

# Il terrorismo e l'informatizzazione in Rete

Rosa Cosola

Abstract: In this paper the Author focuses one of the most relevant aspect of the Information Warfare: the use of the Internet against Terrorism. After the 11<sup>th</sup> September some laws was enforced to fight Terrorism, but what about the fundamental right to anonymity? Here are some suggestions on how to balance this contrast.

SOMMARIO: 1. Cosa si intende per terrorismo. – 2. Le relazioni tra terrorismo e rete informatica. 3. La tecnologia contro il terrorismo: la sorveglianza globale. – 4. Come è intervenuto il diritto: a) negli U.S.A. b) in Italia. 5. Le libertà contestate: il diritto di restare anonimi. - 6. Conclusioni.

## *1. Cosa si intende per terrorismo*

Il tema che si affronterà in questo saggio riguarda la correlazione tra terrorismo e informatizzazione, soprattutto per quel che riguarda la Rete.

Prima di addentrarci nell'analisi specifica dell'argomento, credo sia opportuno fare un breve cenno su come il terrorismo viene inteso.

La parola viene dal latino *terrere*, “far tremare”, ed è entrata nel linguaggio comune nel senso politico di “assalto all'ordine pubblico e civile”; infatti il terrorismo ha lo scopo di terrorizzare.

Perciò la reazione alla violenza, la paura che il terrorismo provoca viene fornita da noi in quanto testimoni e non dalla parte che ha commesso l'atto.

Siamo noi che etichettiamo questi atti di violenza come terrorismo, atti pubblici di violenza commessi senza un chiaro obiettivo militare e che suscitano un diffuso sentimento di paura.

Il terrorismo viene frequentemente associato a gruppi di emarginati che cercano disperatamente di ottenere un brandello di potere o di influenza.

Pur non avendo la stessa capacità di uccidere su larga scala che hanno i Governi, questi gruppi, grazie al numero ridotto dei militanti, all'alto grado di dedizione alla causa e alla loro assoluta imprevedibilità, sono in grado di esercitare un'influenza largamente sproporzionata rispetto alle loro esigue risorse militari.

Alcuni di loro si battono per cause esclusivamente laiche, molti sono spinti da motivazioni religiose. Un primo problema viene sollevato dallo stesso termine terrorista: il termine non distingue chiaramente gli organizzatori di un attacco da coloro che lo eseguono e dai molti che lo sostengono. Sono tutti terroristi o solo alcuni di loro?

In realtà la linea che separa i terroristi dai loro sostenitori è molto sottile.

Non è neppure sicuro che esista una realtà chiamata “terrorista” finché qualcuno non trama per commettere un atto terroristico.

Ogni società è formata da individui sociopatici che provano un piacere sadico nell’uccidere, ma sono pochi quelli coinvolti in questi eventi programmati che prendono il nome di “terrorismo”.

Anche se molti individui coinvolti nel terrorismo sono affetti da problemi mentali, molti appaiono ben inseriti socialmente.

Infatti il vecchio detto che recita “quello che per qualcuno è un terrorista per qualcun altro è un combattente per la libertà” ha un fondo di verità.

Gli attivisti religiosi militanti e i loro sostenitori per descrivere l’operato del loro gruppo non usano il termine “terrorista”, ma “combattente”.

Non è solamente una questione semantica, perché usare o no il termine terrorismo per descrivere atti violenti è direttamente legato a ritenere o meno questi atti giustificati.

Il terrorismo è raramente un atto isolato: perché esso abbia successo, è necessaria una comunità di supporto e, in molti casi, una grande rete organizzativa.

Ci vuole anche una grande dose di presunzione morale da parte di chi commette questi atti, per giustificare la distruzione di proprietà su scala così imponente o per condonare un brutale attacco alla vita altrui, soprattutto per qualcuno che non si conosce, e ci vogliono anche una buona dose di convinzione interna e il riconoscimento sociale da parte di un’associazione legittimante e di un’autorità rispettata.

C’è una caratteristica significativa in queste culture dedite al terrorismo: la percezione che la loro comunità sia già sotto attacco e che le loro azioni non siano altro che una risposta alle violenze che stanno subendo.

I catastrofici eventi al World Trade Center e al Pentagono, le bombe alle ambasciate americane in Africa, all’edificio federale di Oklahoma City, non sono semplici atti di violenza, ma sono atti di violenza spropositata.

