espressioni dei vari interessi coinvolti, di cui si fanno portavoce Stati, organizzazioni internazionali e organismi sovranazionali.

Un'attenta analisi della realtà odierna mostra, tuttavia, come sia sempre maggiore l'esigenza non tanto di una regolamentazione specifica delle attività svolte all'interno dello spazio cibernetico - ciò anche in ragione dell'attività ermeneutica di giurisprudenza e dottrina che hanno saputo applicare al mutato contesto tecnologico leggi pensate per una realtà "analogica" -, quanto piuttosto di quelle che al di fuori di esse vengono svolte e che, sfruttando le falle della rete, si alimentano con l'intento di minare l'ordine e la certezza delle norme fondamentali della democrazia.

I dati statistici[1] mostrano, infatti, come gli attacchi cibernetici a siti e reti informatiche siano compiuti sempre più spesso con l'aiuto inconsapevole di utenti che

[1] v. Rapporto Akamai sulla sicurezza informatica del quarto trimestre 2014 che ha evidenziato un aumento del 57% di attacchi di tipo DDoS.

divengono ignari strumenti per il compimento di attività illegali che spaziano dalla sottrazione informativa alla promozione di organizzazioni criminali di stampo terroristico.

La possibilità di diffusione "in tempo reale" ed in tutto il globo delle informazioni fa sì che il cyberspazio si trasformi in un amplificatore anonimo per il reclutamento di individui già intenzionati al compimento di azioni criminose[2], ovvero per la persuasione di soggetti facilmente influenzabili, sebbene geograficamente e politicamente lontani dai focolai di guerra (c.d. *foreign fighters*)[3].

In questo contesto, il rispetto da parte delle autorità pubbliche delle libertà fondamentali degli utenti della Rete, quali il diritto all'anonimato, all'inviolabilità delle comunicazioni e del domicilio informatico, rende vulnerabili i Paesi occidentali, così come emerso dai recentissimi fatti che hanno colpito la vicina Francia.

Alla luce di questi accadimenti, infatti, diviene ancor più stringente la necessità di analizzare il tema della sicurezza cibernetica, con il compito di descrivere i contorni dei possibili rimedi e strumenti di intervento, guardando anche alla possibilità di usare, oltre ai consueti strumenti normativi, anche strumenti tecnico-informatici condivisi e adottati su scala globale. Le rivelazioni sull'attività di filtraggio e monitoraggio svolta dall'NSA all'insaputa degli altri Paesi ha dimostrato come un'attività non adeguatamente coordinata non sia in grado di apportare reali benefici in termini di prevenzione dal terrorismo.

Tale necessità, peraltro, è stata rappresentata dallo stesso Presidente della Repubblica italiana, Sergio Mattarella, il quale, in occasione del suo discorso di insediamento, ha dichiarato: "per minacce globali servono risposte globali" ricordando che "i predicatori d'odio e coloro che reclutano assassini utilizzano internet e i mezzi di comunicazione più sofisticati, che sfuggono, per loro stessa natura, a una dimensione territoriale".

Per conseguire questo indefettibile risultato è necessario che a livello globale vengano adottate regole condivise che, partendo dalle caratteristiche tecniche, si rivelino strumenti normativi in grado di bilanciare gli interessi in gioco.

2. Lo stato dell'arte sugli strumenti normativi di sorveglianza pubblica on-line rispetto alla sicurezza dei cittadini: Unione Europea e U.S.A. a confronto.

L'interesse dell'Unione Europea per la materia della *cybersecurity* è nata all'indomani degli eventi che hanno colpito Madrid nel marzo 2004 e Londra nel luglio dell'anno dopo, là dove una serie di attacchi terroristici, di matrice islamica, vennero coordinati per colpire il sistema dei trasporti pubblici locali e gli utenti del servizio[4].

[2] Presidenza del Consiglio dei Ministri – Sistema di informazione per la Sicurezza della Repubblica, Relazione al Parlamento sulla politica dell'informazione per la sicurezza, 2014, p. 12.

