ANDREA DE PETRIS

IL *PATRIOT ACT* E LE LIBERTÀ DIGITALI

SOMMARIO: I.1. Le peculiarità della sicurezza pubblica in ambito informatico. — I.2. Definire il problema: come proteggere società aperte ed altamente tecnologiche? — I.3. Le principali forme di rischio per le tecnologie informatiche: dalla Internet-propaganda al cyberterrorismo. — I.4. La distinzione tra dissenso e guerra: una precisazione. — I.5. La prospettiva giuridica. — II.1. Lo USA PATRIOT Act ed il suo impatto sulle libertà digitali. — II.2. La distinzione tra sorveglianza investigativa esterna e sorveglianza interna. — II.3. L'incremento dei poteri di indagine del Governo nel Cyberspazio. — II.3.1. Estensione ai reati terroristici ed informatici del nuovo regime di sorveglianza elettronica: il fenomeno *Hacking*. — II.3.2. *Pen Register* e *Trap and Trace Orders* (USAPA §§ 214, 216). — II.3.3. Accesso ad informazioni ed altri beni materiali (§ 215 USAPA). — II.3.4. Intensificazione nell'utilizzo delle disposizioni di *Subpoena* (§ 210 USAPA). — II.3.5. Intercettazione di messaggi in voce emessi ed archiviati (§ 209 USAPA). — II.3.6. La « *National Security Letter* » (§ 505 USAPA). — II.4. Espansione dei poteri di soggetti privati. — II.4.1. Autorizzazione delle vittime di fenomeni di *Hacking* a condurre indagini proprie (USAPA § 217). — II.4.2. Rivelazioni di emergenze da parte di *Internet Provider* (§ 212 USAPA). — II.4.3. *Clarification of Scope of Cable Act*. — II.5. Altre disposizioni del *Patriot Act* riguardanti la privacy nel cyberspazio. — II.5.1. *Warrants* « *Sneak and Peek* » (§ 213 USAPA). — II.5.2. L'esperibilità delle misure di *Warrant* in qualunque distretto giudiziario (§§219, 220 USAPA). — II.5.3. Intercettazioni itineranti (*Roving Wiretapes*) (§ 206 USAPA). — II.6. Disposizioni del *Patriot Act* che estendono le capacità del Governo di ottenere accesso ad informazioni private. — II.6.1. Definizioni più ampie del reato di attività terroristica. — II.6.2. Riduzione delle tutele previste nel processo penale. — II.6.3. Incremento dei poteri della CIA. — II.6.4. Aumento di spesa per la sorveglianza informatica. — II.7. Altri provvedimenti dell'Amministrazione USA in materia di sorveglianza elettronica. — III.1. Le reazioni alla reazione: oltre il *Patriot Act*. — III.2. Il ruolo dei giudici. — III.3. Le risposte della politica. — III.4. Il *Patriot Act* oltre il « viale del tramonto ».

I.1. Le peculiarità della sicurezza pubblica in ambito informatico.

Sebbene fondata su criteri e valori tipici della più generale regolamentazione del rapporto tra sicurezza e diritti, la necessità di contemperare la tutela dell'incolumità pubblica con la difesa delle libertà fondamentali nello speciale contesto informatico non può essere soddisfatta richiamandosi a convinzioni e modalità di intervento normalmente in uso in ambiti tradizionali.

Nessuna delle attività abitualmente esercitate da un membro della cosiddetta « Società dell'Informazione » — volendo con ciò intendersi le società contemporanee altamente tecnologizzate ed informatizzate[1] —, è infatti in grado di coinvolgere contemporaneamente tutte le sfere di interesse di un individuo nella misura in cui questo accade nella navigazione in Internet. È noto, infatti, come attraverso il collegamento alla Rete sia oggi possibile esercitare un catalogo pressoché infinito di attività, il cui carattere spazia dall'ambito prettamente lavorativo-professionale a quello tipicamente ludico, da quello economico e commerciale a quello sociale, in una varietà di contesti nella quale la dimensione pubblica e quella privata degli interessi individuali convergono in un'unica sfera mediatica.

Conseguentemente, ogni tipo di intervento in detto contesto — a prescindere dalla sua liceità e dagli obiettivi che esso si prefigge — si traduce inevitabilmente *anche* in una pesante intrusione nell'ambito dei diritti fondamentali che tali interessi riconoscono e tutelano. Il pensiero va in primo luogo al diritto alla riservatezza dei dati personali, alla libertà di informazione e di manifestazione del pensiero, ma anche al diritto di associazione e riunione, per il cui esercizio la comunicazione *on-line* si è ormai affermata come uno strumento pressoché indispensabile; se si allarga appena un po' l'orizzonte, tuttavia, ci si accorge come non solo il tradizionale catalogo dei diritti personali, ma anche quello di più recente definizione dei diritti economici e sociali sia ormai potenzialmente coinvolto nell'attività di navigazione sul *Web*, e dunque nella sua sorveglianza[2].

D'altro canto, proprio la capillare diffusione degli strumenti di comunicazione informatici a livello mondiale fa sì che oggigiorno la circolazione di dati avvenga ormai quasi esclusivamente per questa via: di conseguenza, l'esigenza della sicurezza dell'informazione in Rete si rivela strategicamente irrinunciabile per la stessa sopravvivenza dell'ordine globale[3]. La peculiarità del contesto in esame comporta quindi che l'espressione « sicurezza dell'informazione » vada concepita secondo una duplice accezione: quale sicurezza dei sistemi informatici da attacchi e sabotaggi, ma anche come sicurezza — intesa come salvaguardia ed affidabilità — delle informazioni fornite e di chi le fornisce. Dal momento che ogni forma di controllo della Rete si traduce inevitabilmente anche in una maggiore complessità del suo utilizzo e funzionamento, dunque, qualunque soggetto scelga di adottare provvedimenti del genere dovrebbe mantenere sempre ben presente che, così facendo, rischia di limitare anche la possibilità di azione di singoli ed organismi promotori di posizioni conflittuali nei confronti dell'ordine costituito, ma nondimeno perfettamente lecite[4].

---

[1] Per un'analisi del problema della diseguaglianza nella ripartizione delle risorse digitali (il cosiddetto « *Digital Divide* ») v. per tutti P. NORRIS, *Digital divide: civic engagement, information poverty, and the Internet worldwide*, Cambdridge University Press, Cambridge & New York 2001.

[2] Cfr. *Privacy International, Privacy and Human Rights 2002. An International Survey of Privacy Laws and Developments, 2002, passim*, in *http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf* (ultimo accesso: 5 dicembre 2006).

[3] Da ultimo sul punto cfr. R.L. POPP-J. YEN, (ed.), *Emergent information technologies and enabling policies for counter-terr*orism, John Wiley (distributor), Hoboken (N.J.) 2006.

[4] G. GEIGER, *Risiken und Chancen der Kommunikationstechnologie*, in *Sicherheitspolitik im 21. Jahrhundert*, Informationen zur politischen Bildung, Bun-

Il significato e la percezione del concetto di sicurezza hanno assunto connotazioni profondamente differenti da quelle in voga prima degli attacchi dell'11 settembre 2001: la stessa configurazione del terrorismo informatico ha conosciuto un'evoluzione, e, come si mostrerà nel corso di questo lavoro, i provvedimenti adottati contro i *cybercrimini* dalle pubbliche autorità a livello nazionale, sovranazionale e globale hanno mostrato un netto balzo in avanti in termini di severità e pervasività, accomunando nella medesima tendenza di estensione del controllo sia regimi dittatoriali ed autoritari che ordinamenti di democrazia consolidata. Nell'analizzare più da vicino queste misure, tuttavia, si avverte la sensazione che la precipitazione con la quale si è inteso rispondere alla minaccia del terrorismo internazionale dal 2001 in poi abbia pericolosamente pregiudicato l'attenzione verso l'altro piatto della bilancia, quello della tutela dei diritti individuali. A fronte dell'indefinitezza della minaccia che tali misure intendono combattere, quindi, si profila sempre più concretamente il pericolo che questo pregiudizio per uno dei poli di interesse in gioco — quello dei diritti — a favore dell'altro — quello della sicurezza — risulti al fine difficilmente reversibile, che il ripristino dell'auspicabile equilibrio iniziale rischi di rivelarsi sempre più problematico e distante.

I.2. Definire il problema: come proteggere società aperte ed altamente tecnologiche?

I fattori di rischio di società moderne ed ampiamente sviluppate sul piano tecnologico sono molteplici: si va dalla dipendenza ed *inter*dipendenza delle infrastrutture tecnologiche e dei mezzi di informazione alle profonde interrelazioni sul piano internazionale degli assetti finanziari e della produzione di energia, ai reiterati appelli alla deregolamentazione e privatizzazione dell'economia[5]. Il tutto viene complicato dal fatto che, rispetto ai pericoli convenzionali, nel caso in questione abbiamo a che fare con rischi e minacce di natura variabile e mutevole: le società aperte ed altamente tecnologizzate, pertanto, rappresentano un campo di azione estremamente attraente per organizzazioni criminali e terroristiche.

Il caso delle *Information Technologies* (IT) interconnesse a livello globale, minacciate dal crescente pericolo del cosiddetto « *cyberterrorismo* »[6], mostra chiaramente come i confini tra sicurezza interna ed esterna vadano gradualmente dissolvendosi, e come sia sempre più difficile individuare misure di sicurezza in questo ambito capaci di distinguere tra il settore economico privato e quello pubblico.

---

deszentrale für politische Bildung, Bonn, Nr. 291/2006, pp. 36-39.

[5] « È un triste dato di fatto: questa idea neoliberale,... — questa taccagneria dello Stato da un lato, e la tripartizione di deregolamentazione, liberalizzazione e privatizzazione dall'altro — ha purtroppo reso il Paese più vulnerabile da parte di attacchi terroristici ». [...] « Un Paese può anche liberalizzarsi fino alla morte », U. Beck, *Ein bewegliches Ziel*, in *Die Zeit*, 7 febbraio 2002.

[6] R. W. Hutter, « *Cyber-Terror* »: *Risiken im Informationszeitalter*, in *Aus Politik und Zeitgeschichte* 10-11/2002, pp. 31-39.

I.3. Le principali forme di rischio per le tecnologie informatiche: dalla internet-propaganda al cyberterrorismo.

Fin qui l'analisi in termini generali dello « stato dell'arte » rispetto ai pericoli che attualmente minacciano le infrastrutture telematiche. Il carattere delle operazioni informatiche, del resto, fa sì che i confini tra la sicurezza esterna ed interna, tra i compiti delle forze armate e di quelle responsabili per la sicurezza pubblica vadano sempre più scomparendo. In questo senso, si rendono necessarie nuove definizioni di funzioni e ripartizioni di competenze, mentre da più parti l'informazione viene ormai considerata alla stessa stregua di elementi come la forza, lo spazio ed il tempo rispetto alla classica conduzione dei conflitti bellici. Con tali premesse, lo scenario di una serie concentrata di iniziative coercitive apportate parallelamente dall'interno e dall'esterno contro i sistemi informatici di un governo nazionale e gli imprenditori economici e fornitori di energia appare sempre più probabile.

Da un'analisi più dettagliata dell'argomento, peraltro, emerge come in generale esistano tre categorie differenti di interventi « antagonisti » apportabili attraverso le IT, il cui carattere, tuttavia, non può essere indistintamente qualificato come aggressivo, sovversivo o criminale, dovendosi piuttosto procedere in ciascuno caso a valutazioni specifiche caso per caso prima di esprimere giudizi di merito[7].

1. *Acquisizione e sfruttamento di informazioni per via informatica*. L'informazione elettronica viene utilizzata in misura crescente per obiettivi di politica protezionistica o totalitaria, ma anche da forze terroristiche e criminali. Ciò include controlli eterodiretti all'accesso alle banche dati, filtri all'informazione finalizzati al raggiungimento di precisi obiettivi e casi di propaganda. Come esempi possono essere citati il blocco di siti *Web* considerati sovversivi da parte del Governo cinese[8], o le azioni di propaganda e contro-propaganda dei contendenti nella guerra del Kossovo, nel conflitto afgano o in quello iracheno. Ancora, in Internet vengono diffuse teorie ed idee di estrema destra o legate al fondamentalismo islamico, come i miliziani palestinesi *Hezbollah*, che sul loro sito *Web* riportano le descrizioni dei loro attacchi contro obiettivi israeliani. La Rete viene utilizzata sempre di più anche da organizzazioni, associazioni e forme di cospirazione virtuale: è il caso del Gruppo J18, che nel 1999, a margine della conferenza del G8 di Colonia, ha invitato ad un'azione coordinata contro i vertici finanziari ed i produttori di energia caratterizzata da marce, manifestazioni ed operazioni di *hacking*. Gli Stati Uniti, dal canto loro, sorvegliavano segretamente il traffico telefonico mondiale attraverso ECHELON[9]. In via

[7] D.E. Denning, *Activism, Hacktivism and Cyberterrorism*, Information axioms-papers, 1999. The Internet as a Tool for influencing Foreign Policy, disponibile on-line in *http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf* (5 dicembre 2006).

[8] In merito v. ampiamente G. Wacker, *Widerstand ist zwecklos: Internet und Zensur in China*, in: G. Schucher (Hrsg.), *Asien und das Internet*, Institut für Asiankunde, Hamburg 2002, pp. 70-96.

[9] Secondo il rapporto presentato nel maggio 2001 dalla Commissione Temporanea del Parlamento Europeo sul Sistema di Intercettazioni Echelon, insediata nel giugno 2000, ECHELON costituisce un sistema creato all'inizio della Guerra Fredda

di principio, si tratta di fenomeni non nuovi, e purtuttavia Internet fornisce a queste forme di intervento un grado di pericolosità assolutamente nuovo in termini di velocità, diffusione ed anonimità.

2. *Hacking*. Si tratta di un esempio di infiltrazione attiva nel *software* informatico e nelle banche dati, il cui spettro di azione è di ampiezza pressoché infinita[10]. Le forme più pericolose hanno come obiettivo la raccolta, la manipolazione o la distruzione di dati, spingendosi fino a provocare il collasso strutturale di grandi sistemi informatici. A questo tipo di iniziative appartengono anche i « sit-in » virtuali, ad esempio sotto forma di blocchi, i cosiddetti attacchi *Denial-of-Service*, condotti contro i *server* di Yahoo o Ebay, o come il tentativo di simpatizzanti zapatisti italiani di infiltrarsi nelle pagine *Web* del Presidente messicano Zedillo o di quello statunitense Bill Clinton, o l'attacco dei ribelli Tamil contro le ambasciate dello Sri Lanka di tutto il mondo attraverso bombardamenti di messaggi di posta elettronica nel 1998, o ancora come il ricatto perseguito dall'ETA contro un *Provider* di servizi Internet attraverso un « bombardamento elettronico », fatto di massicci e continui invii di *E-mail* ed altre forme di sabotaggio informatico, per costringerlo a ritirare delle pubblicazioni indesiderate. Lo stesso dicasi per il sistema operativo di Microsoft, penetrato da « scassinatori » virtuali per sottrarne o quanto meno esaminarne il codice di *software* utilizzato, o per il governo cinese, che si inserisce nei *Server* stranieri di seguaci della setta Falun Gong, o ancora per un appello ad una « manifestazione via Internet » contro la Lufthansa per la sua partecipazione al trasferimento coatto di cittadini stranieri, che ha portato a 1,3 milioni di contatti da parte di 12.000 indirizzi di *Internet Provider* in tutto il mondo[11]. A fronte della crescita della prossima generazione di terroristi, sembrano sempre più probabili soprattutto gli attacchi alle cosiddette « infrastrutture critiche ». Secondo informazioni raccolte dai servizi di *intelligence*, uno sparuto gruppo di seguaci di Bin Laden in Germania era in grado di condurre un attacco informatico alla Rete delle Reti. Un gruppo di *Hacker* pakistani (« G-Force ») ha attaccato l'amministrazione statunitense, minacciando di fornire a Bin Laden dati segreti del Governo di Washington se non fossero cessate le operazioni militari in Afghanistan[12].

per la raccolta di informazioni, sviluppatosi successivamente come una rete di stazioni di intercettazione diffuse in tutto il mondo, con l'obiettivo principale di captare comunicazioni private e commerciali, ma non informazioni militari. Il rapporto si conclude raccomandando a cittadini ed aziende dell'Unione Europea di intraprendere misure di « autodifesa » finalizzate alla protezione delle comunicazioni dalle iniziative di sorveglianza, cfr. European Parliament, Temporary Committee on the Echelon Interception System, Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI)), 18 maggio 2001, approvato l'11 luglio 2001, disponibile in *http://cryptome.org/echelon-ep-fin.htm* (20 dicembre 2006). Per un'approfondita analisi del fenomeno ECHELON v. soprattutto P. Radden Keefe, *Intercettare il mondo. Echelon e il controllo globale*, Einaudi, Torino 2006.

