Internet, sicurezza e libertà personali nell'epoca dell'emergenza terrorismo: alcune riflessioni

Giovanni Ziccardi[1]

1. Il delicato rapporto tra internet e terrorismo.

Il rapporto tra internet (e le tecnologie strettamente correlate alla rete, quali la crittografia, lo scambio di *file* e d'informazioni, i protocolli di comunicazione, i siti web) e il mondo del terrorismo nazionale e internazionale è stato caratterizzato, in questi ultimi cinque anni, da una sensibile evoluzione: ben presto internet è stata vista, dal legislatore di tutti i paesi, come una possibile minaccia, una tecnologia tanto potente e trasparente quanto difficile da gestire (si pensi al problema dell'anonimato) e, in molti casi, impossibile da controllare.
In un recente, dettagliato rapporto dello *United States Institute of Peace*, dal titolo significativo di "How modern terrorism uses the Internet", e redatto nel 2004 da G. Weimann, sono descritte, con dovizia di particolari, tutte le modalità con cui si manifesta questo rapporto tra internet e il mondo del terrorismo[2].
Le prime presenze di gruppi terroristi in internet risalgono all'anno 1998, quando oltre la metà delle trenta organizzazioni che erano definite quali "organizzazioni terroristiche straniere" dal *U.S. Antiterrorism and Effective Death Penalty Act* del 1996[3] avevano il loro sito web in rete, pubblicamente accessibile.
Nell'anno 2000 si è registrato un aumento esponenziale, e tutte le organizzazioni terroristiche avevano pubblicato il loro sito web; nel 2005 sono stati recensiti, in tale rapporto, centinaia di siti che forniscono informazioni sui terroristi e, soprattutto, forniscono servizi ai loro potenziali sostenitori (V. Musacchio, 2005).
Contestualmente, molti studiosi (che operano soprattutto nel settore dell'*information security* e della *computer and network forensics*) hanno evidenziato un nuovo ambito di studio: accanto alla "presenza" in rete dei terroristi, si è iniziato a studiare anche la rosa delle minacce strettamente correlate al cyberterrorismo e alla *cyberwarfare* (D. Verton, 2003).
In particolare, l'attenzione si è equamente divisa tra l'uso di internet come strumento per la visibilità delle attività terroristiche e l'uso di internet per portare attacchi informatici con finalità terroristiche (M. Strano, B. Negre, P. Galdieri, 2002). Nel rapporto citato si parla, in questo caso, di "utilizzo quotidiano di internet da parte dei terroristi" (in questo caso, il singolo terrorista o le organizzazioni terroristiche utilizzano internet con le stesse modalità di un utente comune, cambiando solamente i contenuti della comunicazione) e di "attacco via network per finalità terroristiche" (in questo caso, il terrorista usa internet per portare attacchi informatici o per commettere altri tipi di reato).
La presenza delle organizzazioni terroristiche in internet si è rivelata, in questi anni, molto dinamica: i siti web vengono pubblicati improvvisamente, senza alcun annuncio, e

---

[1] Professore Associato di Informatica Giuridica e Informatica Giuridica Avanzata presso l'Università degli Studi di Milano. Avvocato, Membro del *Board of Directors* di *IP Justice* (http://www.ipjustice.org).
[2] Il testo completo del *Report* è consultabile sul sito dello *United States Institute of Peace*, all'indirizzo web http://www.usip.org/
[3] Si tratta di un importante provvedimento normativo emanato all'indomani degli attentati di Oklahoma City e del *World Trade Center* in New York.