[3] A differenza di quel che si potrebbe essere spinti a sostenere, il fenomeno dei *foreign fighters* non affligge solamente l'Europa. Invero, esso trova un'inaspettata fonte di sviluppo nel territorio canadese: Paese che ha partecipato accanto agli U.S.A. alle guerre in Iraq e Afghanistan ma che, a differenza del popolo statunitense, per ragioni socio-politiche, registra un consistente numero di accoliti del regime islamico.

[4] v. COM (2006) 786 del 12 dicembre 2006

A seguito di quei tragici eventi, l'Unione Europea ha preso atto della necessità di rafforzare la rete della pubblica sicurezza ed ha, a tal fine, costituito un'apposita Agenzia, la European Network Information Security Agency (ENISA) cui è stata affidata la delicata attività di studio e predisposizione di una strategia di sicurezza comune ai Paesi dell'Unione.

I lavori dell'Agenzia sono stati fatti propri dalla Commissione Europea che li ha trasmessi al Parlamento Europeo, al Consiglio, al CESE ed al CR, con la Comunicazione (2009) 149[5], atto che ha segnato il formale avvio del processo legislativo che si è concluso con l'elaborazione della Proposta di Direttiva per una strategia europea sulla sicurezza cibernetica del 7 febbraio 2013, approvata con modifiche dal Parlamento Europeo il 13 marzo 2014.

La Direttiva NIS (Network and Information Security), frutto della Comunicazione congiunta della Commissione europea e dell'Alta Rappresentanza dell'Unione Europea per gli Affari Esteri e le Politiche di Sicurezza destinata al Parlamento e al Consiglio, costituisce il testo normativo di riferimento a livello europeo. *Ratio* dell'intervento è quello di fornire ai vari organi dell'Unione i principi per il corretto bilanciamento degli interessi nelle future iniziative[6], con particolare riferimento al rapporto tra la tutela della pubblica sicurezza e la tutela alla riservatezza e dei dati personali. Riprova di ciò è che, non a caso, tale proposta di Direttiva è stata elaborata in concomitanza alla Risoluzione del Parlamento Europeo sui rapporti UE – U.S.A. in materia di trattamento dei dati personali.

Nonostante la proposta di direttiva approvata si discosti sotto molteplici aspetti dal testo inizialmente presentato dalla Commissione Europea, essa individua come suoi principali destinatari gli Internet provider infrastrutturali sui quali grava l'obbligo di notifica di "incidenti", da intendersi quali circostanze o eventi aventi un effetto avverso sulla capacità di una rete o di un sistema informativo di resistere, con un determinato livello di certezza, ad incidenti o azioni dolose che possano compromettere la disponibilità, l'autenticità, l'integrità e la confidenzialità di dati immagazzinati o trasmessi, o di servizi correlati offerti per mezzo o accessibili attraverso tale rete o sistema informativo. Detta previsione - si sottolinea - grava necessariamente sugli operatori infrastrutturali in quanto essi sono gli unici in possesso delle informazioni in grado di tracciare la provenienza dei segnali, ad esempio andando a verificare l'indirizzo IP di un utente che ha postato su un dato blog un messaggio volto ad incitare all'odio razziale o che ha provato ad accedere abusivamente ad un *database* riservato governativo.

---

[5] Commissione Europea, COM(2009) 149 definitivo del 30 marzo 2009, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, avente ad oggetto Proteggere le infrastrutture critiche informatizzate: Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai cyber attacchi e dalle cyber perturbazioni.

[6] Si veda in questo senso la Comunicazione della Commissione Europeo, JOIN(2013) 1 final del 7 febbraio 2013, Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, avente ad oggetto avente ad oggetto: "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*".

Fatta eccezione per la previsione sopra citata, peraltro legittimata da esigenze tecniche indefettibili, la proposta di Direttiva non reca disposizioni che consentano di imporre agli operatori infrastrutturali ulteriori obblighi di *facere*, rimanendo invece ferma la linea di una generale collaborazione, da affrontare sul livello di coinvolgimento volontario, basato sullo scambio di informazioni reciproche (c.d. *info sharing*).