[10] Il fenomeno hacking è estremamente variegato e complesso. Per una esposizione più articolata del tema, specialmente in rapporto alle novità legislative istituite con l'emanazione dell'USA PATRIOT *Act*, v. *infra*, par. II.3.1.

[11] Gli episodi in questione sono accuratamente descritti in R.W. Hutter, *Cyber-Terror«* , op. cit., p. 34 s.

[12] R.W. Hutter, *Wie lassen sich offe-*

3. *Cyberterrorismo e Cyberwar*. Si tratta di attacchi mirati, motivati politicamente, condotti con l'ausilio di tecnologie informatiche e/o all'interno delle tecnologie informatiche stesse, con rilevanti conseguenze sulla vita e la salute delle popolazioni interessate o per la capacità di intervento economica e/o politica degli Stati, in alcuni casi — ma non necessariamente — anche con il coinvolgimento di forze armate. Spionaggio, indagini, inganni, gestione elettronica delle contrapposizioni, distruzione fisica dei sistemi informatici, attacchi all'informazione, sono tutti potenziali componenti di prossime operazioni informatiche offensive e difensive all'interno di una possibile « cyberguerra », o parti di future contrapposizioni armate. In generale, questi elementi non rappresentano una novità: la peculiarità è costituita dall'importanza e dal peso di questo tipo di operazioni nei futuri casi di conflitto. A ciò si aggiunga che, proprio a causa nel profondo grado di interconnessione dei diversi sistemi informatici, un attacco contro una particolare infrastruttura può rivelarsi fatale anche per soggetti ed apparati pubblici o privati assolutamente estranei all'obiettivo dell'attacco stesso[13].

I.4. La distinzione tra dissenso e guerra: una precisazione.

Una classificazione del genere, sebbene oggettivamente corretta e strategicamente efficace nel prospettare le diverse tipologie di minaccia che le reti informatiche pubbliche e private sono oggi chiamate a fronteggiare, porta con sé un pericolo di estrema rilevanza. Ove si considerino con attenzione gli esempi esplicativi apportati, si noterà infatti come alcune delle azioni « incriminate » perseguano obiettivi discutibili nei contenuti, ma di per sé più che legittimi sul piano democratico — a meno di non voler bollare per principio come sovversive delle forme di critica contro determinate categorie di soggetti, per lo più di carattere pubblico ed istituzionale: è il caso, ad esempio, degli atti di dissenso o dei « sit-in » virtuali condotti ai danni dei siti di istituzioni nazionali ed internazionali, per protestare contro provvedimenti politici che queste ultime hanno deciso di emanare o implementare. Rispetto a casi reali di dimostrazioni, marce ed azioni di resistenza passiva, quindi, ciò che muta, dunque, non è il contenuto o l'obiettivo dell'iniziativa, ma il contesto nel quale questa viene posta in essere. Se però tra gli esempi di *Hacking* vengono comprese anche iniziative di protesta le quali, se condotte con mezzi tradizionali e conformemente alle generali garanzie costituzionali del diritto di manifestazione del pensiero e di riunione, sarebbero probabilmente ritenute lecite, allora la loro classificazione *tout court* come una possibile minaccia alle tecnologie dell'informazione al pari delle azioni di sabotaggio a scopo di estorsione dei pirati informatici o degli attentati contro la collettività ad opera di gruppi terroristici, costituisce il primo passo per una loro criminalizzazione, e rischia ancora una volta di compromettere la difesa delle libertà individuali in nome della lotta per la sicurezza collettiva. A questo punto, appare indispensabile chiedersi se il *mezzo* scelto per la realizzazione di

ne und hochtechnologisierte Gesellschaften schützen? Das Beispiel Cyberterror, in: W. Weidengeld (Hrsg.), *Heransforderung Terrorismos. Dies Zukunft der Sicherheit*, VS Verlag für Sozialwissenschaften, Wiesbaden 2004, pp. 173-193 (187).

[13] S. Blancke, *Information Warfare*, op. cit., p. 26.

un atto possa influenzarne la percezione al punto tale da far passare in secondo piano il *fine* che esso persegue[14].

I.5. La prospettiva giuridica.

Per tutte queste ragioni, la cosiddetta « *Information Warfare* », o Guerra dell'Informazione, si rivela essere una zona grigia per la quale è assai arduo individuare gli strumenti normativi da applicare. Raramente in questo contesto l'esercizio di operazioni giuridicamente illegittime, come l'intercettazione di dati informatici, vengono a conoscenza delle istituzioni internazionali. Abitualmente, infatti, i fenomeni appena descritti vengono analizzati attentamente dal punto di vista tecnologico, mentre sono pressoché ignorati da quello giuridico: un errore principalmente strategico, a cui soprattutto i soggetti tipici della comunità internazionale, ovvero gli Stati, dovrebbero prontamente porre rimedio, dal momento che un intervento su singoli soggetti privati protagonisti di singole azioni di « guerra informatica », indipendentemente dalla portata delle loro conseguenze, sarebbe difficilmente praticabile senza il coinvolgimento dello Stato nel cui ordinamento dette azioni sono state materialmente commesse. Contrariamente alle operazioni informatiche di carattere difensivo, che possono risultare ammissibili entro una certa intensità, un attacco informatico di tipo offensivo può giustificare il ricorso all'art. 2 IV dello Statuto delle Nazioni Unite[15], che proibisce ogni forma di minaccia ed uso della forza, spettando poi al Consiglio di Sicurezza dell'ONU accertare se si sia effettivamente verificata tale fattispecie. A seguito di tale accertamento, l'art. 51 dello Statuto delle Nazioni Unite prevede il diritto all'autodifesa da parte dello Stato interessato. Il punto centrale, in questo contesto, è stabilire quando possa parlarsi di un'operazione informatica di tipo offensivo. Tradizionalmente, il diritto internazionale considera aggressione l'impiego di armi ed il ricorso alla forza militare, mentre la Risoluzione dell'ONU del 14 dicembre 1974 porta come esempi in tal senso il blocco di porti e coste e la violazione dell'integrità territoriale di uno Stato[16]. Se stanno così le cose, l'attuazione di un'azione condotta attraverso le IT potrebbe rientrare in questa tipologia di interventi, dal momento che il blocco di reti informatiche e di comunicazione sarebbe indubbiamente in grado di produrre effetti del genere, quando non più gravi[17]. Anche in un frangente simile, dunque, in via di principio sembra giustificato un intervento di autodifesa da

[14] Sul punto v. più ampiamente *infra*, par. II.3.1., II.4.1.

[15] « I Membri [dell'ONU] devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite ». Il testo integrale dello Statuto ONU è disponibile in lingua italiana in *http://www.admin.ch/ch/i/rs/i1/0.120.it.pdf* (29 novembre 2006).

[16] Cfr. N.A. Nyiri, *The United Nations » Search for a Definition of Aggression*, Resolution 3314 (XIX), Peter Lang, New York 1989.

[17] Cfr. K. Anderson, *Intelligence-Based Threats Assessment for Information Networks and Infrastructures*, Portland 1998, disponibile on-line in *http://www.aracnet.com/~kea/Papers/threat_white_paper.pdf* (5 dicembre 2006).

parte dello Stato colpito, pur non dimenticando anche in questo caso il rispetto del principio di proporzionalità e quindi tenendo ben presente l'entità del danno che l'attacco informatico ha provocato.

Se il principio può apparire pacifico, tuttavia, uno scenario del genere solleva una serie di questioni di dettaglio di non facile soluzione, quali: è possibile riconoscere inequivocabilmente aggressioni informatiche? Se ne riesce ad identificare la fonte responsabile? È legittimo rispondervi con gli stessi mezzi? Quale intensità dovrebbe avere l'azione di risposta da parte dello Stato colpito? Come dovrebbe comportarsi lo Stato vittima dell'azione, quando questa ha comportato l'uso illegittimo della rete di comunicazioni di uno Stato terzo estraneo alla vicenda? Ove lo Stato vittima dell'azione non sia tecnologicamente attrezzato in modo da potervi rispondere allo stesso modo, può esso eventualmente porre in essere operazioni difensive con mezzi militari convenzionali? Le azioni informatiche dirette contro uno Stato possono essere ritenute ammissibili dal punto di vista del diritto internazionale, dovendosi in tal caso interpretare come forme legittime di contro-informazione, oppure vanno considerate come iniziative illegittime di propaganda volte solamente ad offendere il Governo nemico o ad incitarne la popolazione alla sovversione[18]? Come si vede, dunque, la materia con cui si ha a che fare risulta particolarmente fluida e difficile da interpretare secondo canoni giuridici certi. A ciò si aggiunga la circostanza che anche soggetti non statuali, quindi ancor meno vincolati e vincolabili sul piano del diritto internazionale, tendono sempre più a servirsi di strumenti informatici per porre in essere atti di ostilità contro ordinamenti nazionali.

La reazione dei soggetti a rischio di attacchi, sia pubblici che privati, è in primo luogo quella di dotarsi degli apparati tecnologici necessari per poter resistere ad azioni informatiche su larga scala: si sviluppano così *Firewalls* (sistemi di protezione delle reti informatiche) sempre più aggiornati, o si costruiscono sistemi di comunicazione omologhi ad Internet su cui testare tanto delle operazioni di aggressione simulata che l'efficacia delle contromisure di difesa. Soprattutto gli Stati, in presenza del pericolo di attacchi informatici terroristici, tendono a chiamare in causa la « sicurezza nazionale » sia in generale che con particolare riferimento ad Internet: caso emblematico è quello degli Stati Uniti, per i quali tuttavia si è accertato che meno dell'1% degli attacchi condotti attraverso la Rete contro apparati statunitensi hanno finora avuto origine nei Paesi appartenenti al cosiddetto « Asse del Male », mentre la stragrande quantità di tali azioni è stata posta in essere su territorio statunitense ed è attribuibile ad *Hackers* tradizionali[19]. Le pesanti limitazioni dei diritti civili anche in ambito informatico prodotte dal recente USA *Patriot Act*, dunque, risultano difficilmente giustificabili[20].

---

[18] Sotto questo profilo, ad esempio, le azioni informatiche condotte dagli Stati Uniti contro l'Iraq nel corso del 2003 sollevano non pochi interrogativi di legittimità.

[19] Cfr. *Fighting the worms of mass destructions (Special Report. Internet Security)*, in *The Economist*, 29 novembre 2003, p. 75 ss., disponibile on-line in *http://www.economist.com/science/displayStory.cfm?story_id=2246018* (5 dicembre 2006).

[20] Per un'analisi dettagliata dell'argomento v. *infra*, par. II.

II.1. Lo USA PATRIOT Act ed il suo impatto sulle libertà digitali.

Lo USA PATRIOT *Act* (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, USAPA)[21] è stato approvato il 26 ottobre 2001. Il provvedimento, lungo 342 pagine e contenente emendamenti a 15 differenti leggi federali[22], è il frutto di un lavoro di elaborazione molto rapido, se si pensa che dalla presentazione della prima bozza di proposta alla sua definitiva trasformazione in legge passarono solamente cinque settimane[23]: sia nel corso dei

[21] Pub. L. No. 107-56, 115 Stat. 272 (2001). Cfr. il testo integrale del provvedimento in *http://www.epic.org/privacy/terrorism/hr3162.pdf* (29 novembre 2006).

[22] Oltre che sull'opportunità dell'acronimo scelto, il *Patriot Act* ha ricevuto forti critiche per la sua lunghezza e complessità: in effetti, sono molti i casi in cui una delle 1016 sezioni del provvedimento viene emendata nel suo significato originario attraverso modifiche, aggiunte o eliminazioni contenute in altre parti della stessa legge. Così V. Fanchiotti, *Il dopo 11 settembre e l'Usa Patriot Act: lotta al terrorismo e effetti collaterali*« , in *Questione Giustizia*, n. 2-3/2004, pp. 283-297, e L. Magliaro, *Le libertà della persone dopo l'11 settembre*, in *Questione Giustizia*, n. 2-3/2004, pp. 314-329. Sull'argomento in lingua italiana v. anche A. Manna, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la* privacy, in *Rivista italiana di diritto e procedura penale*, 2004, pp. 1024 ss.; M. Miraglia, *Paura e libertà (Legislazione antiterrorismo e diritti di difesa negli Stati Uniti)*, in *Questione Giustizia*, n. 2-3/2004, pp. 298-313; P.L. Zanchetta, *Nuove guerre, antiche violenze, perenne violazione del diritto*, in *Questione Giustizia*, n. 2-3/2004, pp. 811 ss.. Sull'evidenza della strumentalità dell'acronimo attribuito al provvedimento, chiaramente inteso a catalizzare su di esso un consenso meramente emozionale a poche settimane dagli attentati delle Twin Towers cfr. C. P. Raab, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties?*, in *Duke Law & Technologies Review* 2/2006, pp. 1-51, il quale riporta tra l'altro la sdegnata reazione del membro della Camera dei Rappresentanti Barney Frank all'acriticità con cui il Congresso ha approvato il provvedimento: « *This bill, ironically, which has been given all of these high-flying acronyms, it is the PATRIOT bill, it is the U.S.A. bill, it is the stand up and sing the Star Spangled Banner bill, has been debated in the most undemocratic way possible, and it is not worthy of this institution* », 147 Cong. Rec. H7159, 7206 (2001).

[23] In verità, al momento della presentazione al Congresso del provvedimento, il Procuratore Generale John Ashcroft aveva concesso appena una settimana al Parlamento statunitense per approvare la legge, escludendo assolutamente la possibilità di introdurre emendamenti. Solo in seguito alle pressioni del Senatore Democratico del Vermont Patrick Leahy, presidente della Commissione Giustizia del Senato, il Dipartimento della Giustizia ammise la possibilità di modificare il progetto di legge, di cui fecero uso soprattutto i membri della Camera dei Rappresentanti. Ad ogni modo, Ashcroft non mancò di stigmatizzare il proprio dissenso in proposito, ammonendo che nuovi attacchi terroristici erano imminenti, e che ove il Congresso non avesse provveduto ad approvare immediatamente la norma avrebbe rischiato pesanti critiche per tale ritardo. Il tutto si tradusse in un'approvazione repentina al Senato, senza dibattito o emendamenti, e con la sola obiezione del Senatore Russ Feingold, eletto per il partito democratico nel Wisconsin, il quale — senza tuttavia ottenere un particolare seguito tra i colleghi — contrapposе ad un accoglimento precipitoso della norma soprattutto il rischio che l'impulsività del momento avrebbe prodotto a medio e lungo termine effetti indesiderati in termini di tutela delle libertà fondamentali. Alla Camera bassa furono introdotti emendamenti di poco conto, procedendo poi all'approvazione della legge con 357 voti favorevoli contro 66 contrari. Su tutto v. Electronic Privacy Information Center — EPIC, The USA PATRIOT Act Page, *http://www.epic.org/privacy/terrorism/usapatriot/* (29 novembre 2006). Per un'analisi del procedimento di approvazione del Patriot Act cfr. anche B.A. Howell, *Seven Weeks: the Making of the Usa Patriot Act*, in *George Washington Law Re-*

serrati lavori parlamentari che alla loro conclusione l'opinione pubblica statunitense rimase priva di un'adeguata copertura della vicenda da parte dei principali organi di informazione, al punto che nei mesi successivi le critiche al provvedimento da parte delle organizzazioni di difesa dei diritti civili e le secche smentite dei rappresentanti del Governo, questi ultimi intenti a disegnare i primi come sconsiderati agitatori sociali e più o meno involontari favoreggiatori dei terroristi, erano sistematicamente intervallate da interventi di privati cittadini preoccupati di comprendere in quale misura il *Patriot Act* rappresentasse una restrizione delle loro libertà costituzionali[24].