Gli obiettivi spesso sono stati scelti per l’immagine di familiarità e sicurezza che offrono: centri commerciali, mercati o posti di grande transito di gente: questi esempi di violenza sono stati costruiti come in un teatro.

Che senso hanno queste forme così teatrali di violenza?

Una possibile risposta risiede nel vedere la violenza come elemento di un piano strategico, e non come un gesto affidato al caso o alla follia.

Il punto più appropriato da dove cominciare è la scena, il luogo dove gli atti vengono commessi. Quando i membri di Al- Qaeda hanno cercato un luogo da colpire per esprimere il loro risentimento contro gli Stati Uniti e il loro potere militare ed economico, hanno scelto il World Trade Center, che si era rilevato il luogo più adatto per una serie di ragioni simboliche: gli edifici più alti di New York che ospitavano le sedi centrali di imprese internazionali e grosse corporation finanziarie.

L’America, più di ogni altra nazione, è stata insignita del ruolo di nemico primario da parte degli attivisti.

Come gli attacchi dell’11 settembre hanno dimostrato, nell’ampia cerchia di bersagli rientrano gli uomini d’affari, la cultura e il sistema americano.

La ragione fornita da Osama bin Laden sul perché considera l’America un nemico mondiale va ricercata, a suo dire, nella lunga lista di crimini che ha commesso, tra cui il fatto che occupa le terre dell’Islam, depreda le loro ricchezze, detta ordini ai loro

governanti e umilia la gente. Sarebbe quindi compito di ogni musulmano, in nome di Dio, uccidere gli americani e depredate le loro ricchezze.

## 2. *Le relazioni tra terrorismo e rete informatica*

I terroristi usano molto i *media* perché le informazioni girano più veloci e, grazie al loro aiuto, possono sapere subito quale reazione determinerà un avvenimento sulla gente.

Internet permette ai terroristi di avere una maggiore ricchezza di informazioni, ed inoltre può essere anche un valido strumento di reclutamento. Un recente studio mette in evidenza come le organizzazioni terroristiche e i loro sostenitori abbiano utilizzato tutti i sistemi tecnologici che offre la Rete per reclutare i propri adepti.

Internet ha ampliato significativamente la possibilità di conseguire elementi pubblici da parte dei gruppi terroristici, i quali non solo hanno dimostrato di avere molta abilità con il *marketing on-line*, ma si sono anche dimostrati particolarmente esperti nel tradurre informazioni da più di un milione di siti che si occupano di telegrafia e crittografia mondiale.

Per mezzo di Internet possono addivenire alla localizzazione dei loro obiettivi, come servizi di trasporto, edifici pubblici, aeroporti, porti, proprio allo stesso modo dei servizi antiterroristici. Secondo il segretario della difesa Donald Rumsfeld, un manuale di “intrattenimento” di Al Qaeda, ritrovato in Afganistan, recitava ai suoi lettori che è possibile riunire quasi il cento per cento di tutte le informazioni che riguardano il nemico, attraverso l’uso di fonti pubbliche e senza ricorrere a metodi illegali.

Un computer di uno dei membri di Al-Qaeda, sequestrato alcuni mesi fa, conteneva tutti i dettagli riguardanti la struttura architettonica di una diga, dettagli che erano stati raccolti in rete e che avevano permesso agli ingegneri e ai progettisti di Al-Qaeda di simulare delle falle catastrofiche. Un altro computer sequestrato dagli investigatori statunitensi conteneva tutta una serie di istruzioni raccolte, sempre navigando in Rete, su come interrompere digitalmente il funzionamento delle reti di energia, acqua, trasporti e comunicazione.

Allo stesso modo, altre organizzazioni politiche e gruppi terroristici utilizzavano Internet per raccogliere fondi: Al-Qaeda dipende economicamente, in larga misura, dalle donazioni fatte mediante la rete attraverso società beneficiarie, associazioni non governative e no profit e altre associazioni finanziarie che dispongono di siti Internet. Inoltre è di dominio pubblico che i membri di Al-Qaeda si servirono per lo più di Internet per progettare e coordinare gli attacchi dell’11 settembre.

Il computer di Abu Zubayda, terrorista appartenente al gruppo, si dice che contenesse il piano di azione degli attentati alle Twin Towers e al Pentagono e che gli agenti federali trovarono migliaia di messaggi codificati prelevati da un sito Web protetto da un codice segreto.