dopo pochi giorni, a volte poche ore, spariscono dal web oppure riappaiono ad un altro indirizzo (S. Portesi, 2004).
Il primo problema che è evidenziato da molto studiosi è, in questo caso, l'estrema decentralizzazione delle tecnologie informatiche utilizzate (D. Verton, 2003).
Per sua stessa natura, internet si configura, in molti casi, come un'arena ideale per il terrorismo e per le attività correlate alle organizzazioni terroristiche: *in primis* si è in presenza di una tecnologia che offre un accesso facile. In molti paesi, poi, vi è poca regolamentazione, e a ciò si aggiunge la possibilità di raggiungere un'*audience* altissima, molto spesso mondiale.
Le caratteristiche informatiche e sociali che hanno decretato il successo di internet, si sono rivelate ideali anche per un suo *misuse* o *abuse*: si pensi alla possibilità di effettuare comunicazioni con un alto livello di anonimato, alla velocità e immediatezza del flusso di comunicazioni, a quanto sia poco costoso, sovente gratuito, il mantenimento di un sito web o di un ambiente multimediale (con registrazioni di proclami, riprese video di interventi terroristici o di cattura e interrogatorio di ostaggi) e, ultimo ma non ultimo, a quanto sia facile, tramite internet, riuscire a contattare le redazioni dei *media* tradizionali, che molto spesso valutano Internet quale fonte attendibile.
Il rapporto citato ha analizzato, nel dettaglio, centinaia di siti di organizzazioni terroristiche: come prevedibile, il contenuto di tali siti è *standard*. Di solito è riportata la storia dell'organizzazione, le attività, le basi sociali e ideologiche della protesta, le biografie dei *leader*, le mappe delle zone territoriali coinvolte, i comunicati ai *media* e, sovente, proclami critici nei confronti degli avversari politici e dei nemici.
Il *target* cui si rivolgono tali siti viene, dagli studiosi, suddiviso in tre direzioni (G. Weimann, 2004): un primo messaggio è solitamente rivolto a sostenitori attuali e potenziali, un secondo messaggio è pensato per raggiungere la pubblica opinione internazionale (di solito è la parte del sito dedicata ai comunicati stampa) e una terza parte dei siti è solitamente rivolta agli avversari, al fine di demoralizzarli (minacciando attacchi o colpevolizzando determinati loro comportamenti).
Nel *report*, infine, sono delineate otto modalità con le quali i terroristi usano Internet.
Il primo metodo di utilizzo delle nuove tecnologie viene definito "psychological warfare": in questo caso Internet è usata come mezzo per una vera e propria guerra psicologica, diffondendo notizie non vere, minacce, immagini di operazioni recenti, o *videotapes* (come capitò con il giornalista americano Daniel Pearl).
Il secondo fine per cui Internet viene utilizzata è un mero fine di pubblicità e propaganda: in realtà tale utilizzo ha dimostrato, ben presto, un potenziale enorme, in quanto, prima della diffusione di Internet su larga scala, era molto difficile, soprattutto per le nuove organizzazioni o a seguito di azioni terroristiche medio-piccole, raggiungere i *media*.
Il terzo uso di Internet a fini terroristici è il *data mining*, ovvero la ricerca di informazioni, in rete, utili per azioni di terrore. Internet può fornire informazioni dettagliate su obiettivi, linee di trasporti, edifici pubblici, aereoporti, porti. Queste informazioni, unite a software che, ad esempio, possano analizzare le eventuali debolezze di una struttura, possono essere molto utili a fini pratici. Gli esperti sono convinti che usando informazioni pubbliche (ovvero disponibili in rete) senza ricorrere ad alcuna azione illegale per carpire informazioni riservate, si possa ottenere almeno l'80 per cento delle informazioni su un obiettivo di interesse pubblico.
Il quarto utilizzo comune di Internet a fini terroristici è per la raccolta di fondi. Tramite internet viene creata una vera e propria rete di organizzazioni, fondazioni, enti, che hanno il solo scopo di raccogliere fondi per la causa. Non è raro trovare, sui siti, gli estremi dei conti correnti per effettuare versamenti.

Il quinto uso che sovente è fatto delle tecnologie è quello di predisporre la presenza in Internet quale mezzo per reclutare, per spostare o per coordinare potenziali terroristi.
Internet, inoltre, ha dimostrato grande efficienza nell'uso come sistema di *networking* per mantenere i contatti: ciò si è dimostrato di immediata utilità, in quanto esistono numerosissime cellule terroristiche che non operano sotto la diretta gerarchia di un soggetto, ma sono semi-indipendenti.
Internet viene, poi, costantemente utilizzato come mezzo per condividere le informazioni, ad esempio per costruire armi chimiche, bombe o per elaborare sostanze velenose.
L'ultimo utilizzo tipico è ai fini di programmazione e di coordinamento delle azioni, ad esempio con il *post* di messaggi cifrati in *forum* privati.