Sull'altro versante dell'Oceano Atlantico si registra un'iniziativa legislativa, che ha preso le mosse dall'ordine esecutivo "*Improving Critical Infrastructure-Cybersecurity"* del 12 febbraio 2013, con la quale è stato avviato un procedimento di consultazione pubblica guidato dalle varie agenzie di settore volto a produrre un quadro regolamentare condiviso in materia di *cybersecurity* che definisca regole, metodi, procedure specifiche e misure di contenimento dei rischi cyber per le infrastrutture[7].

Risulta significativa la scelta legislativa statunitense di incentrare le disposizioni in materia di sicurezza informativa su una *partnership* pubblico – privato, laddove fino all'indomani dello scandalo NSA le organizzazioni governative per la sicurezza chiedevano – ed ottenevano – dai fornitori di servizi di connettività informazioni sulle attività svolte dagli utenti non solo in presenza di concreti attacchi, come sarebbe stato peraltro legittimo fare, ma altresì per mera prevenzione, *rectius* sorveglianza preventiva.

Nel contesto globale appena delineato appare evidente come i singoli Paesi non possano intraprendere percorsi legislativi disallineati rispetto alle scelte di *policy* europea e statunitense.

3. L'intervento del legislatore italiano, in particolare: il Decreto Legge antiterrorismo.

Come anticipato, sul tema infrastrutture critiche, anche l'Unione Europea ha già da tempo avviato il processo di *policymaking* volto a dotare i Paesi membri di un *framework* normativo rispettoso del contemperamento delle diverse esigenze di tutela. Invero, prima dell'approdo alla proposta di Direttiva NIS, l'UE aveva adottato il termine "infrastruttura critica", equivalente al termine riportato nell'ordine esecutivo statunitense, all'interno della Direttiva 2008/114/EC dell'8 Dicembre 2008, il cui ambito di applicazione era tuttavia circoscritto ai settori, strategici, dell'Energia e dei Trasporti, seppur con un'accezione parzialmente diversa.

Il decreto legislativo n. 61/2011, con il quale è stata recepita la direttiva sopra citata, e, successivamente, la legge n. 33/2012, con specifico riferimento agli aeroporti nazionali, hanno definito le modalità per l'individuazione delle Infrastrutture Critiche Europee (ICE) situate sul territorio nazionale e costituiscono, dunque, il primo passo per delineare un quadro normativo nazionale in materia di *cybersecurity*.

Con il successivo DPCM del 24 Gennaio 2013 è stato definito "*in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza*

[7] Cfr. Administration of Barack Obama - Statement on the Release of the "*Framework for Improving Critical Infrastructure Cybersecurity*" by the National Institute of Standards and Technology, February 12, 2014.

nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi" (così art. 1, comma 1, del citato DPCM).

In questo contesto con due successivi DPCM del 27 gennaio 2014, sono stati adottati il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ed il Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Il primo individua i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, attribuisce specifici ruoli e compiti ai diversi soggetti pubblici e privati coinvolti ed individua strumenti e procedure con cui perseguire l'accrescimento delle capacità del Paese di prevenire e rispondere in maniera compartecipata alle sfide poste dallo spazio cibernetico, mentre il Piano Nazionale indica le priorità, gli obiettivi specifici e le linee d'azione per dare concreta attuazione al Quadro Strategico[8].

I due DPCM da ultimo richiamati rappresentano i due strumenti principali di cui il Paese si è dotato per attuare le strategie di difesa contro gli attacchi cibernetici: azioni più o meno automatizzate volte a distruggere o a danneggiare il funzionamento dei sistemi, o comunque destinate a compromettere l'autenticità, l'integrità e la riservatezza dei dati custoditi.

Nel Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico vengono individuate sei linee di intervento per potenziare la sicurezza cibernetica del Paese: il miglioramento delle capacità tecnologiche per l'incremento delle capacità di monitoraggio e dell'analisi preventiva, il potenziamento delle capacità di difesa mediante l'individuazione di un'Autorità nazionale cui affidare i compiti in materia di sicurezza informatica e delle reti che cooperi con le omologhe Autorità europee per la condivisione delle informazioni, l'incentivazione della collaborazione tra Autorità ed imprese, la promozione e la diffusione della cultura della sicurezza cibernetica, il rafforzamento delle tecniche di contrasto dei contenuti illegali on-line e l'attivazione di una rete di cooperazione con i Paesi terzi.