La conseguenza di una tale rapidità nella gestione del procedimento si è tradotta in una inevitabile provvisorietà della maggior parte delle disposizioni ivi contenute (definite in gergo « *sunset provisions* »), destinate a perdere vigore il 31 dicembre 2005 ove non fossero state reiterate nelle forme adeguate[25]: peraltro, è stato correttamente rilevato come il § 224 USAPA, che introduce una considerevole deroga alla citata clausola di cessazione di validità del provvedimento, grazie alla quale questo resta applicabile anche oltre il 31/12/2005 *indipendentemente da un'eventuale reiterazione del Patriot Act* per tutte le attività di indagine in materia di *intelligence* straniere iniziate prima della data della supposta espirazione della norma, o per qualunque reato effettivo o potenziale (sic!) iniziato o verificatosi prima di tale data[26], finisca per tradursi in un comodo espediente per chi tra le fila del Governo intenda provare ad eludere la restrizione temporale di validità del provvedimento[27], non rendendo tuttavia giustizia all'essenza della norma[28], che in quanto emergenziale non potrebbe prescindere

view, 72, Aug. 2004, pp. 1145-1207. Da rilevare, ad ogni modo, come sebbene il Congresso abbia approvato una versione dell'USAPA sostanzialmente identica a quella proposta dal Governo, l'Assemblea parlamentare statunitense ne abbia respinto alcune delle disposizioni più estreme, come il ridimensionamento delle corti ordinarie sulla condotta dell'Esecutivo, cfr. L. SALAS, *Primi appunti sul « Patriot Act » statunitense*, in *La legislazione penale*, 3/2004, pp. 474-512.

[24] Un'analisi della copertura dell'emanazione del provvedimento da parte dei principali network televisivi nazionali rivela che sia NBC che ABC non prestarono particolare attenzione alla notizia. Per una valutazione critica molto dettagliata dell'intero processo di approvazione del *Patriot Act* e delle reazioni che questo provocò v. K.C. WONG, *The Making of the USA PATRIOT Act. I: The Legislative Process and Dynamics*, 2005, disponibile in *http://law.bepress.com/expresso/eps/793* (2 gennaio 2007).

[25] Proprio la provvisorietà delle restrizioni alla libertà personale sancite dal *Patriot Act* è stato uno degli argomenti principali portati a sostegno di un'approvazione in tempi rapidi del provvedimento, la cui temporaneità avrebbe dovuto nelle intenzioni dei suoi promotori bilanciarne l'eccezionalità giustificandone l'adozione agli occhi dell'opinione pubblica: in che modo tali argomentazioni siano state riprese e « rielaborate » al momento di decidere sulla reiterabilità del *Patriot Act* è ampiamente descritto *infra*, par. III.

[26] Il § 224 del *Patriot Act* riporta testualmente che « *with respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection a*) cease to have effect [il 31 dicembre 2005, *N.d.A.*], *or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect* ».

[27] Così P. TORRETTA, « *Diritto alla sicurezza* » *e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano 2003, pp. 451 ss., in part. 479.

[28] Nel dettaglio, le disposizioni del *Patriot Act* configurate dal § 224 come *Sunset Provisions* ed in quanto tali destinate a

dalla temporaneità della sua validità se non al costo di un suo radicale snaturamento[29].

È noto come il *Patriot Act* abbia comportato tra l'altro un incremento del potere dell'Esecutivo nel monitorare l'attività degli individui ed ottenere informazioni private riducendo le garanzie costituzionali tradizionalmente previste in materia[30]. Probabilmente meno noto, invece, è il fatto che molte delle disposizioni relative alla sorveglianza elettronica erano state presentate nelle sedi istituzionali già prima dell'11 settembre 2001, suscitando in quelle occasioni aspre critiche ed un vivace dibattito[31], per

perdere vigore ove non prorogate dal Congresso entro il 31 dicembre 2005 sono:

§ 201. Authority To Intercept Wire, Oral, And Electronic Communications Relating To Terrorism.

§ 202. Authority To Intercept Wire, Oral, And Electronic Communications Relating To Computer Fraud And Abuse Offenses.

§ 203(b). Authority To Share Electronic, Wire and Oral Interception Information.

§ 203(d.). General Authority To Share Foreign Intelligence Information.

§ 204. Clarification Of Intelligence Exceptions From Limitations On Interception And Disclosure Of Wire, Oral And Electronic Communications.

§ 206. Roving Surveillance Authority Under The Foreign Intelligence Surveillance Act Of 1978.

§ 207. Duration Of FISA Surveillance Of Non-United States Persons Who Are Agents Of A Foreign Power.

§ 209. Seizure Of Voice-Mail Messages Pursuant To Warrants.

§ 212. Emergency Disclosure Of Electronic Communications To Protect Life And Limb.

§ 214. Pen Register And Trap And Trace Authority Under FISA.

§ 215. Access To Records And Other Items Under FISA.

§ 217. Interception Of Computer Trespasser Communications.

§ 218. Foreign Intelligence Information.

§ 220. Nationwide Service Of Search Warrants For Electronic Evidence.

§ 223. Civil Liability For Certain Unauthorized Disclosures.

Sono invece prive di indicazioni circa la durata della loro validità, e dunque da considerarsi permanentemente in vigore fino alla loro eventuale modifica o esplicita abrogazione da parte del Congresso, le seguenti disposizioni:

§ 203(a). Sharing Grand Jury Information.

§ 203(c). Attorney General Guidelines For Sharing Grand Jury Information.

§ 205. Employment of FBI Translators.

§ 208. Number And Residence Of FISA Court Judges.

§ 210. Nation Wide Subpoenas For Electronic Communications Records.

§ 211. Clarification Of Scope Of Cable Provider Obligations.

§ 213. Delayed Notification Of Sneak and Peek Warrant Execution.

§ 216. Modification Of Authorities Relating To Pen Registers And Trap And Trace Devices.

§ 219. Single-Jurisdiction Search Warrants For Terrorism.

§ 222. Assistance To Law Enforcement Agencies.

Cfr. C. DOYLE, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, Congressional Research Service - The Library of Congress, Report for Congress, 10 dicembre 2001, pp. 18-19.

[29] Sul tema della temporaneità come caratteristica insita nell'emergenza, spec. di natura terroristica, v. da ultimo P. BONETTI, *Terrorismo, emergenza e costituzioni democratiche*, Il Mulino, Bologna 2006, in part. pp. 30 ss., 61 ss.

[30] Per un'analisi in lingua italiana degli effetti del *Patriot Act* sulla tutela della Privacy v. R. BILLÉ, « *Patriottismo* » *costituzionale e libertà d'informazione: il caso statunitense*, in questa *Rivista*, 2006, pp. 125-154.

[31] Cfr. EPIC, The USA PATRIOT Act Page, op. cit., p. 2. Analisi condotte sul tema registrano come gli Stati Uniti stiano in realtà promuovendo a livello globale misure invasive della privacy e di controllo delle telecomunicazioni — in particolare finalizzate ad indurre i produttori di apparecchi informatici e di accesso alla Rete ad inserire nei loro prodotti strumenti « *wiretap friendly* », capaci di facilitare le intercettazioni e monitorare attraverso una sorta di « scatole nere » l'attività di navigazione degli utenti della Rete — già da almeno 15 anni. Un particolare standard di assetto delle telecomunicazioni, in grado di favorire le operazioni di *intelligence* in questi ambiti, è stato sviluppato con il so-

essere poi respinte « per i timori in materia di diritti civili », al punto da infondere negli scettici il sospetto che gli attacchi terroristici abbiano rappresentato l'occasione da tempo attesa per dotare l'Esecutivo di poteri eccezionali lungamente auspicati[32].

Relativamente all'analisi delle informazioni disponibili nel Cyberspazio, il *Patriot Act* ha esteso l'applicabilità nel contesto virtuale di quattro differenti metodi di indagine, comunque già previsti dalla disciplina investigativa, a cui corrispondono altrettanti gradi di autonomia nel potere di *intelligence* da parte delle autorità di pubblica sicurezza:

1) *Pen Register* e *Trap and Trace Orders*: un *Pen Register Order* consente di registrare tutti i numeri di telefono chiamati da un determinato telefono, nonché la data, l'ora e la durata delle chiamate. Un *Trap and Trace Order*, al contrario, registra i numeri di telefono degli apparecchi utilizzati per chiamare una determinata utenza.

2) *Wiretaps* (intercettazione di comunicazioni telefoniche o elettroniche): metodo di investigazione utilizzato per la sorveglianza continua di una linea telefonica o di altro tipo di comunicazione elettronica. Esso consente l'intercettazione di contenuti (ad esempio conversazioni o altre informazioni) che passano attraverso la linea intercettata.

3) *Search Warrants*: richiesta di perquisizione sottoposta all'osservanza di speciali garanzie a favore del soggetto destinatario del provvedimento. Abitualmente vi si fa ricorso quando quest'ultimo presenta ragionevoli esigenze di rispetto della privacy di cui il giudice che dispone l'emanazione del provvedimento deve tenere conto: pertanto, ad esempio, un *Search Warrant* deve indicare con precisione il luogo in cui la perquisizione deve avvenire, o gli oggetti che attraverso la perquisizione si spera di trovare.

4) *Subpoena*: richiesta di autorizzazione ad indagini sul conto di un individuo per la cui concessione non è necessario che si verifichino particolari condizioni di rilevanza. Ad esempio, non è richiesto che le informazioni ricercate siano rilevanti per un'indagine penale in corso. Un provvedimento di *Subpoena* può essere emanato anche da un procuratore, senza autorizzazione di un giudice, ma non può essere emesso per ottenere prove o informazioni protette dal Quarto Emendamento della Costituzione degli Stati Uniti[33], a meno che le condizioni ivi previste non vengano comunque rispettate.

---

stegno dell'FBI nei primi anni '90 attraverso un'apposita serie di seminari (l'« *International Law Enforcement Telecommunications Seminar* - ILETS) a cui parteciparono anche rappresentanti di Canada, Hong Kong, Australia e dell'Unione Europea. Gli standard ILETS furono in seguito adottati anche dal Consiglio dell'Unione Europea il 17 gennaio 1995 con una risoluzione segreta, poi pubblicata sulla Gazzetta ufficiale n. C 329 del 04/11/1996 pagg. 1-6, disponibile in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:IT:HTML*. (2 gennaio 2007). Sul punto v. ampiamente Privacy International, Privacy and Human Rights 2002, op. cit., p. 33 ss.

[32] R. O'Harrow, Jr., *Six Weeks in Autumn*, in *Washington Post*, 27 ottobre 2002, p. W06.

[33] « Il diritto dei cittadini a godere della sicurezza per quanto riguarda la loro persona, la loro casa, le loro carte e le loro cose, contro perquisizioni e sequestri ingiustificati, non potrà essere violato; e nessun mandato giudiziario potrà essere emesso, se non in base a fondate supposizioni, appoggiate da un giuramento o da una dichiarazione sull'onore e con descrizione specifica del luogo da perquisire, e delle persone da arrestare o delle cose da sequestrare », trad. tratta da: P. Biscaretti di Ruffìa, *Costituzioni straniere contemporanee*, Giuffrè, Milano 1994[6], p. 19.

II.2. La distinzione tra sorveglianza investigativa esterna e sorveglianza interna.

Attualmente, nell'ordinamento statunitense esistono due differenti forme di competenza che possono essere chiamate in causa per giustificare attività di sorveglianza: la competenza investigativa esperibile in base al *Foreign Intelligence Surveillance Act* (FISA)[34], e l'autorità di condurre attività investigative in base ad una serie di leggi (*Statutes*) federali. Il FISA, emanato nel 1978[35], ha disciplinato specificamente il potere dell'Esecutivo di condurre attività di ricerca e di sorveglianza di agenti o governi stranieri, con il preciso scopo di ottenere informazioni di *intelligence*[36].

Sussistono varie e rilevanti differenze tra un ordine di investigazione emanato ai sensi del FISA ed un ordine di investigazione ottenuto per svolgere investigazioni su attività criminali, tra cui:

1) Non è necessario che ricorra la condizione di fondato sospetto (*probable cause*)[37] per esperire un'indagine ai sensi del FISA;

2) Non c'è bisogno di notifica (*notice*) per autorizzare un'indagine ai sensi del FISA;

3) L'individuo oggetto di indagini *ex* FISA non può essere informato della disposizione giudiziaria che autorizza l'investigazione a suo carico. Pertanto, questi non può efficacemente contestare un provvedimento di intercettazione (*wiretapping*) o di perquisizione eseguito ai sensi del FISA, ed infine

4) Il FISA ha istituito un organo giudiziario speciale (la *Foreign Intelligence Surveillance Court* - FISC), originariamente composta da sette giu-

---

[34] Pub. L. No. 95-511, 92 *Stat*. 1783, codificato in U.S.C. §§ 1801-11 (2000) e 18 U.S.C. §§ 2511, 2518-19 (2000).

[35] Cfr. il testo originale del provvedimento in *http://www4.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36.html* (29 novembre 2006).

[36] Sulla creazione e le applicazioni del FISA dalle sue origini alle emergenze *post* 11 settembre 2001 cfr. P. P. Swire, *The System of Foreign Intelligence Surveillance Law*, in *George Washington Law Review*, 72, Aug. 2004, 1306-1350. In termini generali, ad ogni modo, sembra ormai un dato acclarato — grazie anche ad una reiterata giurisprudenza in questo senso — che con il FISA si sia inteso creare un sicuro contesto all'interno del quale l'Esecutivo possa condurre legittime operazioni di sorveglianza elettronica al fine di conseguire informazioni di *intelligence* straniere nel pieno rispetto dei dettami statuiti dal Quarto Emendamento, cfr. *United States v. Falvey*, 540 F. Supp. 1306 (E.D.N.Y. 1982); *United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987); *United States v. Duggan*, 743, F.2d 59 (2d Cir. 1984).