2. La carta di Madrid del marzo 2005: terrorismo, Internet e democrazia.

Nel marzo del 2005, in una Madrid ancora scossa dai recenti attacchi terroristici, si tenne l'*International summit on democracy, security and terrorism*, un evento che riuniva studiosi, tecnici ed *ex* capi di stato al fine di elaborare linee guida, principi e suggerimenti per contrastare, a livello internazionale, il terrorismo.
Una sessione *ad hoc* fu dedicata, durante il *summit*, a internet: studiosi quali Rebecca MacKinnon e Joi Ito elaborarono, e pubblicarono, un documento intitolato "The infrastructure of democracy: strenghtening the open internet for a safer word", datato 11 marzo 2005, che ha destato grande interesse nel mondo scientifico.
Tale documento muove in una direzione completamente differente: non più un aumento di controllo e di chiusura della rete, per prevenire il terrorismo, ma una sempre maggiore apertura delle tecnologie, con la ferma convinzione che più la tecnologia è aperta e trasparente, più aumenta l'efficienza delle azioni di contrasto.
La "carta di Madrid" è basata su alcuni principi che cercano di elaborare un approccio che sia rispettoso nei confronti della tecnologia, consapevole del bene culturale e sociale che ha portato internet e, soprattutto, diffidente nei confronti dell'azione del legislatore su questi temi.
Il primo principio, introduttivo delle problematiche, evidenzia internet come vera e propria base della società democratica del XXI secolo, in quanto i valori che sono al centro di internet e del concetto di democrazia sono allineati e sovrapponibili.
Internet è, fondamentalmente, basata sull'apertura, sulla partecipazione, sulla libertà di manifestazione del pensiero diffusa, sulla diversità e, contestualmente, sulla possibilità di raggiungere informazioni e idee d'ogni tipo. Permette alle persone di comunicare e di collaborare attraverso i confini fisici, e al di là delle convinzioni locali, sino ad unire famiglie e culture che sono in conflitto.
Questa grande capacità di connettere le persone, fornisce un aiuto per formare società civili, foraggiando l'economia e lo sviluppo, e collegando le persone ai mercati e alle informazioni. Internet introduce nuove idee e nuovi punti di vista soprattutto nel pensiero di coloro che potrebbero essere isolati e portati alla violenza politica. Il tutto in un ambiente dove, chiaramente, internet non è né al di là né al di sopra della legge: gli stessi principi giuridici che si applicano nel "mondo fisico", si applicano anche alle attività umane che vengono condotte in Internet.
Dopo queste premesse, la carta di Madrid muove verso il secondo punto, ovvero che i sistemi decentralizzati (quei sistemi dove non vi è né un'autorità di potere né un sistema tecnologico centralizzato, ma il potere di agire è in mano a una molteplicità di soggetti) sono il mezzo ideale per combattere e contrastare le ondate di violenza decentralizzate.

I redattori del documento in oggetto notano, *in primis*, come i *network* delle organizzazioni terroristiche siano altamente decentralizzati e distribuiti; uno sforzo centralizzato in sé non può, allora, combattere efficacemente il terrorismo.
Inoltre il terrorismo è, essenzialmente, un problema di tutti i cittadini, e Internet ha la capacità unica di connettere tutti: l'idea di una "cittadinanza connessa" viene vista da questi studiosi come la migliore difesa contro la propaganda terroristica, e l'attentato spagnolo dell'11 marzo ha dimostrato come internet abbia consentito una risposta rapida ed efficace. I cittadini furono capaci di utilizzare internet per organizzarsi, e la rete fece notare al mondo come, nel mondo distribuito dei *web log* (*Blog*) e di altri mezzi di comunicazione gestiti direttamente dai cittadini, la verità potesse emerge meglio in una conversazione aperta, anche tra persone di differenti vedute.
Questi due primi punti di dibattito hanno portato, come conseguenza logica, al terzo, e fondamentale, concetto contenuto nella carta di Madrid, ovvero che la migliore risposta all'abuso di apertura della rete è di concedere ancora più apertura, sia dal punto di vista delle tecnologie utilizzabili, sia dal punto di vista della regolamentazione futura.
Gli ambienti aperti e trasparenti sono, nella visione di questi studiosi, molto più sicuri e più stabili di ambienti chiusi e opachi. Del resto, mentre i servizi correlati a internet possono essere interrotti, internet come sistema globale può benissimo resistere agli attacchi, anche a quelli sofisticati e distribuiti su larga scala. La connessione che internet fornisce, permettendo alle persone di parlare continuamente tra loro, contrasta la divisione che i terroristi cercano di creare.
I principi poco sopra enunciati sono strettamente connessi alla regolamentazione normativa delle nuove tecnologie e di internet. Una regolamentazione di internet troppo vincolante negli stati democratici attuali può minacciare lo sviluppo di democrazie emergenti. Le attività terroristiche, si è visto, non possono danneggiare più di tanto internet, ma un'attività legislativa troppo vivace e stringente, anche se emanata in risposta ad atti di terrorismo, lo può fare.
Secondo questi eminenti studiosi, i governi dovrebbero intervenire, dal punto legislativo, sul cuore di internet con estrema cautela: alcune iniziative governative che possono sembrare giuste in linea di principio, di fatto violano i principi basilari che hanno reso internet un successo. Ad esempio, molti gruppi d'interesse hanno chiesto una legislazione che portasse alla fine della possibilità di anonimato in rete. Un'attività legislativa simile non avrebbe alcun effetto sul panorama del terrorismo, però avrebbe un'influenza politica molto forte e ridurrebbe libertà di manifestazione del pensiero e trasparenza.
In conclusione, l'idea di un'internet aperta si presenta come il nuovo fondamento della democrazia del XXI secolo e come uno strumento di importanza critica nella lotta contro il terrorismo. Riconoscere il valore di internet come un sistema di comunicazione e un'infrastruttura critica, comporta il fatto che occorre investire per rafforzare l'infrastruttura tecnologica contro gli attacchi, e fare in modo che si possa ripristinare in maniera più rapida possibile da eventuali danni.
Contestualmente, occorre progettare una politica che diffonda ancora di più l'accesso, abbattendo il *digital divide* e fornendo connessione a Internet per tutti.
Da un punto di vista giuridico, infine, occorre sempre proteggere la libertà di manifestazione del pensiero e l'associazionismo, consentire la disponibilità di sistemi di comunicazione anonima per tutti, e resistere ai tentativi di regolare Internet a livello governativo, in quanto si possono introdurre processi nocivi per l'evoluzione di Internet stessa.