Si evince, quindi, come Internet oggi non è soltanto un luogo di informazione, comunicazione, commercio e cultura, ma anche un luogo di attivismo politico che ha facilitato il diffondersi delle “cyber protest”, le quali coinvolgono non necessariamente interessi politici, ma problemi più ampi come quelli sociali e religiosi.

Se, fino ad oggi, i fatti del mondo tangibile hanno prodotto danni ben più ingenti di quelli del mondo virtuale, potrebbe non essere così in futuro.

Infatti, fra Israele e Palestina si combatte già da tempo un'altra guerra, quella informatica.

Il 6 ottobre 2000, con una sorprendente e strana coincidenza con la violenta guerriglia nelle regioni, subirono danneggiamenti 40 siti Web israeliani e 15 palestinesi.

Successivamente, gli hackers palestinesi colpirono ogni tipo di sito israeliano che fossero capaci di compromettere, spesso distruggendoli con messaggi tipo: "free palestine" o "free Kashmir".

Dalla guerriglia urbana condotta con strumenti rudimentali, si passa ad una guerra informatica dove Paesi poveri e poco evoluti socialmente, sono capaci di condurre una guerra informatica con virus e strumenti altamente tecnologici che li rendono identici per potenzialità offensive ai Paesi occidentali.

Fra occidente e oriente vi sarà sicuramente una disuguaglianza che riguarda il mondo tangibile, infatti l'occidente è più evoluto socialmente, economicamente, militarmente e una guerra compiuta con mezzi tradizionali, difficilmente proclamerà vincitori i paesi dell'oriente.

Le cose stanno diversamente per quel che riguarda il mondo virtuale.

Un'analisi approssimativa e superficiale, potrebbe far credere che l'essere produttori e utilizzatori delle nuove tecnologie rappresenti un insuperabile muro tra il mondo occidentale e quello orientale, ma non è così perché questa apparente evoluzione costituisce il nostro punto debole.

Quello che sorprende è che i popoli considerati meno evoluti come Palestina, Pakistan, Afganistan, vincono e vinceranno contro avversari che da sempre sono considerati potenze informatiche del Paese.

La nostra società, ormai, ha organizzato tutti i servizi pubblici essenziali come l'energia elettrica, le telecomunicazioni, l'economia, il traffico aereo, sotto l'egida delle nuove tecnologie e, quindi, una guerra informatica condotta contro uno solo di questi servizi, porterebbe il panico e il blocco totale dell'intera attività civile di un Paese.

Tutto questo, se per un verso ci permette di essere più rapidi, di interagire di più e meglio, dall'altro manifesta inesorabilmente il nichilismo del XX secolo: tutto ciò che era non è più... e tutto ciò che è potrebbe non essere.

Ed è proprio questo che si è verificato l'11 settembre a New York: i gruppi terroristici hanno assunto di colpo il ruolo di nuovi attori globali in concorrenza con gli Stati occidentali, all'economia e alla società civile.

Le reti terroristiche, in quanto organizzazioni decentrate e transnazionali, si servono di Internet ponendo fine al monopolio del potere. Questo significa che il terrorismo transnazionale non è vincolato necessariamente al terrorismo islamico, ma può legarsi a qualsiasi possibile obiettivo, ideologia e fondamentalismo.

La potenza delle azioni terroristiche aumenta in presenza di una serie di condizioni: con la vulnerabilità della nostra civiltà, con la presenza globale della minaccia terroristica e con la stessa disponibilità dei terroristi ad eliminarsi.

Inoltre, come abbiamo constatato, il terrorismo aumenta in modo esponenziale la sua potenzialità con il crescere del nostro progresso tecnologico.

La differenza tra questo nuovo terrorismo tecnologico e le armi atomiche di una volta, è notevole.

Si tratta di innovazioni basate su conoscenze che possono essere facilmente diffuse e che si modificano continuamente, sfuggendo a quella opportunità di controllo e monopolio da parte dello Stato, cui invece sono soggette le armi atomiche e chimico-biologiche.

Delegare agli individui l'azione contro gli Stati significherebbe, quindi, aprire politicamente un vaso di Pandora, in quanto non verrebbero solo abbattuti i muri esistenti tra militari e società civile, ma anche quelli tra innocenti e colpevoli.

Finora la legge ha fatto una distinzione netta tra queste categorie, ma se incombesse l'individualizzazione del conflitto, toccherebbe al cittadino dimostrare di non essere pericoloso, perché in queste circostanze tutti sarebbero sospettati di essere potenziali terroristi.