Nel Quadro Strategico Nazionale viene data grande importanza alle *partnership* Pubblico-Privato (PPP) considerate un elemento strutturale indefettibile all'interno dell'architettura nazionale preposta a garantire la sicurezza cibernetica. Tali forme di collaborazione si incentrano, secondo quanto indicato all'interno del Piano Nazionale, sul sistema di *info-sharing*, ossia di condivisione delle informazioni detenute, in un disegno volto ad assicurare l'interoperabilità dei dati e la condivisione degli *standard* di comunicazione e di valutazione delle vulnerabilità[9].

[8] Si veda il comunicato stampa della Presidenza del Consiglio dei Ministri, su www.governo.it, 20 febbraio 2014.

[9] Cfr. Presidenza del Consiglio dei Ministri, Piano nazionale per la protezione cibernetica e la sicurezza informatica, dicembre 2014, p. 16.

In particolare gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, sono chiamati a rispondere ad una serie di obblighi tra i quali: l'apertura delle proprie banche dati per consentire l'accesso ai controlli da parte delle Autorità competenti, la comunicazione al Nucleo per la Sicurezza Cibernetica (NSC) di ogni significativa violazione dell'integrità e della sicurezza informatica, l'adozione di *best practices* per il conseguimento della sicurezza cibernetica e, più in generale, l'obbligo di collaborazione per il ripristino della sicurezza in caso di infrazione della rete[10].

Nelle more della piena attuazione del Piano nazionale per la protezione cibernetica e la sicurezza informatica il legislatore nazionale ha ritenuto di poter confidare sul coinvolgimento volontario dei privati nell'ottica di prevenzione al terrorismo, quale esigenza necessitata dalla presa d'atto dei recenti fatti di cronaca.

Nella giornata di ieri, da ultimo, il Consiglio dei Ministri ha approvato - su proposta del Presidente del Consiglio, Matteo Renzi, e dei Ministri dell'Interno, Angelino Alfano, degli Affari Esteri e della cooperazione internazionale, Paolo Gentiloni, della Difesa, Roberta Pinotti, e della Giustizia, Andrea Orlando - un decreto legge riguardante misure urgenti per il contrasto del terrorismo.

L'adozione di questo testo è fondamentale perché in esso viene per la prima volta individuata nella Direzione Antimafia il centro di coordinamento di tutte le attività di contrasto al terrorismo sul territorio nazionale. Non poteva, infatti, essere più rimandata l'individuazione dell'autorità competente e responsabile del coordinamento di tutte le attività investigative e di repressione avverso un fenomeno che per sua natura non ha caratteri esclusivamente locali o regionali.

Il provvedimento richiamato prevede sul piano penale l'introduzione di una nuova figura di reato destinata a punire chi organizza, finanzia e propaganda viaggi per commettere condotte terroristiche (reclusione da tre a sei anni) e, in questa prospettiva, la punibilità anche del soggetto reclutato nonché del soggetto che si "auto-addestra" alle tecniche terroristiche.

È stata, inoltre, introdotta la possibilità di applicare la misura della sorveglianza speciale di pubblica sicurezza ai potenziali *foreign fighters* nonché di contestuale ritiro del passaporto da parte del Questore con obbligo di soggiorno.

Per quanto qui di specifico interesse il decreto aggiorna gli strumenti di contrasto all'utilizzazione della rete internet per fini di proselitismo e agevolazione di gruppi terroristici, prevedendo aumenti di pena per i delitti di apologia e di istigazione al terrorismo commessi attraverso strumenti telematici.

La cooperazione tra Autorità Giudiziaria e fornitori di connettività, di servizi di *hosting* o di altri servizi connessi alla rete *Internet* viene indicata dal decreto come primo strumento per la prevenzione ed il contrasto al cyberterrorismo.