3. Terrorismo e Internet nel panorama legislativo italiano: il "pacchetto Pisanu".

L'approccio del legislatore italiano al fenomeno del terrorismo in internet muove da considerazioni opposte rispetto a quelle elaborate nella carta di Madrid. Non vi è alcuna concessione a una maggiore apertura, ma vi è un aumento del controllo, la volontà di registrazione di ogni accesso, la regolamentazione delle strutture private e imprenditoriali che offrono l'accesso a Internet al pubblico e l'obbligo di mantenere i *file* di *log*, ovvero tutte le tracce delle navigazioni e delle comunicazioni elettroniche.
Del resto, la visione del legislatore italiano con riferimento alle tecnologie informatiche è sempre stata, negli ultimi quindici anni, quella di vedere i computer come una minaccia, soprattutto se utilizzati dal tanto temuto *mad scientist*: dal 1993, anno della prima normativa sui *computer crimes* in Italia, sino alla recente riforma normativa in tema di *privacy*, l'uso intenso della repressione penale ha creato un panorama giuridico di estrema rigidità sanzionatoria e di grande inefficienza pratica.
In realtà, analizzando con attenzione la recente riforma normativa che ha riguardato Internet, si nota come la mancata completa comprensione, da parte del nostro legislatore, del funzionamento e della natura delle tecnologie abbia creato, in prospettiva, problemi applicativi di non poco conto.
Infine, ultimo ma non ultimo, la riforma dell'ambiente elettronico voluta dal "pacchetto Pisanu" ha la peculiare caratteristica di non dedicare nulla alla prevenzione: tutte le norme correlate al mondo elettronico sembrano finalizzate alla reazione ad atti terroristici già avvenuti, e ciò è preoccupante, dal momento che tutti sono concordi nel ritenere che la lotta al terrorismo è, essenzialmente, lotta di prevenzione.
Procedendo con ordine, con riferimento al problema dell'anonimato, il pacchetto normativo italiano non interviene esplicitamente su tali temi.
Si può però correlare il problema degli *anonymous remailer*, ovvero dei *server* che rendono impossibile risalire al mittente di un messaggio di posta elettronica, alle norme del pacchetto che parlano di conservazione dei *log* e dei dati del traffico telefonico e telematico, di monitoraggio delle operazioni dell'utente e di archiviazione dei relativi dati.
Il decreto ministeriale attuativo, datato 16 agosto 2005[4], specifica che i titolari e i gestori sono tenuti ad adottare le misure occorrenti per il monitoraggio delle attività, che consistono nel memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni. In tal caso, quindi, se la legge stabilisce che si devono memorizzare e mantenere i dati, ciò impedirebbe l'utilizzo di sistemi che non consentono di farlo (come, appunto, alcuni *server* che consentono la corrispondenza e la navigazione anonima).
D'altro canto, nel caso in cui un fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico volesse offrire ai suoi clienti, desiderosi di mantenere un certo livello di anonimato in rete, un servizio di posta o navigazione anonima, non vi è nessuna norma che esplicitamente vieti un servizio di questo tipo. Il problema sorgerebbe unicamente nel caso in cui i *server* alla base di questi sistemi non conservassero i dati e, quindi, rendessero impossibile l'applicazione della legge. La cosa non è di poco conto: offrire un servizio di *mail* o navigazione anonima e tenere i *file* di *log* delle attività di quel servizio non si escludono a vicenda, è ben noto. Da