Ognuno di noi dovrebbe quindi accettare di essere controllato per motivi di sicurezza anche non avendo dato adito a nessun sospetto concreto. In questo modo l'individualizzazione della guerra finirebbe per condurre alla morte della democrazia.

### **3. La tecnologia contro il terrorismo: la sorveglianza globale**

Verso la fine degli anni Ottanta gli Stati Uniti coinvolsero la Nuova Zelanda in un nuovo e segretissimo progetto di spionaggio e monitoraggio globale: ECHELON.

Progettato e amministrato dalla NSA, il sistema ECHELON è nato per intercettare normali e-mail, fax, telefax, e telefonate che viaggiano nella rete di telecomunicazione mondiale; esso fu progettato principalmente per obiettivi non militari quali Governi, organizzazioni, aziende, gruppi ed individui in ogni parte del mondo.

Il sistema lavora indiscriminatamente intercettando grandissime quantità di comunicazioni, ed usando i computer è in grado di estrarre messaggi di qualsiasi tipo. I computer posti nelle stazioni del sistema ECHELON cercano, tra milioni di messaggi intercettati, quelli contenenti le keywords (parole chiave) precedentemente inserite.

Le keywords includono tutti i nomi, le località, i soggetti che potrebbero essere contenuti nei messaggi intercettati.

Ogni parola di ogni messaggio viene scansionata automaticamente, sia che il telefono o il fax siano nelle liste di quelli da controllare, ma anche nel caso provengano da qualsiasi altra utenza.

I computer in giro per il mondo che formano il network ECHELON sono chiamati "dizionari" e sono connessi fra di loro permettendo ai cinque paesi firmatari del UKUSA Strategy Agreement (USA, UK, Canada, Australia e Nuova Zelanda) di funzionare come elementi di un sistema integrato.

Una delle principali caratteristiche di ECHELON è costituita da una serie di stazioni orientate sui satelliti di comunicazione internazionale (Intelsats) usati dalle compagnie telefoniche di molti Paesi. Un anello formato da questi satelliti è posizionato in orbita stazionaria intorno al mondo (all'altezza dell'equatore), e ognuno di questi satelliti serve come trasmettitore per decine di migliaia di chiamate telefoniche, fax, e-mail.

Oltre alle comunicazioni radio e satellitare, l'altro maggiore metodo per trasmettere grandi quantità di comunicazioni è costituito da una combinazione di cavi sottomarini che attraversano gli oceani e reti a microonde sulla terraferma.

Pesanti cavi posti sul fondo marino si fanno carico del grosso delle comunicazioni internazionali del mondo. Le reti a microonde, invece, sono costituite da una catena di tralicci di antenne che trasmettono messaggi per tutto il paese.

L'intercettazione di quest'ultime dà la possibilità di accesso alle comunicazioni internazionali sottomarine, e una volta che queste escono in superficie, anche a quelle attraverso i continenti.

Sono anche un bersaglio per intercettazioni di comunicazioni nazionali tra persone.

Anche i ministri europei degli interni e della giustizia e i più alti funzionari della sicurezza stanno lavorando per l'elaborazione di un sistema di sorveglianza totale simile ad ECHELON.

Il consiglio UE e l'Enfopol si sono impegnati a redigere un sistema di sorveglianza e di intercettazione sull'Europa e sul resto del mondo, e secondo l'istituto britannico Statewatch, esistevano già accordi segreti sotto forma di "Memorandum of Understanding Concerning the Lawful Interception of Telecommunication".

Ufficialmente gli accordi servono alla lotta contro i grandi criminali ed alla protezione della sicurezza nazionale. Questi accordi mirano a creare un sistema di registrazione automatica e scambio di informazioni sia tramite e-mail, telefono fax.

I dati dovrebbero essere analizzati, stimati e poi trasmessi alle istituzioni interessate.

I progetti di sorveglianza e controllo globale, sono stati sviluppati nel 1991 nell'ambito della conferenza TREVI (Terrorism, Radicalism, Extremism, Violence) durante la guerra del golfo dai ministri dell'UE per poi concretizzarsi nel 1993 a Madrid.