[37] Nell'ordinamento statunitense il concetto di « *probable cause* » — più che con il quasi letterale « clausola di probabilità », traducibile forse con la più efficace definizione di « fondato sospetto » — ha a che fare con il tipo di regime seguito dalle autorità di polizia per eseguire un arresto, condurre una perquisizione personale o ambientale, od ottenere un'autorizzazione a procedere con provvedimenti del genere. Il termine si riferisce anche agli standard in base ai quali una giuria decide se un crimine è stato commesso, e trae origine dalla definizione contenuta nel Quarto Emendamento della Costituzione USA. La più ampia definizione del concetto potrebbe essere quella di « un ragionevole sospetto che un crimine sia stato commesso » e che la persona a cui il provvedimento di *probable cause* si riferisce sia collegata a tale crimine con lo stesso grado di fondatezza. Per una approfondita analisi diacronica del tema cfr. B.J. Shapiro, *Beyond Reasonable Doubt and Probable Cause. Historical Perspectives on the Anglo-American Law of Evidence*, University of California Press, Berkeley 1999. Per uno studio recente dell'istituto nell'ordinamento statunitense cfr. J. F. Anderson, B. Thompson, *American criminal procedures*, Carolina Academic Press, Durham 2006.

dici di Corte di distretto federale provenienti da circuiti differenti, nominati dal *Chief Justice* della Corte Suprema, in carica per sette anni e non rieleggibili. Il *Patriot Act* ne ha ampliato la composizione, portandola a undici membri, e richiedendo nel contempo che almeno tre di loro provengano da Corti comprese in un'area di non oltre venti miglia dal Distretto di Columbia. La FISC è competente a valutare tutte le richieste presentate dal Procuratore Generale di applicazione dei metodi di indagine previsti nel FISA, comprese le istanze relative alle misure di sorveglianza elettronica finalizzate ad ottenere informazioni di *intelligence* straniere. I giudizi non prevedono contraddittorio, ma si basano esclusivamente sulle presentazioni delle richieste effettuate dal Dipartimento di Giustizia. Inoltre, audizioni, decisioni e conclusioni della Corte ricadono in un regime di assoluta segretezza. Peraltro, una volta ottenuta l'autorizzazione all'investigazione, il Governo non è tenuto a dare conto delle attività di indagine alla FISC. Dal 2002 è stato istituito anche un Tribunale di revisione (la *Foreign Intelligence Surveillance Court of Review*) per assicurare un secondo grado di giudizio rispetto alle decisioni assunte dal FISC, che è comunque tenuto ad operare nello stesso regime di segretezza a cui sono vincolati i giudici di primo grado.

Sia per la segretezza delle investigazioni ai sensi del FISA, sia per l'ampiezza di intervento che queste concedono agli agenti, le finalità per le quali si è fatto ricorso a questa forma di indagine sono state tradizionalmente sempre molto limitate. Abitualmente le investigazioni previste dal FISA possono essere utilizzate solamente qualora la raccolta di informazioni su soggetti o contesti stranieri costituisca lo scopo unico o primario dell'indagine, anche in assenza di un preciso sospetto di reato ma purché il destinatario del provvedimento abbia collegamenti « con lo spionaggio straniero »[38]: non a caso, gli obiettivi di tali investigazioni sono sempre stati agenti di Stati esteri o i loro governi.

Il *Patriot Act* amplia significativamente le finalità per le quali è possibile ricorrere al potere di investigazione sancito dal FISA, che infatti può essere fatto valere anche se lo scopo principale dell'intervento è un'indagine penale, e la raccolta di informazioni rappresenta solo un obiettivo « significativo » per l'inchiesta[39]: termini alquanto indefiniti, la cui vaghezza può facilmente condurre ad un utilizzo improprio o eccessivo degli standard fissati dalla norma[40]. L'autorizzazione a porre in essere un'investigazione *ex* FISA può anche essere richiesta ed ottenuta malgrado i soggetti

---

[38] D. Lithwick-J. Turner, *A Guide to the Patriot Act*, Part 2, in *Slate*, disponibile in *http://www.slate.com/id/2088106/* (2 gennaio 2007).

[39] Il § 216 dell'USAPA si limita a prevedere che gli apparati necessari a condurre intercettazioni telefoniche e telematiche possono essere legittimamente utilizzati dalle autorità di pubblica sicurezza qualora « the information likely to be obtained by such installation and use is *relevant* to an ongoing criminal investigation » (corsivo nostro). Sul punto cfr. ampiamente *infra*, par. 3.1.

[40] Cfr. FISA Page dell'Electronic Privacy Information Center - EPIC, p. 6, disponibile in *http://www.epic.org/privacy/terrorism/fisa/* (2 gennaio 2007). Esprimendosi sulla precedente disciplina, la Corte Suprema aveva comunque sancito la costituzionalità della riduzione degli standard probatori poi recepita dal FISA ove sia in gioco la sicurezza nazionale, rilevando tra l'altro nell'occasione come i requisiti per l'emanazione di un'ordinanza giurisdizionale possano variare in base alla natura degli interessi dello Stato e dei privati effettivamente coinvolti, cfr. *United States v. United States District Court*, 407 U.S. 297, 322-323 (1972).

che la inoltrano non siano in grado di addurre elementi che soddisfano la condizione di *probable cause* nella vicenda *a quo*[41]. Persino le esigue condizioni di cui il FISA esige il rispetto per la concessione delle misure di sorveglianza elettronica — così come emendate attraverso l'USAPA — decadono se quest'ultima riguarda soltanto le comunicazioni utilizzate esclusivamente tra potenze straniere, e quando appare improbabile che le comunicazioni a cui prende parte un cittadino statunitense saranno intercettate. Secondo la nuova disciplina, il Governo degli Stati Uniti può condurre attività di sorveglianza fino al massimo di un anno senza il bisogno di autorizzazioni da parte dell'autorità giudiziaria ordinaria — una libertà di manovra talmente ampia da far prospettare da più parti il pericolo che la nuova versione del FISA possa costituire per il Governo l'occasione per svolgere indagini sul territorio nazionale non necessariamente collegate alla minaccia terroristica[42]. Ad ogni modo, quand'anche non si vogliano alimentare sospetti di mutamenti strumentali della materia, appare evidente come la modifica del regime di applicazione del FISA seguita all'emanazione dell'USAPA costituisca un improprio stravolgimento della norma in questione[43]: se infatti l'allentamento delle garanzie costituzionali previ-

[41] Cfr. EPIC, The USA PATRIOT Act Page, op. cit., p. 5.

[42] È il caso dell'*American Bar Association*, l'organizzazione rappresentativa degli interessi degli avvocati statunitensi, che nel 2003 ha invitato il Congresso a vigilare sulle modalità di applicazione del FISA successivamente agli eventi dell'11 settembre 2001, e nel 2006 ha presentato un rapporto che richiede al Presidente il rispetto del sistema di *checks and balances* sancito dalla Costituzione federale e la cessazione dei provvedimenti di sorveglianza elettronica in contrasto con la reale finalità del FISA, disponibile in *http://www.abanet.org/media/docs/domsurvrecommendationfinal.pdf* (2 gennaio 2007). Altro esempio di dissenso in proposito è venuto da una coalizione di gruppi di difesa dei diritti civili, che in un *amicus brief* presentata alla *Foreign Intelligence Surveillance Court* ha invitato i giudici a respingere una richiesta del Governo di ampliare i poteri di sorveglianza per « sicurezza nazionale » su cittadini statunitensi, ritenendo che un tale provvedimento avrebbe messo in pericolo interessi fondamentali costituzionalmente tutelati.

[43] L'artefice di questo cambiamento radicale è il § 218 dell'USAPA: con questa norma, infatti, si elimina la distinzione statuita dal legislatore nel 1978 attraverso il FISA tra indagini interne e attività di *foreign intelligence*. Come detto, quindi, la *Foreign Intelligence Surveillance Court* può ora autorizzare anche la sorveglianza di cittadini statunitensi, purché una delle finalità delle indagini sia il conseguimento di informazioni spionistiche. Prima dell'emanazione del *Patriot Act*, infatti, le procedure di investigazione previste dal FISA potevano essere applicate solamente ove lo *scopo unico* della sorveglianza fosse il conseguimento di *foreign intelligence information*; a partire dal 26 ottobre 2001, invece, alla dicitura « scopo unico » (*the purpose*) viene sostituita quella di « scopo significativo » (*a significant purpose*), sancendo il definitivo superamento dell'esclusività dell'oggetto di indagine nelle investigazioni condotte ai sensi del FISA. La dottrina non ha lesinato critiche in proposito: P.P. SWIRE, *The System of Foreign Surveillance Law*, op. cit., ritiene che la più eclatante modifica apportata dal *Patriot Act* al regime di investigazioni disciplinato dal FISA sia consistita nell'aver eliminato la fondamentale separazione tra le attività condotte dall'FBI e quelle gestite dalla CIA, con tutto quello che ciò comporta in termini di riduzione delle garanzie giurisdizionali, mentre O.S. KERR, *Internet Surveillance Law After the Usa Patriot Act: The Big Brother That Isn't*, in *Northwestern University Law Review*, Winter 2003, pp. 607-673, pur ritenendo il *Patriot Act* una semplice ufficializzazione di una prassi giurisprudenziale già affermatasi in precedenza, sostiene che tutti gli emendamenti apportati al FISA si siano tradotti in conseguenze negative per la privacy, proprio per aver essi ridisciplinato i rapporti tra FBI e CIA in modo da consentire ai due uffici una sostanziale condivisione di informazioni sensibili, precedentemente vietata.

ste dalla versione originaria del FISA si giustificava con la peculiarità dei fini che il provvedimento perseguiva — ovvero la raccolta di materiale di *intelligence* relativo a contesti stranieri ed a possibili rischi di spionaggio internazionale —, la sua esperibilità in un ambito completamente differente come quello delle indagini penali interne instaura una deroga ragguardevole rispetto alle fondamentali tutele previste dalla disciplina della sorveglianza elettronica precedentemente in vigore.

Un altro aspetto della nuova regolamentazione delle intercettazioni telefoniche e telematiche introdotta con l'USAPA che merita un'attenta considerazione riguarda la tipologia delle comunicazioni interessate dal provvedimento: se infatti la disciplina originaria interessava specificamente le comunicazioni via telefono, il nuovo regime della materia si estende indifferentemente all'attività di navigazione in Internet, comprendendo ad esempio sia l'invio e il ricevimento di messaggi di posta elettronica che la visita di siti *Web*. Porre esattamente sullo stesso piano i due ambiti, tuttavia, comporta rischi estremamente rilevanti, in primo luogo perché le informazioni conseguibili attraverso l'intercettazione di un numero di telefono chiamato da un sospetto sotto sorveglianza non sono certamente equiparabili a quelle che si possono ottenere conoscendo il tracciato della navigazione *on-line* dello stesso: le seconde, infatti, sono sicuramente più estese e dunque sensibili delle prime, poiché rivelano molto di più del soggetto al quale si riferiscono e dei terzi con cui egli interagisce, e come tali meriterebbero un trattamento assai più cauto di quello che la generalizzazione provocata dall'USAPA ha prodotto[44].

Dall'esame dei rapporti annuali sull'applicazione del FISA si evince in primo luogo una crescita esponenziale delle richieste di applicazione delle misure di investigazione previste nel provvedimento nel quadriennio 2001-2005: la serie storica mostra 934 richieste approvate dalla speciale corte federale competente nel 2001, 1.228 presentate e tutte approvate nel 2002, 1.724 (un record assoluto fino a quel momento, con un minimo quantitativo di domande rifiutate dalla *Foreign Intelligence Surveillance Court*) approvate nel 2003, quando il numero dei *Warrants* di sorveglianza segreta ha superato per la prima volta le misure di intercettazione, 1.758 (nuovo massimo storico) nel 2004, con nessuna istanza respinta ed ancora una superiorità delle richieste di sorveglianza su quelle di intercettazione, e 2.072 richieste di sorveglianza presentate ed accolte nel 2005, con un incremento del 18% rispetto all'anno precedente[45]. Più in generale, nel *Real Security Act* emanato agli inizi di settembre 2006[46] si legge tra l'altro che nel periodo 1978-2003 la *Foreign Intelligence Surveillance Court* ha respinto l'istanza di autorizzazione ad un provvedimento di sorveglianza elettronica solo in cinque delle circa 19.000 richieste ricevute in tal senso[47]. Se-

[44] Cfr. EPIC, The USA PATRIOT Act Page, op. cit., p. 5.

[45] Un ulteriore rapporto mostra come nello stesso anno le Corti statali e federali abbiano comunque autorizzato 1.710 provvedimenti di intercettazione (+ 19% rispetto al 2003) e che i soli funzionari federali hanno presentato 730 richieste di *wiretapping* (+26% rispetto al 2003), cfr. statistiche pubblicate nelle pagine del sito EPIC dedicate all'applicazione dei provvedimenti esperibili attraverso il FISA: *http://www.epic.org/privacy/wiretap/stats/fisa_stats.html* (3 gennaio 2007).

[46] Real Security Act of 2006, S. 3875, 7 settembre 2006.

[47] Sul provvedimento più ampiamente *infra*, par. III.3.

condo i rapporti del Dipartimento della Giustizia, inoltre, nel solo 2005 le forze di sicurezza statunitensi sono state autorizzate ad eseguire 1.773 provvedimenti di intercettazione in tutti gli Stati Uniti, mentre il Governo ha emesso 9.524 *National Security Letters*[48], utilizzabili per ottenere informazioni su individui senza che si applichino le tradizionali garanzie giurisdizionali previste dalla legge[49].

Che la nuova disciplina della materia sollevi più di un dubbio in merito alla sua liceità è comprovato dalla controversia sorta nell'ambito della stessa giurisdizione speciale del FISA[50]: nel maggio 2002 la *Foreign Intelligence Surveillance Court* ha infatti espresso forti critiche sulle linee-guida emanate dal Procuratore Generale in merito alla nuova disciplina[51], in particolare nella parte in cui si incrementavano i poteri di investigazione elettronica delle forze di polizia, sostenendo l'illegittimità di una condivisione di informazioni tra agenzie di *intelligence* ed apparati incaricati di indagini comuni, e rimarcando come la finalità primaria di un'investigazione *ex* FISA debba necessariamente rimanere il conseguimento di informazioni di *intelligence* straniera[52]. Se appare eclatante un intervento del genere da parte di un'istanza tradizionalmente favorevole alle posizioni degli organismi di sicurezza nazionali, ancor più clamorosa è la risposta della *Foreign Intelligence Surveillance Court of Review*, che nel suo primo pronunciamento in assoluto dall'entrata in vigore del FISA ha sostanzialmente cassato la decisione di primo grado, sostenendo che il *Patriot Act* ha radicalmente modificato la disciplina relativa alla condivisione delle informazioni tra *intelligence* ed agenzie di investigazione comuni, sancendo dunque la legittimità dell'ampliamento delle inchieste sulla sicurezza interna prodotto dalle nuove linee-guida emanate dall'*Attorney General*[53].

---

[48] Per un'analisi della riforma dell'utilizzazione delle *National Security Letters* attraverso l'USAPA v. *infra*, par. II.3.6.

[49] Cfr. rapporto citato in FISA Page dell'EPIC, disponibile in *file:///c:/Dokumente%20und%20Einstellungen/Gast/Desktop/2005rept.html* (3 gennaio 2007).

[50] L'episodio è citato in R. Billé, *« Patriottismo » costituzionale e libertà d'informazione: il caso statunitense*, op. cit., pp. 144-145.

[51] Cfr. *U.S. Attorney General Memorandum on Intelligence Sharing Procedure*, 6 marzo 2002, disponibile in *http://www.fas.org/irp/agency/doj/fisa/ag030602.html* (4 gennaio 2007).

[52] Cfr. *In re All Matters to Foreign Intelligence Surveillance* (FISC *Decision*), 218 F.2d 611, 622, 625.

[53] Cfr. *In Re Sealed Case* (FISCR *Decision*), 310 F.3d 717, 746 (Foreign Intel. Surv. Ct. Rev. 2002), ma anche *Memorandum Opinion of the FISC*, 17 maggio 2002, disponibile in *http://www.fas.org/irp/agency/doj/fisa/fisc051702.html* (4 gennaio 2007).Ricognitivo sulla vicenda D. Hardin, *The Fuss Over Two Small Words: The Uncostitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, in *George Washington Law Review*, 71, April 2003, pp. 291-345, mentre risultano assai più critici A. Beeson-J. Jaffer, *Unpatriotic Acts. The FBI's power to rifle through your records and personal belongings without telling you*, in *http://www.aclu.org/FilesPDFs/spies_report.pdf*, p. 8, e P.P. Swire, *The System of Foreign Intelligence Surveillance*, op. cit., pp. 1338 e 1367, secondo il quale la decisione della FISCR produce un assoluto snaturamento del sistema di compromesso tra *intelligence* ed investigazioni comuni instaurato con la versione originaria del FISA, a cui sarebbe possibile rimediare soltanto attribuendo un maggiore controllo in materia di sorveglianza sull'*intelligence* straniera alle Commissioni Giustizia di Camera e Senato.