[4] Si tratta del decreto del Ministero dell'Interno 16 agosto 2005, " Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, ai sensi dell'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155. (GU n. 190 del 17-8-2005).

un lato vi sono servizi che informano l'utente che "non sono tenuti i *file* di log" (e in quel caso la violazione della normativa attuale è palese), ma dall'altro lato vi possono essere servizi che informano l'utente che i *file* di *log* vengono tenuti, ma che il livello di anonimato dell'utente viene garantito a un livello molto alto in quanto i *file* non saranno dati all'esterno se non in casi eccezionali. La garanzia di anonimato si basa, insomma, non sul fatto che i *file* di *log* non siano tenuti, ma sul fatto che venga adottata una *policy* estremamente rigorosa in tema di "rilascio" all'esterno dei *file* di *log*, soprattutto rilascio degli stessi all'autorità inquirente.
Infine, l'art. 7 del decreto parla esplicitamente di "circolo privato" di qualsiasi specie: da ciò sembra derivare che la legge in oggetto non prenda in considerazione, quindi, il privato, e che nessuna norma vieti ad un privato di offrire a terzi un servizio di posta elettronica anonima.
Anonimato a parte, il meccanismo applicativo del pacchetto sicurezza ruota attorno a due cardini: l'imposizione dell'obbligo di conservazione dei dati di traffico circostanziali e l'estensione di obblighi e controlli di polizia amministrativa anche alle associazioni e ai comitati, in modo da rendere praticamente applicabile l'obbligo di licenza anche ai singoli cittadini.
Nell'ottica di fornire adeguata protezione ai cittadini da possibili attentati terroristici, con questo decreto vengono fissati maggiori poteri di controllo e di ingerenza da parte delle forze dell'ordine, che inevitabilmente investono le reti telematiche limitando, di fatto, la riservatezza dei cittadini.
All'articolo 6 del decreto, rubricato come "Nuove norme sui dati del traffico informatico e telematico", è previsto un obbligo di conservazione dei dati relativi al traffico effettuato via telefono o via internet fino al 31 dicembre 2007, al fine di consentire indagini anche abbastanza risalenti nel tempo e, quindi, la repressione di determinate fattispecie criminose.
Questa prima previsione ha subito incontrato le opposizioni, da un lato, dei sostenitori della privacy degli utenti, i quali affermano che il dettato normativo è oggettivamente sproporzionato, anche a fronte di giustissime esigenze investigative, e dall'altro dai *provider* i quali, per conservare questa enorme mole di dati, dovranno affrontare ingenti investimenti economici in termini di soluzioni di *storage*.
Sempre nel già citato articolo 6 del decreto è previsto, inoltre, l'obbligo di mostrare un documento d'identità "al momento della consegna o messa a disposizione" di una scheda elettronica per la telefonia cellulare (SIM). L'utilizzazione dei dati raccolti in ottemperanza a detto articolo avverrà, comunque, sempre dietro presentazione di istanza d'acquisizione da parte del pubblico ministero il quale dovrà darne notizia entro 24 ore al giudice che convaliderà l'istanza nelle 48 ore successive. Senza il rispetto delle seguenti garanzie le risultanze delle acquisizioni non saranno processualmente utilizzabili.
A norma del successivo art. 7 del decreto, l'esercizio dell'attività di internet-cafè, sia che i terminali siano collocati in esercizi pubblici che in circoli privati, sarà soggetta ad apposita licenza da parte del questore. Dovrà richiedere tale licenza anche chiunque possieda, all'interno del proprio esercizio, più di tre terminali connessi ad Internet, sebbene non offrano connettività al pubblico.