Le iniziative dell'UE/FBI erano giunte alla conclusione che con la liberalizzazione dei mezzi di comunicazione un controllo classico dei sistemi stessi non fosse più possibile. Da questa evenienza è nata la necessità di:

- incorporare metodi e tecniche di intercettazione nelle costituzioni dei Paesi dove si era verificata una liberalizzazione dei sistemi di telecomunicazione,
- l'obbligo per gli operatori privati di adattare i loro sistemi a misure illimitate di intercettazione,
- spingere gli operatori di comunicazione telefonica a collaborare ovunque e sempre con la polizia,
- uno sviluppo di quelle tecnologie che permettono l'intercettazione da ogni parte del mondo,
- convincere il maggior numero di paesi a sottoscrivere questi accordi.

I Paesi non disposti ad accettare queste condizioni, vengono comunque sorvegliati contro la loro volontà, visto che le tecniche di intercettazione sono già incorporate nei sistemi di intercettazione esistenti.

#### *4. Come è intervenuto il diritto: a) negli USA*

Le capacità informatiche di certi gruppi islamici, fra i quali Al-Qaeda, sono state recentemente messe in luce da un rapporto della CIA in cui si afferma che vari

gruppi terroristici stanno diventando più esperti nell'utilizzo delle tecnologie informatiche e di Internet.

Ed è proprio in virtù di questo fenomeno che in seno al DARPA (Defence Advanced Research Project Agency) fu istituito un nuovo ufficio denominato IAO (Information Awareness Office) che aveva il compito di curare lo sviluppo di tredici programmi.

Uno di questi, il più importante, denominato TIA (Total Information Awareness) aveva il compito di rivoluzionare la capacità degli Stati Uniti a scovare, classificare e identificare i terroristi, nonché decifrare i loro piani e mettere così in grado gli Stati Uniti di intervenire tempestivamente.

In realtà, l'obiettivo finale del programma TIA era quello di incrementare il controllo sulla circolazione di informazioni e creare, conseguentemente, un piano d'assedio.

In realtà questo, come i progetti degli altri programmi, discussi in un "workshop" di alto livello nell'agosto del 2002 in California fra scienziati informatici e uomini politici, avrebbero ricevuto pesanti critiche.

Come vediamo numerose sono state, dopo quel lontano 11 settembre, le iniziative, che seppur movendosi su diversi fronti, sono sorte per combattere il terrorismo; fra queste vanno citate le numerose proposte di legge. Numerose critiche sono state mosse al Patriot Act dalle organizzazioni dei diritti civili dopo le modifiche che sono state apportate in virtù del tragico attentato al World Trade Center.

In modo particolare va ricordato il paragrafo 2230 che ha modificato l'Electronic Communication Privacy Act in tema di intercettazione e che ha richiamato l'attenzione sulla definizione di "protect computer" e che ha definito inoltre, il "computer trapasser" come un soggetto che accede ad un elaboratore senza autorizzazione e perciò non ha nessuna ragionevole aspettativa di privacy in qualsiasi comunicazione trasmessa al o dal computer protetto.

Il concetto in realtà non include una persona nota al proprietario o all'operatore che ha esercitato un potere contrattuale esistente.

Tutta una serie di altre disposizioni prevedono poi la possibilità per i providers di un servizio di remote computing o di un servizio di comunicazione elettronica offerta al pubblico, di rivelare dati o comunicazioni di utenti, purchè si verifichino determinate circostanze, ovvero qualora esista una emergenza relativa al pericolo di morte o lesioni fisiche gravi ad una qualsiasi persona.

Sicuramente la novità più rilevante a riguardo è quella inerente alla sezione 814 del Patriot Act intitolata "Deterrence and prevention of cyber terrorism" essa in realtà modifica alcune disposizioni del precedente Computer Fraud and Abuse Act.

La sottosezione prevede tre distinti comportamenti considerati gravi e che riguardano chi:

- a1) consapevolmente trasmette un programma informatico, o un codice, o un comando e come risultato di questa condotta causa danni ad un computer protetto, senza essere stato autorizzato,
- a2) intenzionalmente accede ad un computer protetto senza autorizzazione e come risultato di questa condotta, per negligenza causa danni,
- a3) intenzionalmente accede ad un computer protetto senza autorizzazione e come risultato cagiona danni intenzionalmente o negligenzemente nonché I) perdite ad una o più persone durante il periodo di un anno e che raggiunga almeno \$5000, II) la