II.3. L'incremento dei poteri di indagine del Governo nel Cyberspazio.

II.3.1. Estensione ai reati terroristici ed informatici del nuovo regime di sorveglianza elettronica: il fenomeno *hacking*.

Il § 201 dell'USAPA aggiunge i reati di terrorismo e di produzione e/o diffusione di armi chimiche tra quelli il cui sospetto autorizza il Governo a ricorrere alle intercettazioni elettroniche: poiché un potere del genere a favore dell'Esecutivo era già ampiamente riconosciuto dal FISA, il nuovo regime non fa altro che estendere questa facoltà anche a persone sospettate di terrorismo domestico. Più specificamente, attraverso il combinato disposto con il § 805 del *Patriot Act*, la norma consente l'applicazione degli speciali poteri di investigazione citati anche ad un reato di nuova istituzione, consistente nel « fornire supporto materiale al terrorismo » sotto forma di « consiglio o assistenza tecnica ».

Il § 202 dell'USAPA include invece nella lista dei reati per i quali è consentito il ricorso alle intercettazioni per lo svolgimento delle indagini le fattispecie previste nel *Computer Fraud and Abuse Act*[54], che ora comprende tra l'altro: accesso intenzionale non autorizzato ad un computer protetto del Governo allo scopo di ottenere informazioni riservate per clandestini stranieri « con ragione di credere che tali informazioni potrebbero essere utilizzate per danneggiare gli Stati Uniti o a vantaggio di una qualunque nazione straniera »; accesso ad un computer protetto che provochi danni per più di 5.000 dollari; accesso ad un computer protetto a scopo di estorsione. Come si vede, tra i crimini informatici che giustificano il ricorso alla nuova disciplina di sorveglianza elettronica non figurano soltanto reati tipicamente esperibili da organizzazioni terroristiche, ma anche classiche attività di *hacking* che, a prescindere dalla loro effettiva illiceità, non si configurano necessariamente per una matrice eversiva o antisistema, ma possono essere anche mosse da mero scopo di lucro. Il fenomeno *hacking* è troppo ampio e complesso per darne adeguatamente conto in questa sede[55]: basti osservare che in questa categoria di atti rientrano anche tutta una serie di iniziative c.d. antagoniste o di disobbedienza civile, che con i dovuti adeguamenti tecnologici tendono a trasportare nel contesto virtuale comportamenti di protesta e di dissenso tradizionalmente ammessi in quello reale, come lo « sciopero in rete » (*Netstrike*) o il « bombardamento » attraverso messaggi di posta elettronica (*Mailbombing*). Si tratta di azioni con cui gruppi organizzati di navigatori del *Web* concordano ad

---

[54] 18 U.S.C. § 1030

[55] Per un'analisi della complessità del fenomeno *hacking* e delle forme di espressione del dissenso in Rete v. tra gli altri F. Carlini, *Internet, Pinocchio e il Gendarme. Le prospettive della democrazia in rete*, Manifestolibri, Roma 1996; A. Di Corinto-T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, Roma 2002; F. Carlini, *Divergenze digitali. Conflitti, soggetti e tecnologie nella terza Internet*, Manifestolibri, Roma 2002; L. Jeffrey, *Tempo e democrazia on line. Riflessioni sul processo politico nell'era dei network globali*, in D. de Kerckhove (a cura di), *La conquista del tempo*, op. cit., pp. 75-102; S. Gulmanelli-A. Dagnino, *Popwar. Il NetAttivismo contro l'Ordine Costituito*, Apogeo, Milano 2003; G. Meikle *Disobbedienza civile elettronica. Mediattivismo e Internet: costruire insieme una nuova sfera pubblica*, Apogeo, Milano 2004.

esempio di collegarsi contemporaneamente ad un sito (nel primo caso) o di inviare quante più *E-mail* possibili alla casella di posta elettronica (nel secondo) afferenti ad un soggetto privato o pubblico, in dissenso con provvedimenti da questo programmati, emanati o esperiti, per indurlo a recedervi o a modificarli. Lo scopo è quello di mettere temporaneamente fuori uso gli strumenti informatici del soggetto destinatario dell'iniziativa, e può tradursi anche in un ingente danno economico per l'interessato: tuttavia, quando l'azione non sia finalizzata alla semplice estorsione, ma esprima piuttosto un dissenso nei confronti di una determinata strategia posta in essere dal destinatario dell'azione di disturbo, proclamarne l'illiceità a priori per la sola ragione che essa arreca un danno di natura economica — dando per scontato che le modalità di esecuzione dell'intervento restino pacifiche e non si ricorra ad esempio all'invio di virus informatici che non mirano ad un blocco temporaneo degli apparati telematici del soggetto interessato, ma minacciano di provocare una « epidemia » a catena capace di mettere fuori uso in modo definitivo intere sezioni della Rete, danneggiando indiscriminatamente anche milioni di utenti assolutamente estranei alla vicenda — rischia di tradursi in un divieto preventivo del diritto di manifestazione del pensiero[56]. Si tratta dunque di un tema complesso ed articolato, che però proprio per queste ragioni non dovrebbe essere trattato con la precipitazione e l'emotività che hanno caratterizzato l'elaborazione del *Patriot Act*. Per quel che rileva in questa sede, inoltre, preme sottolineare l'incongruità con cui si estende sommariamente un provvedimento dichiaratamente finalizzato alla repressione del terrorismo internazionale anche a contesti del tutto differenti, come quello del « cyberdissenso ».

II.3.2. *Pen Register* e *Trap and Trace Orders* (USAPA §§ 214, 216).

Attualmente gli organismi di pubblica sicurezza coinvolti in attività di *intelligence* possono ottenere un'ordinanza di *Pen Register* o di *Trap and Trace* (*Pen/Trap Order*) con cui sono autorizzati ad accedere ai numeri di telefono in entrata e in uscita da una determinata utenza telefonica. Per questo, l'autorità interessata deve dimostrare che l'informazione che essa sta cercando di ottenere è « rilevante per un'investigazione criminale in corso » e che il sospetto sorvegliato è « in comunicazione con » qualcuno coinvolto in attività di terrorismo internazionale o di *intelligence*. Ad ogni modo, si tratta di uno standard molto più basso di quello abitualmente richiesto nelle indagini criminali.

I §§ 214 e 216 dello USAPA riducono ulteriormente questi parametri: il § 214, ad esempio, cancella la dicitura « in comunicazione con ». Pertanto, chi richiede l'applicazione della norma in questione ora deve solamente dimostrare che l'informazione che sta cercando è rilevante per un'indagine criminale in corso, senza più l'obbligo di provare che lo strumento di cui

[56] Da ultimo sul tema della libertà di manifestazione del pensiero v. A. Pace-M. Manetti, *Art. 21: la libertà di manifestazione del proprio pensiero*, in *Commentario della Costituzione*, Bologna/Roma, Zanichelli/Soc. ed. del Foro Italiano, 2006.

si intende fare uso riguarda investigazioni su agenti stranieri — come richiedeva la disciplina *ante* USAPA del FISA — o un individuo coinvolto nel terrorismo internazionale o in attività clandestine di *intelligence*. Questa liberalizzazione ha comportato un inevitabile snaturamento della disciplina in oggetto rispetto alla sua finalità originaria: infatti, se un allentamento dell'obbligo di osservanza delle garanzie costituzionali in questo contesto a favore di una maggiore libertà di azione del Governo si giustificava con la necessità di porre l'Esecutivo in condizione di adempiere al meglio alle proprie responsabilità in tema di tutela della sicurezza nazionale, nella fattispecie monitorando costantemente l'attività di potenze straniere e dei loro agenti, lo stesso non può dirsi quando la stessa discrezionalità incontrollata viene generalizzata, eliminando il limite dirimente costituito dalle « potenze straniere » e rischiando di fatto di privare potenzialmente l'intera popolazione statunitense di basilari tutele costituzionali[57]. Questo rilievo viene in parte mitigato dal fatto che lo stesso § 214 continua a vietare la sorveglianza di un cittadino degli Stati Uniti attraverso apparecchi di *Pen/Trap* quando l'indagine sia condotta sulla « sola base di attività protette dal Primo Emendamento » della Costituzione federale[58].

Secondo il § 216, invece, se l'autorità di sicurezza richiede l'emanazione di un ordine di *Pen/Trap* ad un giudice, questi *deve* concederlo, senza alcuna discrezionalità in merito alla decisione di procedere o meno in tal senso. In altre parole, un giudice potrebbe anche ritenere la richiesta ingiustificata o impropria, ma non ha alcun potere di rifiutare l'emanazione del provvedimento. Il § 216 estende anche la finalità dell'informazione che si cerca di ottenere attraverso un ordine di *Pen/Trap*. Normalmente, questo tipo di disposizioni poteva essere utilizzato solamente per conseguire numeri telefoni chiamati e ricevuti. Attualmente, invece, il § 216 dello USAPA consente anche l'accesso ad informazioni « in selezione (*dialing*), in circolazione (*routing*) e di segnalazione (*signaling*) ». Il termine « *routing* » si riferisce espressamente all'utilizzo di Internet — sia per l'invio di *E-mail* che per la navigazione sul *Web*. Il *Patriot Act* vieta esplicitamente che i « contenuti » possano essere ottenuti attraverso un ordine di *Trap/Trace*, ma evita di fornire una definizione di ciò che debba intendersi con tale termine[59]. Il timore, quindi, è che sotto questi standard così bassi gli investigatori del Governo possano ottenere informazioni sulle attività di navigazione in Rete che mostrano quali siti un sospetto abbia visitato e quali attività abbia compiuto mentre navigava su questi siti. Diversamente dalle chiamate telefoniche, rispetto alle quali il numero selezionato e ricevuto può facilmente essere separato dal contenuto della conversazione, questo non accade con una rete di scambio di informazioni « a pacchetti » come In-

---

57 Cfr. EPIC FISA Page, p. 7.

58 « Il Congresso non potrà fare alcuna legge per il riconoscimento di qualsiasi religione, o per proibirne il libero culto; o per limitare la libertà di parola o di stampa, o il diritto che hanno i cittadini di riunirsi in forma pacifica e di inoltrare petizioni al governo per la riparazione di torti subiti », trad. tratta da: P. BISCARETTI DI RUFFÌA, *Costituzioni straniere contemporanee*, op. cit., p. 19.

59 Sebbene il termine « contenuto » sia stato definito in un contesto analogo (v. 18 U.S.C. § 2510 (8), in cui esso « include qualunque informazione riguardante la sostanza, l'obiettivo o il significato della comunicazione »), nella fattispecie in esame risulta comunque vago, e non è mai stato testato nel contesto delle comunicazioni via Internet.

ternet, almeno attualmente. Con uno standard basso come quello previsto dagli ordini di *Trap/Trace*, dal momento che il Governo è autorizzato solamente ad ottenere il numero chiamato e/o ricevuto, le autorità di sicurezza non hanno il permesso di ascoltare il contenuto della conversazione telefonica. Nel *World Wide Web*, invece, il contenuto non può essere altrettanto facilmente separato dalle informazioni relative all'attività di navigazione *on-line*. Di conseguenza, per ottenere un indirizzo di posta elettronica, ad esempio, è necessario che all'autorità che svolge l'attività di indagine sia consentito l'accesso all'intero « pacchetto » *E-mail*, che ne comprende anche il contenuto: all'autorità in questione viene dunque concessa la responsabilità (e la discrezionalità) di verificare solamente l'indirizzo di posta elettronica cercato, e di cancellare il contenuto della *mail* senza leggerlo.

Per di più, nella navigazione in Rete il contenuto non può essere agevolmente separato dalle informazioni relative all'attività di *routing*. Immaginiamo, ad esempio, che qualcuno avvii una ricerca su Google cercando informazioni sul terrorismo; immaginiamo che questa persona ponga come criteri di ricerca « *jihad.com* », seguito da « *bombs.com* », « *Osama.org* » e quindi « *ACLU* »[60], seguito da un contatto per ciascuno di questi siti *Web*. A questo punto non è più possibile separare l'attività di navigazione dal « contenuto » delle pagine viste, dal momento che quest'ultimo è rivelato dalla navigazione in Rete e dalle URL[61] delle pagine visitate.

Le organizzazioni per i diritti civili hanno criticato la concessione alle autorità di pubblica sicurezza di un simile potere di accesso ad informazioni come i siti *Web* visitati, senza inserire ulteriori e più gravosi vincoli a carico del Governo nel condurre una tale ricerca. In effetti, alcune delle tecnologie utilizzate per la raccolta di informazioni sulla navigazione *on-line* forniscono dati anche su altri soggetti che utilizzano lo stesso *Internet Service Provider* (ISP). Ad esempio, il sistema di sorveglianza della Rete *Carnivore* adottato dai servizi segreti statunitensi è fondato su un procedimento di raccolta delle informazioni che non riguardano solo l'obiettivo dell'investigazione, ma anche altri utenti dello stesso ISP[62]. All'FBI viene quindi affidato il delicato

[60] « ACLU » è l'acronimo di *American Civil Liberties Union*, una delle più note organizzazioni non governative degli Stati Uniti finalizzate alla tutela dei diritti civili, reperibile in Rete in*: www.aclu.org*.

[61] Un « URL » (acronimo di « *Uniform Resource Locator* ») è una sequenza di caratteri che identifica in maniera univoca l'indirizzo di una risorsa in Internet, come un documento o un'immagine, localizzandola all'interno del *World Wide Web*.

[62] Il sistema di controllo della Rete *Carnivore*, successivamente ribattezzato DCS 1000, è stato creato dall'FBI per consentire la sorveglianza elettronica delle comunicazioni attraverso il *Web*. Una volta installato presso un *Internet Provider*, esso permette di registrare e conservare tutti i dati scambiati dai suoi utenti. Secondo il giornale in rete « Wired », all'indomani dell'11 settembre 2001 agenti dell'FBI si sono presentati presso i principali fornitori di accesso alla Rete degli Stati Uniti per installare *Carnivore*, richiedendo ed ottenendo dai responsabili delle compagnie le informazioni relative a collegamenti alla Rete che riguardassero anche pagine *Web* il cui indirizzo contenesse la parola « Allah »: seguendo l'esempio di Hotmail, tutti i grandi *Provider* avrebbero offerto piena collaborazione ai servizi di sicurezza statunitensi, cfr. *Reporters Sans Frontières*, *Internet en liberté surveillée*, op. cit., p. 5. Considerato in grado di « controllare milioni di *E-mail* al secondo » e di « offrire al Governo, almeno in via teorica, la capacità di sorvegliare tutte le comunicazioni digitali degli utenti, dalle *E-mail* alle operazioni di *Internet Baking* ed alla navigazione in Rete », nel corso del 2000 il *Carnivore* divenne il bersaglio di feroci critiche soprattutto da parte di organizzazioni preoccupate della tutela delle libertà fonda-

compito di filtrare dai dati raccolti le informazioni non rilevanti per l'indagine. Questo solleva dei seri dubbi sul diritto alla *privacy* tanto delle parti oggetto delle investigazioni che di quelle non soggette ad indagine ma sorvegliate solamente in quanto clienti dello stesso *Provider*.