Nell'ambito delle PPP, già individuate nel Quadro Strategico Nazionale, viene, infatti, previsto che gli *internet service provider* collaborino con il Servizio Polizia

[10] Cfr. Presidenza del Consiglio dei Ministri, Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, dicembre 2014, p. 25.

Postale e delle Telecomunicazioni della Polizia di Stato per la creazione ed il costante aggiornamento di una *"black list"* dei siti internet utilizzati per le attività di cui agli artt. 270-bis c.p. e le finalità di cui all'art. 270-sexies c.p., comprese quelle di "proselitismo", di arruolamento, nonché di addestramento ad attività con finalità di terrorismo anche internazionale.

In questo contesto si inserisce anche la modifica dell'articolo 53, comma 1, del decreto legislativo 30 giugno 2003, n. 196 (cd. Codice della privacy), ai sensi del quale, nella nuova formulazione, le Forze di polizia e gli altri organi di pubblica sicurezza sono esentati dall'osservanza di alcune disposizioni del predetto Codice nell'effettuazione di trattamenti di dati personali per finalità di polizia espressamente individuati da norme di legge.

Infine, in relazione alle fattispecie delittuose sopra citate, le previsioni legislative conterrebbero, in analogia con quanto previsto dalla direttiva 2000/31/CE e dal d.lgs. n. 70/2003, l'obbligo diretto ai fornitori di connettività di servizi, di *hosting* o di altri servizi connessi alla rete *Internet* di ottemperare, nell'arco di quarantotto ore, al decreto motivato dell'Autorità Giudiziaria contenente l'ordine di rimozione di specifici contenuti Internet qualora vi siano concreti elementi per ritenere che detti reati siano stati compiuti per via telematica.

Appare indubbio che i recenti accadimenti abbiano spinto il legislatore nazionale ad intraprendere azioni immediate per scongiurare il pericolo di derive di "cyber anarchia" e di una nuova militarizzazione attraverso l'uso di questo spazio, con la possibilità per gli Stati di ospitare o sponsorizzare reti criminali, terroristiche o di spionaggio via web, analogamente a quanto accaduto in questi giorni con riferimento al documento programmatico, di chiaro stampo propagandistico, a firma dell'Isis dal titolo "The Islamic State 2015", il quale ha sfruttato il sito Wikilao per essere divulgato sulla rete e reclutare combattenti per riempire i campi di combattimento dello scacchiere siro-iracheno.

Deve osservarsi, peraltro, come il Governo abbia saputo delineare una disciplina che, seppur di emergenza, non si esaurisce in una mera compressione di diritti, analogamente a quanto accaduto in Francia (v. *infra*) e già prima negli Stati Uniti d'America, ma che, al contrario, si dimostra equilibrata nel bilanciare i vari interessi in gioco anche grazie ad efficaci strumenti di coinvolgimento dei soggetti privati, rimettendo sempre le decisioni finali all'Autorità Giudiziaria, che è, per sua intrinseca natura, garante del rispetto dei diritti.

Queste tipologie di interventi rappresentano chiaramente le conseguenze dell'uso dei soli strumenti normativi per il bilanciamento degli interessi in gioco, bilanciamento che talora purtroppo costringe ad un sacrificio o a una compressione di diritti e libertà fondamentali di rango comunque equi-ordinato a quello cui si intende dare protezione.

4. Il bilanciamento di diritti individuali e interessi collettivi raggiunto mediante strumenti non normativi.

Il rischio maggiore nell'affrontare un tema tanto delicato come quello della repressione dei gruppi terroristici è quello di adottare misure legislative eccessivamente repressive sull'onda emotiva di eventi tragici analoghi a quelli accaduti in Francia, così come in passato è stato per il *Patriot Act*[11] adottato negli Stati Uniti d'America dopo l'attacco alle Torri Gemelle del 2001.