modificazione, l'alterazione o la potenziale modifica di esami, diagnosi, trattamenti o cure relative ad una o più persone III) danni fisici a persone, IV) una minaccia alla salute o alla sicurezza pubblica, V) danni ad un computer usato da o per il governo o da organizzazioni governative al servizio dell'amministrazione della giustizia o della difesa e sicurezza nazionale. Le pene previste vanno dalla pena pecuniaria alla detenzione fino a 20 anni. Inoltre l'Act chiarisce che con il termine "computer protetto" si intende un computer usato nel commercio o nelle comunicazioni interstatali o estere degli Stati Uniti, ivi incluso anche un computer collocato fuori dal territorio nazionale, ma che comunque è usato per il commercio e per le comunicazioni con gli Stati Uniti. L'Act dichiara che il termine condanna (conviction), include una condanna in base ad uno qualsiasi degli Stati per un crimine punibile con la detenzione superiore ad un anno, mentre il termine "perdita" (loss), intende qualunque ragionevole costo per una vittima ed include il costo della infrazione, quello dell'accertamento del danno, e del ripristino dei dati e dei programmi, allo scopo di rimettere il computer nello stato in cui era prima dell'infrazione, inoltre comprende la perdita degli incassi e i conseguenziali danni che si sono verificati a causa dell'interruzione del servizio. Il termine "persona" invece indica qualsiasi individuo, istituzione, società, corporation o entità governativa o legale. L'Act prevede poi una sezione dedicata allo sviluppo delle possibili forme di cyber security, compreso un percorso formativo per il personale federale e statale. Un altro importante atto che si occupa della materia presa in considerazione è l'Homeland Security Act approvato il 19 novembre 2002 e che ha istituito il Department of Homeland Security le cui caratteristiche consistono nella considerevole espansione dei poteri delle forze di polizia, in modo che le stesse possano condurre sorveglianze elettroniche su vasta scala, incluso il monitoraggio delle intercettazioni telefoniche. L'H.S.A. stanziava \$500.000.000 per ricerche sulle nuove tecnologie che possano individuare in tempo minacce e prevenire un attacco, ed inoltre aumenta le pene già previste. Rende possibile irrorare sanzioni a vita per gli hackers catturati durante un attacco elettronico che abbia causato o tentato di causare dei decessi, mentre nel caso l'attacco abbia causato "serious bodily injury" potrebbe essere irrorata una pena pari a 20 anni di reclusione.

La nuova normativa assicura anche una nuova protezione legale agli Internet providers, come la Microsoft Network, che forniscano agli agenti governativi, informazioni circa i loro utenti durante particolari casi di emergenza. Un'altra sezione dell'H.S.A. fornisce maggiori poteri alle autorità U.S.A. per rintracciare e-mail o altro tipo di traffico via Internet durante un cyber attack senza aver ottenuto una autorizzazione giudiziaria.

### *B) in Italia*

In America la minaccia del terrorismo informatico non è fantascienza, ma realtà.

E in Italia che cosa potrebbe accadere?

Dopo i terribili attentati verificatisi in U.S.A. anche il governo italiano è intervenuto con urgenza per prendere tutte le misure idonee a contrastare il terrorismo internazionale.

Il Decreto Legge del 18 ottobre 2001 n. 374, manifesta apertamente le scelte di politica internazionale, ponendo il cittadino dinnanzi ad una serie di novità.

Interessante è la tecnica legislativa di emergenza che il legislatore ha usato e che si occupa in misura maggiore delle disposizioni processual-penalistiche anziché di quelle di diritto penale sostanziale, e questo perché da un punto di vista sostanziale non si può far altro che individuare i soggetti responsabili e aumentare la pena; difatti, le condotte terroristiche punite, erano già predeterminate nelle disposizioni esistenti nel nostro codice penale.

Per quanto riguarda invece le prove, ci si è resi conto che senza gli strumenti idonei ad intercettare le comunicazioni, ben difficilmente si renderà possibile impedire il verificarsi di nuovi attentati.

Da un punto di vista di diritto penale sostanziale, il terrorismo informatico è compiuto con condotte nuove o diverse da quelle disciplinate dal nostro codice penale?

In realtà il D.L. 374/2001, nulla prevede circa nuove condotte di terrorismo informatico, anche perché il cyber-terrorismo potrebbe contraddistinguersi dai tradizionali reati informatici, solo per i danni economici maggiori in grado di provocare.

Analizzando le disposizioni processual-penalistiche, ci rendiamo conto come l'art.4 del D.L.374/2001, prescrive la non punibilità degli ufficiali di Polizia Giudiziaria "che nel corso di speciali operazioni di polizia, previamente autorizzate, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo anche internazionale per cui procedano, anche indirettamente, acquistano, ricevono, sostituiscono od occultano denaro, armi, documenti, beni ovvero cose che sono oggetto di prodotto, profitto, o mezzo per commettere il reato, o altrimenti ostacolano l'individuazione della provenienza e ne consentano l'impiego".