4. Alcune considerazioni conclusive.

Il terrorismo e la diffusione di materiale pedo-pornografico in Internet sono i due elementi che, da diversi anni, sono alla base di un'azione normativa volta a reprimere i comportamenti in rete e le possibilità di utilizzo delle tecnologie. Sono due problemi

gravissimi, che devono essere contrastati con estremo vigore, ma sempre tenendo a mente i diritti di libertà e la tutela della privacy degli utenti.
In tema di pedo-pornografia, scriveva Rodotà, già nel 1997, sulla Rivista *Telèma*, le seguenti, chiare, frasi, al fine di descrivere simili tipi di azioni normative (Rodotà, 1997): "Non si può certo trascurare la formidabile capacità moltiplicatrice di un mezzo come Internet, insieme alla (relativa) facilità di accesso. Ma fenomeni come la diffusione di materiale pornografico e, soprattutto, la facilitazione della pedofilia non nascono, né si intensificano per il solo avvento di Internet. Se è giusto che governi e istituzioni internazionali si preoccupino del rischio di avere 'paradisi telematici', dove collocare informazioni sfuggendo ai divieti nazionali, altrettanta attenzione non viene dedicata al fatto che i paradisi della pedofilia esistono già, sono reali e non virtuali, sostengono l'industria turistica di più d'un Paese".
Le tre "P" – Pornografia, Proprietà e *Privacy* – sono le tre motivazioni principali per regolamentare e, in alcuni casi censurare, Internet: scrive Rodotà che "Volendo schematizzare assai, si può dire che oggi siano tre i condizionamenti più evidenti e le spinte maggiori per una regolamentazione giuridica di Internet, simboleggiati da tre P: Pornografia, Proprietà, Privacy. Riproducendo un vecchio schema, mille volte utilizzato per aprire la strada alle più diverse forme di censura, si mette l'accento sulla capacità corruttrice di Internet. Si elencano siti dove è possibile trovare materiale pornografico. Ormai quasi non v'è fuga di ragazzine che non venga collegata, dai mezzi di informazione, a contatti stabiliti su Internet".
Quali sono, allora, in definitiva, le strade corrette da percorrere per mettere a punto una disciplina che non fornisca pretesto per applicare regole censorie o di palese violazione della privacy e delle garanzie processuali? Secondo Rodotà, sarebbero necessari tre aspetti: " 1) inquadrare ogni azione rivolta specificamente al settore telematico in una strategia di carattere globale; 2) individuare comportamenti ritenuti assolutamente inaccettabili, come la pedofilia o altre gravi forme criminali, e perseguirli sempre e comunque con la massima severità; 3) rispettare, negli altri casi, la libertà di scelta individuale, anche in casi sgradevoli come la pornografia, sempre con il limite della tutela dei minori".
Il terrorismo è, in conclusione, uno di quei settori dove il legislatore, sovente, ha dimenticato simili principi e, soprattutto, stenta a comprendere la reale natura del mezzo telematico e, soprattutto, le influenze benefiche che internet può avere nella lotta al terrore.
Ciò comporta un quadro normativo che, con il pretesto di reagire a situazioni contingenti (e sovente già avvenute) si rivela impreciso, inefficace e inapplicabile e, soprattutto, che limita lo sviluppo delle nuove tecnologie.

BIBLIOGRAFIA

Musacchio V. (2005), *Internet and international terrorism: a dangerous association*, in *Ciberspazio e Diritto*, Vol. 6, n. 3, september 2005, pp. 415 – 422

Portesi S. (2004), *Potential application of advances in technology to prevention and response to cases of terrorism and criminality: the role of information and communication technologies*, in *Ciberspazio e Diritto*, Vol. 5, n. 2, july 2004, pp. 159 – 183.

Rodotà S. (1997), INTERNET, né censura né anarchia selvaggia, articolo pubblicato su Telèma, primavera 1997, e riportato anche su http://www.geocities.com/centrotobagi/news2.htm

Strano M., Negre B., Galdieri P. (2002), *Cyberterrorismo – L'impiego delle reti telematiche da parte del terrorismo internazionale*, Jackson Libri, Milano, 2002.

Verton D. (2003), *Ghiaccio sporco – La minaccia invisibile del cyberterrorismo*, McGraw-Hill, Milano, 2003.

Weimann G. (2004), How modern terrorism uses the Internet, Report dello *United States Institute of Peace*, all'indirizzo web http://www.usip.org/