In questo senso non può non osservarsi come in Francia lo scorso 5 febbraio sia stato adottato il decreto n. 5/2015[12] ai sensi del quale può essere inibito l'accesso ad un sito tramite il blocco del DNS di determinati siti senza bisogno dell'intervento di un giudice, ma solo con l'intervento di una commissione *ad hoc* nel caso in cui il contenuto abbia natura pedopornografica o terroristica. Due sono, *prima facie*, le criticità di cui al citato decreto francese: la prima è riferibile alla misura tecnica che può essere disposta che, per sua natura, comporta il blocco non solo dello specifico contenuto illecito, ma di tutto il sito che lo ospita, la seconda per quanto attiene alla compressione delle libertà costituzionali, anche in termini di equo processo davanti al giudice naturale costituito, non solo per la tutela della sicurezza nazionale, ma anche per la tutela dei minori.

Il compito che il legislatore, prima, e gli interpreti, in fase applicativa, poi, sono chiamati ad assolvere è, dunque, quello di coniugare diritti individuali con interessi collettivi: creare grandi banche dati per la prevenzione dei reati, qualora le stesse non siano sufficientemente protette, potrebbe paradossalmente aumentare la superficie degli attacchi terroristici, agevolando l'accesso delle organizzazioni criminali ai nominativi di soggetti reclutabili per scopi illeciti.

D'altro canto nell'operare il necessario bilanciamento non si può non tenere in considerazione il principio normativo elaborato in via giurisprudenziale; il riferimento è alla pronuncia della Corte di Giustizia dell'Unione Europea in materia di *data retention*[13], la quale ha invitato gli operatori coinvolti nelle procedure investigative a usare strumenti di indagine proporzionati alla tutela della libertà dei cittadini, senza che un diritto prevalga sull'altro.

Invero, l'interesse ad un equo contemperamento non è legato solamente alla questione, pubblicistica, della tutela dei diritti individuali e fondamentali ma anche a esigenze di carattere commerciale avuto riguardo al fatto che da una violazione del diritto alla riservatezza discende una precisa responsabilità in capo ai detentori di dati personali.

Anche gli operatori economici, intendendo qui fare espresso riferimento ai grandi fornitori di servizi della società dell'informazione, devono essere, infatti, messi in condizione di sapere cosa esattamente sono legittimati e obbligati a comunicare alle

[11] Public Law 107–56—OCT. 26, 2001: *Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism* (USA PATRIOT ACT) *act of* 2001.
[12] Decreto n. 2015-125 del 5 febbraio 2015 "*relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique*".
[13] Corte di Giustizia Europea, Grande Sezione, 8 aprile 2014, Cause riunite C-293/12 e C-594/12.

autorità giudiziarie e cosa, invece, devono custodire nel rispetto dei diritti inviolabili dei propri utenti[14], ciò al fine di tutelare anche la loro libertà di iniziativa economica.

In sintesi, dunque, l'adozione di norme che derogano ai presidi legislativi volti a dare concreta tutela alle libertà fondamentali costituzionali richiedono l'esigenza di un equo contemperamento tra i diversi interessi coinvolti. In particolare, se, da un lato, i governi hanno la necessità di preservare la pubblica sicurezza, anche mediante un controllo diffuso di carattere preventivo, dall'altra, viene richiesto ai fornitori di connettività, specie se fornitori globali, di farsi garanti della tutela del diritto alla riservatezza dei relativi fruitori, tramite strumenti tecnici, come ad esempio la criptazione dei dati, che consente di mantenere privati dati che, viceversa, potrebbero esporre eccessivamente gli utenti.

L'assenza di una normativa volta a regolare i rapporti tra autorità pubbliche e privati nell'ambito delle PPP finalizzate alla tutela della sicurezza pubblica, rende anche maggiormente complessa l'adozione di iniziative tecniche e divulgative di questi ultimi che, svincolati da rigide forme di burocratizzazione, sono in grado di essere efficaci al livello delle stesse azioni che contrastano.

5. Conclusioni.

Alla luce delle osservazioni svolte, lo scenario che si propone risulta dunque molto complesso: da un lato la necessità, attualmente quanto mai pressante, di tutelare l'interesse collettivo della sicurezza pubblica, dall'altro la constatazione che le ingerenze del regolatore potrebbero direttamente comprimere diritti individuali inviolabili, ovvero limitare i diritti degli operatori economici, fornitori di servizi della società dell'informazione.