Questo articolo che è uno dei più consistenti dell'intero decreto, disciplina la cosiddetta attività sotto copertura.

Nell'elencazione di attività sotto copertura che l'agente può compiere manca la possibilità di "attivare siti nella rete di comunicazione".

Tale attività è richiamata in modo poco preciso, nel secondo comma dello stesso articolo, ovvero: "gli ufficiali ed agenti di Polizia Giudiziaria possono utilizzare indicazioni di copertura anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazioni, informandone il pubblico ministero entro le 48 ore successive all'inizio dell'attività".

Vediamo come questo secondo comma evidenzia la minore probabile utilizzabilità di questa attività di indagine. In realtà, stando ai fatti che si sono verificati, non si dovrebbe sminuire questo tipo di attività di indagine, perché il fatto che un uomo come Jamal Beghal ad esempio, addestrato in Afghanistan e leader del commando, stava preparando un attentato all'ambasciata americana di Parigi, istruendo il suo gruppo affinché tutte le comunicazioni fossero fatte attraverso la rete, è cosa che deve far riflettere.

E forse entrare in contatto con i soggetti all'interno delle reti di comunicazione è fondamentale per la lotta al terrorismo.

Ciò diventa ancora più importante in quanto è dimostrato come i terroristi utilizzino la tecnica della stenografia per comunicare tra di loro, una vera e propria scienza che consente di nascondere all'interno di file digitali, ogni tipo di messaggio segreto invisibile ad occhio nudo ma decodificabile per chi lo conosce o ha imparato a riconoscerlo.

Si può comprendere così, l'importanza delle intercettazioni "preventive", disciplinate dall'art.5 del D.L. contro il terrorismo internazionale.

Il suddetto articolo permette l'intercettazione di comunicazioni o conversazioni anche per via telematica, ma tale attività di prevenzione deve essere eseguita per una durata massima di quaranta giorni, prorogabile una sola volta per venti giorni.

A questo punto è lecito chiedersi, ma questo termine massimo sarà sufficiente?

Solo l'utilizzo ce lo potrà confermare, ma è certo che non è la durata, ma le modalità e i mezzi con cui tali attività vengono eseguite a garantire la riuscita delle indagini.

L'esistenza e la promulgazione di diversi atti legislativi nelle diverse nazioni, ci fanno pensare e riflettere su come il terrorismo informatico, in realtà, non è cosa troppo fantasiosa, ma rappresenti un pericolo concreto.

##### *5. Le libertà contestate: il diritto di rimanere anonimi*

Che la grande rete telematica sia un importante mezzo di comunicazione fra i terroristi e uno strumento attraverso il quale compiere anche il così detti cyber-attack, non è più una remota possibilità, ma viene da pensare che una legislazione emanata dall'Amministrazione Bush e non solo, ma anche nell'ambito dell'Unione Europea, rappresenti una reale minaccia per tutti i diritti di libertà e di manifestazione del pensiero dei cittadini, tra i quali anche il diritto di rimanere anonimi. Da sempre l'anonimato ha rappresentato una condizione fondamentale per la libertà di parola e di espressione degli individui, diritto importantissimo e riconosciuto da tutti i governi democratici. Voci irriverenti verso il potere di maggioranza, si sono fatte sentire grazie alla copertura dell'anonimato, infatti, molti uomini che temevano di essere perseguitati a causa dei loro pensieri, hanno così avuto modo di esprimere le loro opinioni liberamente e senza temere ritorsioni. Nonostante queste condizioni più o meno diffuse, la situazione di Internet è vista in modo piuttosto diversa: la rete viene spesso vista come una realtà sui generis, in quanto molti governi, soprattutto negli ultimi anni, cercano di limitare o eliminare completamente l'anonimato e quindi la libertà di espressione in rete.

Ovviamente, questa inversione di marcia, rappresenta il riflesso di quell'ansia di sicurezza che circola nella società europea e in quella americana e che è stata alimentata dal timore che gli autori degli attacchi a New York e Washington, abbiano usato Internet per preparare gli attentati.