Inoltre, un giudice federale o il magistrato di una singola giurisdizione possono emanare un ordine di *Pen/Trap* in bianco che non presenta l'indicazione del *Server* sottoposto ad indagine, con la conseguenza che la disposizione finisce per essere applicabile a qualunque ISP all'interno degli Stati Uniti. Al pari delle ordinanze che consentono attività di *Search Warrants* da eseguire in qualunque distretto, questo incoraggia operazioni di *forum shopping* da parte delle autorità di sicurezza e limita la capacità del *Server* di opporsi all'ordine di *Pen/Trap*. La debolezza dei controlli giurisdizionali previsti è stata tra le principali accuse rivolte al provvedimento, e non è mancato chi ha proposto di rifarsi agli standard di garanzia previsti dall'*Electronic Communications Privacy Act* - ECPA[63], che prevede l'obbligo per il giudice di accertare la rilevanza dell'informazione ricercata ai fini dell'indagine in corso[64]. Un sostegno (probabilmente involontario) alle severe critiche sulla norma in oggetto viene da una comunicazione del Dipartimento di Giustizia alla Commissione Giustizia della Camera dei Rappresentanti nel maggio 2003, in cui si precisava che le disposizioni del § 216 avevano fino a quel momento trovato applicazione soprattutto nelle seguenti fattispecie di indagini: 1) cospirazioni terroristiche; 2) almeno un grande spacciatore di droga; 3) « ladri di identità » appropriatisi dei dati bancari delle loro vittime avendole poi derubate dei loro risparmi; 4) un individuo colpevole di quadruplice omicidio; 5) un evaso fuggito durante il processo utilizzando un passaporto falso[65]. La varietà dei reati menzionati è tale da rendere estremamente difficile continuare a sostenere che l'eccezionalità delle misure contenute nel *Patriot Act* trovi la sua giustificazione nella straordinarietà della lotta al terrorismo. Il fatto che il § 216 faccia parte delle norme dell'USAPA prive di un termine di scadenza, peraltro, non facilita la situazione[66].

II.3.3. Accesso ad informazioni ed altri beni materiali (§ 215 USAPA).

Il § 215 del *Patriot Act* rientra sicuramente tra le disposizioni che più di tutte hanno suscitato critiche e preoccupazioni riguardo a possibili indebite ingerenze nella privacy degli individui da parte degli organismi investigativi[67]. La norma, che emenda profondamente il Titolo V del FISA, so-

---

mentali legate ai mezzi di comunicazione, al punto da indurre l'allora Procuratore generale Janet Reno a convocare una commissione tecnica incaricata di verificare le accuse mosse al sistema, e che concluse le proprie indagini con un rapporto presentato nel dicembre dello stesso anno, nel quale si raccomandava di apporvi considerevoli modifiche, cfr. *Independent Technical Review of the Carnivore System, Final Report*, 8 dicembre 2000, disponibile in *http://www.epic.org/privacy/carnivore/carniv_final.pdf* (3 gennaio 2007).

63 28 U.S.C. § 2703.

64 Così J. Podesta, *USA Patriot Act. The Good, the Bad, and the Sunset*, in *Human Rights Magazine*, Winter 2002, p. 2.

65 D. Lithwick-J. Turner, *A Guide to the Patriot Act*, Part 3, Slate, in *http://www.slate.com/id/2088161/* (3 gennaio 2007).

66 Cfr. *supra*, nota 28.

stituendo i §§ 501-503 con nuove versioni dei §§ 501 e 502 appositamente riscritte per l'occasione, consente al direttore dell'FBI o a soggetti da questi designati di obbligare biblioteche e *Internet Provider* a produrre qualsiasi bene materiale tangibile (« *any tangibile things* »), includendo in questa categoria libri, giornali, documenti — compresi quelli in ambito medico, abitualmente protetti dal massimo grado di riservatezza[68] —, archiviazioni di dati personali (« *records* ») ed altri mezzi di prova, nell'ambito di indagini difensive contro il terrorismo internazionale o attività clandestine di *intelligence*, per poter procedere al loro sequestro, con l'unico limite che tali investigazioni non siano condotte su cittadini statunitensi esclusivamente sulla base di attività protette dal Primo Emendamento della Costituzione federale[69]. Dal momento che tale norma sancisce una serie di garanzie a favore di altrettanti diritti fondamentali della persona, al punto da statuire una sostanziale aura di inviolabilità della sfera personale dell'individuo, ammettere la possibilità che un tale potere di indagine possa essere validamente esperito senza confliggere con l'ambito di tutela difeso dal Primo Emendamento appare quanto meno discutibile: se a ciò si aggiunge che, in questa come in altre occasioni già menzionate[70], l'investigatore che domanda l'emissione di un provvedimento ai sensi del § 215 non deve motivare la richiesta, ma solamente dichiarare che i dati in oggetto sono « ricercati per indagini difensive contro il terrorismo internazionale o attività clandestine di *intelligence* », che il giudice della *Foreign Intelligence Surveillance Court* incaricato di emettere tale autorizzazione non dispone di alcuna discrezionalità di valutazione rispetto alle asserzioni di rilevanza delle informazioni ricercate *ex* § 215 ai fini delle indagini da parte delle forze di polizia federali, e che il destinatario di tali misure non viene nemmeno informato di esserne oggetto fin quando le informazioni ottenute non vengano utilizzate in giudizio contro di lui, privandolo dunque fino a quel momento di poter contestare la legittimità delle dichiarazioni esperite dal Governo a suo carico, si comprende come nella fattispecie in esame il rispetto del Primo Emendamento si riveli un principio tutt'altro che prescrittivo. Inoltre, dal momento che non è specificato che l'individuo destinatario di un provvedimento in base alla norma in oggetto debba essere sospettato di attività criminali, il regime di garanzia delle libertà fondamentali si riduce ulteriormente per i non-cittadini statu-

[67] Sul piano dottrinale, si vedano in particolare le osservazioni di S. FREIWALD, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, in *Alabama Law Review*, 56, Fall 2002, 9-83, secondo la quale la democrazia statunitense potrebbe rischiare un pericoloso allontanamento dalla sua propria essenza originaria qualora il Governo riuscisse a porsi in una posizione di controllo assoluto dell'intera società, dal momento che in quel caso non si perderebbe soltanto la *privacy* individuale, ma anche il diritto di manifestazione del pensiero, di associazione e di dissenso.

[68] Così R. BILLÉ, « *Patriottismo* » *costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 143, n. 53, la quale sottolinea come prima della riforma del FISA attraverso il *Patriot Act* era possibile sequestrare soltanto alcuni tipi di documenti, come quelli prelevati in hotel, in motel o nelle auto.

[69] Scettica sulla possibilità che un funzionario dell'FBI possa autodenunciare il proprio intento di violare tale limite — ciò che vanifica l'effettività della tutela che la norma intende garantire ai cittadini — N. TRIVEDI, *Section 215 of the USA PATRIOT Act and National Security Letters: An Update* (Oct. 2005), in The Free Expression Policy Project, disponibile in *http://www.fepproject.org/commentaries/patriotact.oct2005.html* (3 gennaio 2007).

[70] Cfr. *supra*, par. II.3.2.

nitensi, per i quali non vale il citato limite legato al Primo Emendamento della Costituzione USA: così, dal momento che il § 215 USAPA consente anche « di ottenere informazioni di *intelligence* straniere non riguardanti un cittadino degli Stati Uniti », la possibilità che vengano costruite indagini sulla sola base della nazionalità di appartenenza di un individuo, senza che sussista anche il benché minimo sospetto di reato a suo carico, appare molto più che una semplice ipotesi di scuola.

Curiosamente, il § 215 USAPA rientra tra le disposizioni del *Patriot Act* che maggiormente hanno suscitato moti di protesta e disapprovazione, soprattutto presso librai e bibliotecari, che probabilmente anche a causa della scarsezza di informazioni in proposito più di altri hanno mostrato preoccupazioni riguardo alle conseguenze del provvedimento per le attività attinenti alle loro categorie[71].

II.3.4. Intensificazione nell'utilizzo delle disposizioni di *Subpoena* (§ 210 USAPA).

In base alla disciplina precedente, il Governo poteva utilizzare un provvedimento di *Subpoena* per obbligare un *Server* o un sito *Web* a fornire le seguenti informazioni relative ai rispettivi utenti: nome del cliente, indirizzo, durata del servizio e metodo di pagamento (se il pagamento sia stato effettuato con carta di credito, prelievo diretto di denaro da conto corrente bancario, etc.). Il Governo *non* poteva ottenere numeri di carte di credito, numeri di conti correnti, o altre informazioni di identificazione più specifiche attraverso un ordine di *Subpoena*. Secondo il § 210 dello USAPA, le autorità di pubblica sicurezza possono ora utilizzare un provvedimento del genere per conseguire numeri di carte di credito e di conti correnti bancari, sostenendo che queste informazioni sono essenziali, dal momento che moltissime persone si registrano su siti *Web* utilizzando nomi falsi, e che quindi i dati sulle carte di credito ed i conti correnti costituiscono l'unico modo per risalire alla vera identità di un sospetto. Quel che va sottolineato, comunque, è che nessun controllo giurisdizionale è coinvolto nel procedimento di *subpoena*, e dunque non esiste alcun mezzo per verificare che le richieste di un organo di pubblica sicurezza di procedere con tale provvedimento presentino un effettivo fondamento: una circostanza che solleva dubbi considerevoli sulla legittimità dello speciale potere di indagine messo in questo modo a disposizione del Governo[72].

II.3.5. Intercettazione di messaggi in voce emessi ed archiviati (§ 209 USAPA).

Prima dell'emanazione dello USAPA, l'accesso del Governo alle *E-mail* ed alle comunicazioni in voce archiviate era disciplinato rispettivamente dal citato *Electronic Communications Privacy Act* e dalla Legge Federale

---

[71] Cfr. K.C. Wong, *The Making of the USA PATRIOT Act. I: The Legislative Process and Dynamics*, op. cit., pp. 56 ss.

[72] Cfr. EPIC, The USA PATRIOT Act Page, op. cit., p. 9.

sulle Intercettazioni[73]. La differenza si deve alla distinzione tra le informazioni elettroniche registrate (*E-mail*) e le comunicazioni via cavo archiviate (messaggi in voce - *voice mail*). Secondo la disciplina federale in materia, gli ordini di intercettazione erano emanati per accedere a messaggi vocali archiviati da un terzo soggetto operante come *Provider* (ad esempio messaggi vocali registrati dal fornitore del servizio telefonico). Un ordine di *Search Warrant* poteva però essere utilizzato per accedere e sequestrare una segreteria telefonica custodita in un ufficio o in una residenza privata. La procedura per ottenere un ordine di intercettazione è molto più lunga e complessa di quella necessaria per un *Search Warrant*: pertanto, le autorità di pubblica sicurezza spesso sostenevano che le loro indagini venivano intralciate dalla necessità di dover richiedere un ordine di intercettazione. A seguito dello sviluppo tecnologico e della diffusione del MIME (*Multipurpose Internet Mail Extensions*), un sistema di sfruttamento polifunzionale dei servizi della Rete, la disciplina normativa citata ha posto problemi sempre più frequenti. Il MIME, infatti, consente alle *E-mail* di contenere allegati che possono comprendere anche messaggi vocali. Pertanto, per ottenere l'accesso ad un messaggio di posta elettronica, si rendevano necessari sia un *Search Warrant* che un ordine di intercettazione. Il § 209 dello USAPA modifica il modo in cui operano la legge federale sulle intercettazioni e lo ECPA: con la nuova disciplina, le comunicazioni via cavo archiviate sono gestite dalle stesse regole valevoli per i dati elettronici archiviati, e ad entrambi si può accedere con un *Search Warrant*, ovvero non si rende più necessario l'ordine di intercettazione.

II.3.6. La « *National Security Letter* » (§ 505 USAPA).

Il § 505 consente al Procuratore Generale o ad un suo delegato di richiedere a soggetti possessori di dati personali di un individuo — quali compagnie telefoniche e fornitori di accesso alla Rete — di girarli al Governo, semplicemente scrivendo una « Lettera di Sicurezza Nazionale » (*National Security Letter*), sulla cui ricezione gli organismi destinatari sono tenuti al massimo riserbo con chiunque. Anche in questo caso, prima della novella introdotta dal *Patriot Act* questo tipo di provvedimenti poteva essere esperito solo nei confronti di soggetti sospettati di attività di spionaggio: la nuova norma cancella questa distinzione, rendendo l'intera popolazione degli Stati Uniti potenziale vittima di tali misure, senza nemmeno bisogno che il destinatario della « Lettera » sia sospettato di spionaggio o altre attività criminali. Attraverso il § 505 dell'USAPA un qualunque funzionario dell'FBI può ora far uso del provvedimento semplicemente asserendo che la documentazione richiesta è « rilevante nell'ambito di indagini difensive contro il terrorismo internazionale o attività clandestine di *intelligence* », ancora una volta con l'unico limite che tali investigazioni non siano condotte su cittadini statunitensi esclusivamente sulla base di attività protette dal Primo Emendamento della Costituzione federale[74] e, quel che più conta, senza alcun controllo giurisdizionale della sua fondatezza,

[73] 18 U.S.C. § 2510 (1).

[74] Ma sulla dubbia effettività di tale limite v. ampliamente *supra*, par. II.3.3.

nemmeno a posteriori. Proprio per la mancanza di supervisione da parte di organi giudiziari, le autorità di pubblica sicurezza interessate a pratiche investigative « disinvolte » tendono più facilmente a ricorrere al § 505 piuttosto che al citato § 215[75], che quanto meno prescrive un obbligo di autorizzazione da parte della Corte FISA[76]. Le informazioni che è possibile ottenere attraverso la norma in oggetto, a questo punto tramite la semplicemente affermazione di una loro rilevanza nell'ambito di un'indagine penale in corso, spaziano dai collegamenti telefonici e dalle *E-mail* ad alcuni dati bancari e finanziari, fino alle condizioni creditizie dell'indagato[77]. Il rifiuto del Governo di precisare in che modo siano state utilizzate le migliaia di Lettere emanate dall'FBI dall'ottobre 2001 in poi, adducendo ragioni di sicurezza, non giova di certo ai difensori dell'opportunità del provvedimento[78]. In conclusione, dunque, anche in materia di *National Security Letters* la riforma esperita con il *Patriot Act* ha eliminato la preesistente, cruciale distinzione tra attività di *intelligence* e indagini comuni, in questa sede già ampiamente criticata altrove[79].

II.4. Espansione dei poteri di soggetti privati.

II.4.1. Autorizzazione delle vittime di fenomeni di *Hacking* a condurre indagini proprie (USAPA § 217).

Il § 217 del *Patriot Act* consente alle vittime di attacchi informatici (destinatari di fenomeni di *hacking*)[80] « che agiscano conformemente alla legge » di monitorare gli intrusi nel proprio computer. Precedentemente all'approvazione dell'USAPA, i soggetti privati non erano autorizzati a collaborare con le autorità di pubblica sicurezza per compiere azioni di investigazione e monitoraggio su iniziative di *Hacking*. Ora, qualunque privato cittadino che risponda ai seguenti quattro requisiti può intervenire nel monitoraggio di intrusi informatici dei propri sistemi operativi: 1) possessori o operatori del computer protetto devono autorizzare l'intercettazione delle comunicazioni dell'intruso (singoli utenti individuali non possono prendere iniziative in tal senso, solo il *Provider* o il proprietario del *server* possono farlo); 2) la persona che intercetta la comunicazione deve essere autorizzata ufficialmente nell'ambito delle attività di indagine; 3) la persona che opera conformemente alla legge deve avere sufficienti ragioni per credere che i contenuti della comunicazione intercettata saranno rile-

---

[75] Cfr. *supra*, par. II.3.3.