La vera sfida consiste, dunque, nel raggiungere quell'equo contemperamento che, a fronte di quanto esposto, risulta essere non solo imprescindibile ma altresì assai delicato, avuto riguardo al rango degli interessi in gioco: tutti di livello costituzionale, ognuno tutelato da diverse fonti nazionali e sovranazionali che, talvolta sull'onda di un particolare contesto storico-politico, hanno approntato diverse soluzioni.

La complessità delle questioni suggerisce, come già anticipato, di considerare anche strade alternative agli strumenti normativi, in particolare usando a favore della collettività accorgimenti tecnici e divulgativi: strumenti di carattere informativo che, con gli opportuni correttivi, potrebbero essere in grado di finalizzare le intenzioni del legislatore.

Ciò a cominciare dalla realizzazione e dall'implementazione delle reti inter-istituzionali che potrebbero essere individuate quale modelli di intervento idoneo per

[14] Gli obblighi di tutela del diritto alla riservatezza degli utenti che gravano in capo agli operatori economici sono particolarmente pregnanti. Le conseguenze della loro violazione possono anche essere imprevedibili, come è accaduto per FaceBooK che, tacciata di aver collaborato con la National Security Agency (NSA) tracciando, all'insaputa degli utenti, le informazioni con riferimento alle quali veniva espressa approvazione mediante il pulsante *like*), è stata convenuta in una *class action* sottoscritta da più di venticinquemila utenti.

realizzare un equo bilanciamento tra tutti gli interessi coinvolti, riducendo peraltro il rischio di esposizione dei fornitori di connettività e di servizi globali alle rivendicazioni di tutela del diritto alla riservatezza e alla protezione dei dati personali avanzate dagli utenti.

L'esperienza statunitense richiamata, relativa all'applicazione del *Patriot Act*, ha mostrato come anche l'adozione di tecniche di criptazione dei dati conduca ad un equo bilanciamento tra tutela della sicurezza pubblica e tutela dei diritti e delle libertà costituzionalmente garantite: i dati criptati possono, infatti, essere raccolti e detenuti dalle competenti autorità governative le quali "usano" tali informazioni solo in presenza di un sospetto fondato di una minaccia alla sicurezza proveniente da un individuo in particolare.

Infine, potrebbero tornare utili altri strumenti di carattere tecnico informativo, come ad esempio i cd. *counter-speech* i quali, apparendo in sovrapposizione alla pagina web a contenuto critico, perseguono l'obiettivo di veicolare messaggi positivi, non necessariamente confutando i contenuti visionati (cosa che paradossalmente potrebbe provocare un rafforzamento delle convinzioni dell'utente).

Questi appena elencati sono solamente taluni degli strumenti non normativi che potrebbero limitare e contrastare nel medesimo scenario del cyberspazio gli attacchi terroristici sulla e alla Rete e che si ritiene il legislatore nazionale, o sovranazionale, non possa ignorare nell'ottica di un'efficace repressione di fenomeni pericolosi come il cyberterrorismo senza per questo porre a detrimento diritti inviolabili faticosamente conquistati.

Appare, d'altronde, più facile condividere globalmente uno strumento tecnico, quale ad esempio la criptazione dei dati, o politiche di educazione degli utenti della Rete, quale il *counter-speech*, piuttosto che un testo normativo. Tale carattere deve essere tenuto in massima considerazione in quanto organizzazioni terroristiche che operano su scala globale richiedono e impongono altrettanto globali e unitarie risposte.

In questo scenario, dunque, emerge come la tutela del *cyberspazio* possa essere efficacemente e proficuamente demandata ad iniziative di auto e co-regolamentazione degli operatori economici che, nell'ambito di politiche legislative condivise da parte di vari Paesi, risultano essere maggiormente celeri nel dare una precisa risposta alle istanze di risoluzione dei conflitti.

Roma, 11 febbraio 2015