Infatti dopo quel tragico evento il senato americano ha approvato una serie di provvedimenti che permettono agli agenti del F.B.I. di spiare gli utenti di Internet senza autorizzazioni giudiziarie. Provvedimenti presi sull'onda dell'emozione, ma che hanno trovato terreno fertile, vista l'insistenza con cui negli anni scorsi, gli apparati di sicurezza americana hanno gonfiato i pericoli legati ad Internet per ottenere più poteri di sorveglianza e maggiori finanziamenti.

Si capisce quindi, come il primo prodotto di questa isteria di sicurezza, è che i fornitori di accesso alla rete, gli Internet service providers, hanno messo da parte le storiche resistenze nei confronti della polizia e hanno cominciato a collaborare col F.B.I. per monitorare il traffico Internet utilizzando il sistema Carnivore, un sistema

in grado di copiare tutto il traffico Internet, web, chat, e-mail che transita attraverso le loro macchine.

Tuttavia poiché è possibile eludere qualsiasi programma di intercettazione criptando le informazioni critiche, vengono proposti ulteriori limiti sui programmi di crittazione dei dati che permettono a qualsiasi cittadino di celare le proprie comunicazioni, senza perciò essere un terrorista.

Questi segnali sembrano preludere ad un ulteriore controllo delle rete, tentativo precedentemente fallito grazie alle mobilitazioni delle associazioni per i diritti civili.

Si tratta, comunque, di iniziative su cui gli stessi esperti esprimono dei dubbi, in quanto chi vuole rimanere anonimo sulla rete, usa i web anonymizer, mentre chi vuole scambiare messaggi senza farsi riconoscere, può farlo attraverso gli *anonymus remailers*.

E' il caso, ad esempio, di chi vuole denunciare un fatto di mafia, uno stupro o un abuso, senza subire rappresaglie.

Mentre chi vuole essere sicuro che i suoi messaggi vengano letti da un preciso destinatario e solo da quello, per proteggere i dati sensibili, usa i software di cifratura in codice come il Pgp.

Ma poiché i software di crittografia possono essere utilizzati anche da chi vuole commettere reati, la polizia federale propone una restrizione di questo tipo di produzione tecnologica, e l'installazione di una *backdoor* governativa, ovvero una finestra di controllo sugli stessi programmi di crittografia.

La crisi di questa ricerca in realtà potrebbe portare una serie di conseguenze negative a catena, in quanto oggi, la crittografia viene utilizzata anche per garantire la sicurezza delle infrastrutture nei cyber-attack o nelle comunicazioni fra le forze di polizia, in quanto la polizia stessa ne ha incoraggiato l'uso per proteggere informazioni pubbliche o che riguardino violenze, sparizioni e rapimenti.

Inoltre le tecnologie di crittazione vengono utilizzate per scambi finanziari e commerciali e quindi una restrizione del loro utilizzo danneggerebbe le su dette attività.

Quindi da ciò deriva che il potenziale uso della crittografia da parte dei terroristi, andrebbe contrastato con la creazione di codici di decrittazione e operazioni mirate di intelligence, utilizzando, magari, altri dati per individuare i sospetti e solo allora avviare un attacco per rompere il codice di crittazione usato. Infatti la *defaillance* dei sistemi di sicurezza statunitensi è da imputare in realtà al "fattore umano" e quindi al mancato coordinamento dei servizi stessi.

## *6. Conclusioni*

Da un punto di vista strettamente telematico, la tragedia dell'11 settembre non può costituire un pretesto per mettere insieme sistemi di monitoraggio nel tentativo di limitare le libertà individuali e collettive di espressione in nome di una maggiore sicurezza che in realtà non esiste e mai esisterà, perché se la C.I.A., F.B.I., ECHELON, N.S.A., non hanno saputo, prima dei tragici attentati, analizzare le informazioni in loro possesso e valutarne la precisa attendibilità, cosa succederà un

domani quando questo mare di informazioni diventerà un oceano difficile da governare?

Semplice: ancora più informazioni, magari strategiche, passeranno inosservate insieme alle altre. Quindi il vero problema dal punto di vista della sicurezza non è mantenere in piedi servizi che quando non organizzano omicidi e stragi politiche, ne sono obbiettivamente conniventi, ma cercare di affrontare le questioni con un più diffuso senso politico.

E' arrivato il momento di rilanciare un senso politico della sicurezza, ma anche un senso sociale della stessa, cercando di diffondere quei modelli sociali di comunanza che possono essere i soli garantiti per la serenità del nostro vivere quotidiano, cercando di avvicinare la gente ad un senso comune di fratellanza ed eliminando ogni sorta di barriera.