[76] Così anche N. Trivedi, *Section 215 of the USA PATRIOT Act and National Security Letters: An Update*, *op. cit.*

[77] D. Lithwick-J. Turner, *A Guide to the Patriot Act*, Part 4, Slate, in *http://www.slate.com/id/2088239/* (3 gennaio 2007).

[78] Critici sul punto C.P. Raab, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties?*, op. cit., p. 23; C. Doyle, CRS report for Congress, *Administrative Subpoenas and National Security Letter in Criminal and Foreign Intelligence Investigations: Background amd Proposed Adjustments*, in *http://www.fas.org/sgp/crs/natsec/RL32880.pdf* (3 gennaio 2007); L. Flint, *Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power*, Ctr. For Democracy & Tech., in *http://www.cdt.org/security/usapatriot/030924cdt.shtml* (3 gennaio 2007).

[79] V. *supra*, par. II.2.

[80] Sul fenomeno *hacking* v. ampiamente *supra*, par. II.3.1.

vanti per le indagini in corso e 4) gli investigatori possono intercettare solo le comunicazioni inviate o ricevute dall'intruso. È stato sottolineato come la discrezionalità con la quale l'FBI può, attraverso la norma citata, procedere liberamente all'intercettazione di qualunque informazione ove un *Provider* attesti che un proprio utente sia entrato in Internet senza permesso, finisca per delegittimare gravemente il diritto alla *privacy* di quest'ultimo, in favore di un sostanzialmente inappellabile diritto di investigazione da parte delle autorità di sicurezza[81]. Per di più questa disposizione, aprendo la porta alla possibilità che dei possessori di sistemi informatici conducano operazioni di polizia contro quelli che loro ritengono essere intrusi dei propri sistemi, solleva dubbi di grande rilevanza in merito alle finalità per le quali è possibile autorizzare tali attività di sicurezza, ad esempio in merito all'eventualità che i possessori dei sistemi possano intraprendere azioni offensive per ottenere informazioni utili alla cattura degli *hacker*, o che possano semplicemente creare delle difese per il proprio sistema informatico. Delle azioni offensive possono provocare delle intrusioni nella *privacy* di individui che non hanno alcuna intenzione di violare o danneggiare sistemi informatici, e la disposizione in esame non prevede espressamente delle misure di salvaguardia contro questa eventualità. Un'eccezione prevista dall'USAPA in questo contesto riguarda il divieto di applicabilità del regime di sorveglianza a soggetti noti al proprietario o all'operatore del computer soggetto a protezione per avere con quest'ultimo un rapporto di natura contrattuale[82].

II.4.2. Rivelazioni di emergenze da parte di *Internet Provider* (§ 212 USAPA).

Il § 212 del *Patriot Act* consente rivelazioni volontarie da parte delle compagnie telefoniche e degli *Internet Provider* di informazioni private comprendenti sia i dati personali dei clienti che il contenuto di trasmissioni elettroniche, con grande discrezionalità per gli ISP. La disposizione prevede che i soggetti citati possano decidere volontariamente di svelare informazioni private dei propri utenti se sussiste un « ragionevole sospetto » che queste sono collegate ad un' »emergenza che comporta un rischio immediato di morte o di gravi lesioni fisiche per chiunque », senza che gli agenti dell'FBI debbano ottenere un'autorizzazione di un giudice per poter accedere a tali dati, siano tenuti ad informarne il titolare o tanto meno a ricevere il consenso di questi per poterli utilizzare in sede di indagine[83].

In questo modo ai *Provider* viene concessa la facoltà di rivelare informazioni private sui propri sottoscrittori allo scopo di fornire assistenza nell'ambito di attività di *intelligence*. Va comunque sottolineato come la

[81] R. Billé, « *Patriottismo* » *costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 140, n. 51. Sul punto v. anche http://www.eff.org/patriot/ (3 gennaio 2007).

[82] Cfr. EPIC, The USA PATRIOT Act Page, *op. cit.*

[83] Prima dell'emanazione del *Patriot Act*, per accedere a questo tipo di informazioni l'FBI doveva ottenere un ordine di intercettazione da parte di un giudice, o un provvedimento di *subpoena* da parte di un *grand jury*, cfr. *Electronics Communications Privacy Act* 1978 (28 U.S.C. § 2703), op. cit. *supra*, par. II.3.4.

norma si riferisca al disvelamento *volontario* di informazioni — in altre parole, i *Provider* non sono tenuti a rivelare dati a meno che non sia noto che questi sono connessi a vicende criminali. Questo riduce la possibilità che i fornitori di accesso alla Rete possano essere indotti a monitorare trasmissioni di informazioni di natura criminale, non sussistendo alcun incentivo in tal senso.

II.4.3. *Clarification of Scope of Cable Act*.

Il *Cable Act* (47 U.S.C. § 551), approvato nel 1984, pone delle rigide direttive in merito alla possibilità per le compagnie operanti nelle attività via cavo di rifiutarsi di rivelare informazioni sui propri clienti in forza di legge. Ad esempio, attraverso il *Cable Act* un'impresa operativa in questo specifico settore delle telecomunicazioni non era tenuta a rispondere ad ingiunzioni di *Subpoena* o *Warrant* in merito alla fornitura di informazioni sui propri clienti, dovendo invece semplicemente notificare loro di aver ricevuto una richiesta in tal senso dalle autorità di pubblica sicurezza. Al cliente veniva concessa un'audizione, nella quale il Governo era obbligato a giustificare la richiesta dei dati personali sul suo conto.

Recentemente, le compagnie del settore hanno esteso l'ampiezza delle loro attività, passando dalla semplice fornitura di programmi televisivi via cavo ai servizi telefonici ed informatici: pertanto, le compagnie in questione potrebbero rifiutarsi di ottemperare a ordini di *Pen/Trap* appellandosi al *Cable Act*. Il § 211 dell'USAPA prevede però che le norme di legge in materia di *Trap/Trace* si applichino alla pubblicazione di informazioni da parte delle compagnie via cavo riguardo ad Internet ed ai servizi telefonici: pertanto, le garanzie previste dal *Cable Act* trovano ora applicazione solo in merito alle informazioni relative ai servizi di TV via cavo.

II.5. Altre disposizioni del *Patriot Act* riguardanti la privacy nel cyberspazio.

II.5.1. *Warrants* « *Sneak and Peek* » (§ 213 USAPA).

Un *Warrant* « *Sneak and Peek* » è un provvedimento giudiziale grazie al quale il Governo ottiene il potere di procedere a determinate categorie di atti limitativi delle libertà individuali (quali perquisire immobili, fotografare documenti o copiare file) dandovi esecuzione senza doverne informare il destinatario — o facendolo solo con ritardo. La Corte Suprema ha ripetutamente affermato che la tutela prevista dal Quarto Emendamento contro perquisizioni e sequestri ingiustificati prevede che prima che una perquisizione abbia luogo, le autorità di pubblica sicurezza debbano ottenere un *Warrant* e darne informazione alla parte la cui proprietà è interessata dal provvedimento. Esistono delle limitate eccezioni a questa norma: ad esempio, se esiste un legittimo timore che dare informazioni in proposito possa porre in pericolo la vita di un individuo o rischi di mettere in fuga un sospetto, l'informazione può essere ritardata nel tempo. La verifica giudiziale del provvedimento e la necessità che la parte a cui esso si applica ne venga informata assicura che lo scopo del *Warrant* si limiti soltanto alle perquisizioni necessarie per le indagini, e che la parte oggetto del prov-

vedimento abbia l'opportunità di far valere i propri diritti sanciti dal Quarto Emendamento e possa richiedere la verifica di provvedimenti di perquisizione eccessivamente ampi, per tentare di ridurre al minimo l'invasione della *privacy*. Soprattutto, è opportuno sottolineare come la versione originaria del FISA giustificasse le deroghe prodotte da un *Warrant* « *Sneak and Peek* » solo in casi in cui « potenze straniere o i loro agenti » fossero sospettati di terrorismo[84].

Il § 213 dell'USAPA, invece, introduce ampie eccezioni alla regola secondo la quale l'informazione sull'emanazione del *Warrant* deve essere data in un tempo ragionevole. La norma citata prevede infatti che l'autorità di pubblica sicurezza debba solamente riuscire a convincere il giudice che l'indagine verrà messa in pericolo se venisse data notizia del provvedimento[85]: la disposizione stabilisce in proposito che, al momento della sua emanazione, il giudice debba definire solamente il « ragionevole periodo » di validità del provvedimento di *Warrant*, restando comunque libero di decretarne il prolungamento ove lo ritenga opportuno[86]. L'esecuzione di questa particolare categoria di *Warrant* aumenta enormemente il rischio che la perquisizione venga eseguita senza le adeguate salvaguardie, dando luogo ad ingiustificate violazioni della *privacy*. L'aspetto più pericoloso del provvedimento riguarda proprio la motivazione che mira a giustificare dette deroghe: dal momento che sembra difficile pensare a casi in cui un'indagine penale non potrebbe essere condotta con maggior successo rimandando la notifica del *Warrant* ad un momento successivo alla sua esecuzione, il rischio che l'eccezionalità si trasformi in normalità è tutt'altro che remoto, con buona pace di consolidate (almeno finora) garanzie costituzionali. Anche questa disposizione non prevede una data per la scadenza della sua validità.

II.5.2. L'esperibilità delle misure di *Warrant* in qualunque distretto giudiziario (§§219, 220 USAPA).

La norma 49(a) delle disposizioni federali di procedura penale prevede che una richiesta di perquisizione debba essere ottenuta all'interno del distretto nel quale il provvedimento verrà materialmente eseguito. Permangono delle eccezioni per situazioni estreme, tali per cui è possibile dimostrare la probabilità che il sospetto potrebbe darsi alla fuga, rimediando con delle misure di perquisizione applicabili in più distretti. Il § 219 dell'USAPA, invece, stabilisce che un *Warrant* che autorizzi una perquisizione connessa ad indagini su forme di terrorismo nazionale ed internazionale possa essere emanato in qualunque distretto in cui si sia verificata una

[84] D. Lithwick-J. Turner, *A Guide to the Patriot Act*, Part 2, *op. cit.* Una precisa giurisprudenza federale in materia ha comunque decretato che, per ottenere un'ordinanza per un *Warrant* « *Sneak and Peek* », debba sussistere una « causa ragionevole » che faccia presumere che una immediata notifica del provvedimento potrebbe compromettere gli esiti delle indagini. Cfr. *United States v. Freitas*, 800 F2d 1451 (9th Cir. 1986) e *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990).

[85] *Ibid.*, p. 9.

[86] In proposito cfr. M. Bellazzi, *I « patriot acts » e la limitazione dei diritti costituzionali negli Stati Uniti*, in *Politica del diritto*, nr. 4/2003, pp. 681-706.

qualunque forma di attività terroristica, e possa trovare esecuzione indistintamente nel distretto di emissione o in qualunque altro distretto.

Similmente, il § 220 permette la possibilità di emanare provvedimenti di perquisizione di portata nazionale per le caselle di posta elettronica. Di conseguenza, le autorità di pubblica sicurezza non devono recarsi nel distretto in cui è situato il *Provider* per ottenere un *Warrant* del genere, e i procuratori ed i giudici del distretto nel quale è collocato il *Provider* non hanno alcun controllo sul procedimento di verifica della legittimità del provvedimento richiesto.

L'eccezione viene giustificata con il fatto che i distretti in cui sono situati molti *Provider* (la California del nord, ad esempio) sono stati recentemente inondati di richieste di *Warrant*: ad ogni modo, l'argomento secondo il quale sarebbe più efficiente dividere fra più sedi il compito di emanare provvedimenti di perquisizione sembra piuttosto debole se paragonato alle limitazioni che ne derivano in termini di tutela dei diritti civili. I *Warrant* di perquisizione delle *E-mail* di portata nazionale sollevano seri dubbi rispetto al rischio di attività di *forum shopping* da parte delle forze di pubblica sicurezza (ad es., ricercando un distretto in cui il sentimento popolare o delle autorità giudiziarie sia più favorevole alla concessione di *Warrant*). Più esplicitamente, se un provvedimento di perquisizione venisse emanato da una corte californiana che autorizzasse le ricerche in un piccolo *Provider* con sede a Boston, sarebbe estremamente difficile per il piccolo ISP contestare la legittimità del provvedimento, dal momento che in tal caso questi dovrebbe fornirsi di una tutela legale in California, con considerevole dispendio di denaro e di tempo. Pertanto, è poco probabile che un *Provider* — specialmente se con un volume d'affari limitato — assuma iniziative per proteggere la *privacy* dei propri clienti, mentre è molto più verosimile che si limiti semplicemente ad eseguire il provvedimento. A ciò si aggiungono concreti problemi di notifica delle misure citate ai clienti del *Provider*, con conseguenti violazioni del sistema di pesi e contrappesi che dovrebbe assicurare la conformità del procedimento alle garanzie costituzionali previste in materia. Più in generale, infine, va rilevato come l'eccezionalità delle misure esperibili ai sensi dei §§ 219 e 220 non trovi giustificazione con la motivazione della lotta al terrorismo — sebbene queste siano state presentate come tali agli occhi dell'opinione pubblica —, essendo al contrario utilizzabili in qualunque tipo di indagine, anche quelle prive di quel carattere di straordinarietà che potrebbero eventualmente legittimare le pesanti deroghe alle garanzie costituzionali appena citate[87].

II.5.3. Intercettazioni itineranti (*Roving Wiretapes*) (§ 206 USAPA).

Il Quarto Emendamento è stato tradizionalmente interpretato in modo da esigere che il *Search Warrant* specifichi il luogo della perquisizione. Ciò assicura che il Governo non avvii una raffica di indagini indiscriminate: pertanto, l'autorità di pubblica sicurezza non può utilizzare un *Warrant*

[87] Così R. Billé, «*Patriottismo*» *costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 140, n. 51.

per porre in essere perquisizioni casuali. Per il contesto delle comunicazioni elettroniche, questo significa che le autorità di sicurezza devono indicare esattamente il telefono o il punto di accesso ad Internet da sottoporre ad ordine di *Pen/Trap*, con la conseguenza che un provvedimento di intercettazione itinerante, che segua una persona piuttosto che un particolare apparecchio telefonico o accesso alla Rete, non sarebbe permesso.

Nel 1986 fu introdotta un'eccezione a questo principio, ammettendo che le autorità di sicurezza avrebbero potuto ottenere un provvedimento di intercettazione itinerante ove fossero state in grado di provare al giudice che il sospetto stava intenzionalmente utilizzando degli strumenti tecnologici per contrastare l'efficacia di un tradizionale ordine di *Pen/Trap*. Per poter invocare l'applicabilità di questa eccezione, l'autorità di pubblica sicurezza doveva dimostrare che il sospetto stava deliberatamente cambiando telefono o accesso ad Internet per sfuggire ad una misura di *Pen/Trap*. In tal caso, il giudice avrebbe potuto emanare un provvedimento di « intercettazione itinerante » (*Roving Wiretapes*) per seguire il sospetto da un apparecchio telefonico all'altro. Nel 1998 l'eccezione fu ampliata, in modo che le forze di pubblica sicurezza non avevano bisogno di provare che il sospetto aveva intenzione di ostacolare l'efficacia del provvedimento di intercettazione: di conseguenza, dunque, quando la pubblica autorità affermava che le azioni del sospetto producevano l'effetto di disturbare l'efficienza del *Pen/Trap*, era possibile emanare un provvedimento di intercettazione itinerante prescindendo dalle effettive intenzioni del soggetto sorvegliato.

L'USAPA crea un ambito completamente nuovo per l'applicazione delle intercettazioni itineranti. Il § 206 del *Patriot Act* ne consente infatti l'utilizzo nelle indagini *ex* FISA finalizzate alla raccolta di informazioni. Come già indicato[88], queste intercettazioni sono autorizzate segretamente (dai giudici della *Foreign Intelligence Surveillance Court*), non è previsto che sia soddisfatta la condizione di *probable cause* né che l'autorità di pubblica sicurezza richiedente specifichi quale tipo di comunicazione intenda intercettare: per tutte queste ragioni, il mandato in questione è stato definito « un'autorizzazione in bianco che permette all'FBI di agire indisturbata tra le comunicazioni private di un numero incalcolabile di americani »[89]. Inoltre, dal momento che il già citato § 216 dell'USAPA[90] aumenta le finalità per le quali è possibile richiedere ordini di *Pen/Trap*, includendovi anche informazioni di selezione (*dialing*), circolazione (*routing*) e segnalazione (*signaling*), le intercettazioni itineranti sono ora utilizzabili anche per tracciare il percorso di navigazione in Rete compiuto da un indiziato di reato. Di conseguenza, le autorità di pubblica sicurezza sono autorizzate ad analizzare l'uso di qualunque computer a cui un sospetto abbia mai fatto ricorso. Ad esempio, se nell'ambito di un'indagine su un sospettato l'FBI dispone di un ordine di intercettazione *ex* USAPA per analizzare il percorso di navigazione effettuato sul *Web* attraverso un computer presente in un Internet Café o in

[88] Cfr. *supra*, par. II.2.

[89] R. BILLÉ, « *Patriottismo* » *costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 141, n. 51.

[90] Cfr. *supra*, par. II.3.2.

una biblioteca pubblica, l'FBI è autorizzato a tracciare l'impiego fatto di quel computer, potendo così accedere alle informazioni in esso memorizzate (sotto forma di « *cookies* »[91] e simili) anche da parte di utenti precedenti e successivi al soggetto indagato. Gli altri utenti di quel computer non hanno alcun modo di sapere che l'FBI sta analizzando l'uso di quella macchina, e non riceveranno alcuna informazione del fatto che i loro dati privati sono oggetto di indagini, né da parte delle autorità di sicurezza, né dai gestori del locale in cui è custodito il computer, che devono tenere l'assoluto riserbo a riguardo[92].

Si comprende agevolmente, quindi, come mai siano stati sollevati considerevoli rilievi in merito alla costituzionalità della nuova disciplina delle *Roving Wiretaps*, in primo luogo per via del mancato rispetto del principio costituzionale secondo cui ogni ordine di perquisizione deve indicare precisamente il luogo da perquisire, sancito dal Quarto Emendamento[93]; inoltre, il fatto che tali ordini di intercettazione possano rimanere in vigore per un anno non contribuisce di certo a placare gli animi dei loro detrattori.

II.6. Disposizioni del *Patriot Act* che estendono le capacità del Governo di ottenere accesso ad informazioni private.

II.6.1. Definizioni più ampie del reato di attività terroristica.

Il § 802 dell'USAPA istituisce una definizione per il reato di « terrorismo domestico »: si tratta di una definizione estremamente ampia, in base alla quale qualunque reato che « sembra finalizzato ad intimidire o esercitare coercizioni su una popolazione civile, ad influenzare la politica di un governo attraverso intimidazioni o coercizioni, condizioni l'operato di un governo... » ricade ora nella fattispecie del « terrorismo domestico ». Considerata la vasta gamma delle finalità dei possibili reati, quindi, si crea un'ampia capacità di intervento da parte delle autorità responsabili delle indagini, facilitando la possibilità per gli investigatori di ottenere informazioni private nell'ambito dell'esercizio dell'attività di *intelligence*. Allo stesso modo, il § 808 dell'USAPA aggiunge ulteriori fattispecie alla lista dei delitti che rientrano nel « reato federale di terrorismo ». Di particolare interesse, in questa sede, è l'inserimento di una serie di reati esperibili via computer, che ancora una volta incrementano le finalità che consentono una maggiore ampiezza di intervento alle indagini condotte dal governo.

---

[91] I « *cookies* » (in italiano letteralmente « biscottini ») sono piccoli file di testo che i siti web utilizzano per immagazzinare alcune informazioni nel computer dell'utente. I cookie sono inviati dal sito web e memorizzati sul computer, per poi essere re-inviati al sito web al momento delle visite successive. Le informazioni all'interno dei cookie sono spesso codificate e non comprensibili.

[92] Cfr. EPIC, FISA Page, *op. cit.*

[93] Cfr. *supra*, n. 33.

II.6.2. Riduzione delle tutele previste nel processo penale.

Il § 809 rimuove il limite temporale di otto anni, precedentemente in vigore, per l'esperibilità dell'azione penale relativamente a tutti i crimini federali di terrorismo[94] che minaccino di provocare o abbiano provocato morti o ferimenti gravi. Agli altri reati federali di terrorismo continua di contro ad applicarsi il preesistente termine di otto anni per l'avvio dell'azione penale. Il § 812 dell'USAPA permette invece la sorveglianza di terroristi condannati per le tipologie di reati federali di terrorismo definite nel § 2332 del 18 U.S.C. anche dopo il loro rilascio dalla prigione. In base a questa disposizione, determinate categorie di individui rischiano di rimanere soggette a misure di sorveglianza per tutta la loro vita[95].

II.6.3. Incremento dei poteri della CIA

L'USAPA aumenta considerevolmente il potere di accesso della CIA alle informazioni concernenti i privati cittadini. Tra le numerose occasioni in cui il *Patriot Act* consente di condividere le informazioni raccolte nel corso di indagini figura anche il § 203, il quale permette tra l'altro ai funzionari dell'FBI di condividere informazioni con la CIA quando essi intercettano conversazioni telefoniche e telematiche, senza il bisogno di procurarsi un ordine del giudice per il rilascio di informazioni diffuse in base a questa disposizione. La medesima norma consente alla CIA di passare tali informazioni a governi stranieri, nonostante il grave pericolo che ciò potrebbe rappresentare per i familiari di un sospetto che viva all'estero.

II.6.4. Aumento di spesa per la sorveglianza informatica.

Il § 816 dell'USAPA autorizza la spesa per laboratori di informatica forense. Il provvedimento richiede che il Procuratore Generale individui dei laboratori regionali di informatica forense, e che vengano supportate modalità di investigazione basate su tecniche informatiche applicate all'*intelligence*, in grado di consentire il recupero di informazioni in precedenza cancellate dall'*hard disk* di un computer, nonché il monitoraggio di trasmissioni di dati via Internet. Il § 103 dell'USAPA ha autorizzato la spesa di oltre 200 milioni di dollari all'anno per il triennio 2001-2004 a favore del centro di supporto tecnico dell'FBI, impegnato principalmente nello sviluppo di tecnologie di sorveglianza e nella conduzione di numerose operazioni di vigilanza.

---

[94] Definiti nel dettaglio nel § 2332b(g)(5)(A-B) del 18 U.S.C., successivamente integrato dal §808 dello stesso *Patriot Act*. Secondo tale norma, con « Federal crime of terrorism » deve intendersi « *an offense that [...] is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct* » e che consista nella violazione di una considerevole serie di disposizioni dell'U.S. Code. Il testo della norma è disponibile in *http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002332- - -b000-.html* (3 gennaio 2007).

[95] Cfr. C. Doyle, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, op. cit., p. 52.

II.7. Altri provvedimenti dell'Amministrazione USA in materia di sorveglianza elettronica.

L'emanazione del *Patriot Act* non ha certamente rappresentato l'unica iniziativa assunta dal Governo statunitense in materia di sicurezza seguita agli eventi dell'11 settembre 2001. Sono stati numerosi ed articolati gli interventi di modifica della disciplina della sicurezza da parte dell'Amministrazione Bush, molti dei quali in grado di produrre conseguenze immediate e rilevanti anche in materia di sorveglianza elettronica: è opportuno, quindi, darne conto in questa sede.

In primo luogo, il 20 dicembre 2001 il Governo USA ha istituito un Ufficio di difesa del territorio, incaricato di centralizzare le informazioni e coordinare le azioni di lotta al terrorismo, mentre il 6 giugno 2002 il Presidente Bush ha annunciato la creazione di un nuovo ministero per la sicurezza interna, il *Department of Homeland Security*. Il nuovo ministero accentra le risorse di un numero considerevole tra organismi e servizi già esistenti, disponendo di un budget annuale di 40 miliardi di dollari ed impiegando 170.000 persone: il suo obiettivo principale consiste nell'assicurare la centralizzazione delle informazioni, in particolare attraverso il nuovo obbligo imposto dalla legge a tutte le agenzie federali di *intelligence* (tra cui la CIA, il Dipartimento della Difesa e la *National Security Agency* - NSA) di comunicare al nuovo ministero tutte le informazioni relative alla vulnerabilità dell'infrastruttura tecnica degli Stati Uniti[96]. La nuova disciplina riserva un'attenzione particolare alla gestione dei dati informatici, prevedendo la creazione di uno speciale ufficio di ricerca sulle nuove tecnologie fornito di un budget di 500 milioni di dollari e finalizzato — tra l'altro — a creare gli strumenti per contrastare il crimine informatico. L'8 maggio 2002 è stata inoltre annunciata la creazione di una speciale « cyberdivisione » all'interno dell'FBI, con particolari poteri di indagine in ambito informatico[97].

Come già riportato, dopo gli eventi dell'11 settembre 2001 le intercettazioni delle attività compiute su Internet si sono sviluppate e moltiplicate assai rapidamente[98]: numerosi *Provider* hanno dichiarato di aver ricevuto la richiesta da parte delle autorità di pubblica sicurezza di installare nel proprio apparato informatico il sistema di sorveglianza elettronica *Carnivore*[99], capace tra l'altro di esaminare il contenuto dei messaggi di posta elettronica ed i dati di connessione di un terminale. Prima degli attentati, il *Carnivore* poteva essere utilizzato solamente previa autorizzazione di un giudice, ma grazie al *Combatting Terrorism Act* - CTA, approvato dal Senato USA il 13 settembre 2001, i servizi di sicurezza sono stati esonerati dall'osservanza di tale obbligo. Attraverso il *Patriot Act*, quindi, è stata definitivamente legalizzata la sorveglianza elettronica del *Web*,

---

[96] Cfr. D. Mccullagh, *Bush donne le feu vert à son ministère de la Sécurité intérieure*, ZDNet.Fr-Actualités, 26 novembre 2002.

[97] Per un sunto dell'insieme dei provvedimenti assunti dall'Amministrazione Bush nel quinquennio 2001-2006 riguardo alla « Guerra al Terrore » v. il pamphlet della Casa Bianca 9/11 *Five Years Later: Successes and Challenges*, disponibile in *http://www.whitehouse.gov/nsc/waronterror/2006/* (4 gennaio 2007).

[98] Cfr. *supra*, par. II.2.

[99] Sulla natura e lo scopo di *Carnivore* v. *supra*, par. II.3.2., n. 62.

non solo attraverso le norme esaminate in precedenza, ma anche autorizzando l'FBI ad applicare il sistema *Carnivore* alla rete dei *Provider* allo scopo di controllare la circolazione dei messaggi di posta elettronica e conservare le tracce di navigazione di qualunque individuo sospettato di tenere contatti con una potenza straniera.

Attraverso l'applicazione congiunta di CTA e USAPA, quindi, si raggiunge tra l'altro il particolare effetto di autorizzare una raccolta « preventiva » di informazioni: le indagini, cioè, possono aver luogo anche in mancanza di qualunque effettiva infrazione da parte del sospettato, e a sua totale insaputa; inoltre, dal momento che queste investigazioni sono perfettamente legali, i dati così raccolti possono essere utilizzati anche in un secondo momento, nel caso in cui i soggetti interessati dai provvedimenti di sorveglianza « speciale » siano formalmente sottoposti ad indagine[100].

Il *Cyber Security Enhancement Act* - CSEA[101], approvato definitivamente dal Congresso statunitense il 19 novembre 2002 come misura complementare al *Patriot Act* all'interno dell'*Homeland Security Act*, la legge che ha ridisegnato la disciplina e le competenze nella gestione delle politiche di sicurezza interna[102], ha lo scopo di intensificare il coinvolgimento del settore privato nella tutela della sicurezza interna. Tra l'altro, il provvedimento estende i poteri delle forze di polizia, autorizzandole ad effettuare intercettazioni telefoniche o elettroniche senza mandato giudiziario, come pure di sanzionare l'intrusione in un sistema informatico con una pena che può arrivare anche all'ergastolo laddove l'intrusione — tanto casuale che dolosa — provochi o rischi di provocare la morte di individui[103], mentre ogni atto di pirateria informatica, comprendente anche il mero ingresso non autorizzato in un sistema informatico, *server* o sito governativo, l'utilizzo non autorizzato o il danneggiamento di un computer, è assimilabile ad un'azione terroristica[104]. Con questo provvedimento si vogliono riqualificare le sanzioni previste per gli attacchi informatici, come l'intrusione fraudolenta o la diffusione di virus, in quanto questi reati « mettono gravemente in pericolo la sicurezza nazionale ». Quest'ultima norma consente anche di estendere le prerogative di polizia in materia di intercettazioni telefoniche o di lettura della posta elettronica, autorizzando alcune forme di intercettazione della comunicazione in assenza di una previa autorizzazione giudiziaria. Il progetto autorizza le forze di sicurezza a porre in essere misure di vigilanza, appunto senza autorizzazione di un tribunale, in caso di un « attacco continuato » contro un computer o se « una questione di sicurezza nazionale subisce una minaccia immediata »[105]. In tal caso l'azione di sorveglianza è limitata all'identificazione degli utenti, escludendo l'accesso al contenuto delle *E-mail* — la cui lettura

---

[100] Cfr. J.-C. PAYE, *La fine dello Stato di diritto*, Manifestolibri, Roma 2005, p. 26.

[101] Il testo della norma è consultabile in *http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm* (29 novembre 2006).

[102] Visibile in *http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf* (29 novembre 2006).

[103] Cfr. Sezione 1030(c) del § 18 United States Code così come emendata dal *Cyber Security Enhancement Act*.

[104] T. VERBIEST-E. WERY, *Terrorisme et Internet: vers une dérive sécuritaire?*, in *Droit et nouvelles technologies-Actualités*, 25 marzo 2002, disponibile in *http://www.droit-technologie.org/1_2.asp?actu_id=554* (3 gennaio 2007).

[105] J.-C. PAYE, *La fine dello Stato di diritto*, op. cit., p. 27.

è autorizzata solo in caso di « grave offesa » o nell'ambito della lotta al crimine organizzato. Lo scopo ultimo è anche quello di favorire la collaborazione degli *Internet Provider* con le autorità di pubblica sicurezza, per facilitare l'identificazione dei loro abbonati o utenti in caso di inchieste giudiziarie.

Come è stato opportunamente fatto notare, la riqualificazione dell'intero settore dei reati informatici e delle attività di *hacking* in funzione della lotta alla minaccia terroristica ha comportato uno spostamento della gravità dell'atto illecito dal suo effetto — l'obiettivo che esso persegue — alla sua finalità — ovvero la motivazione per la quale esso è stato posto in essere —, giustificando proprio in virtù di tale passaggio l'aggravamento della sanzione impartita[106]. La lotta al cyberterrorismo riveste un ruolo fondamentale nella strategia seguita dall'Amministrazione Bush in reazione agli attacchi del 2001: il primo Segretario alla Sicurezza Interna Tom Ridge, avvicendato da Michael Chertoff nel 2005, ha dichiarato che il suo dipartimento avrebbe « sorvegliato Internet per rilevare ogni potenziale segnale di attacco terroristico, di cyberterrorismo, di pirateria e di guerra informatica tra gli Stati », precisando che a suo giudizio i cyberterroristi sono pericolosi quanto i loro omologhi tradizionali, e che non si sarebbe operata « alcuna distinzione tra virtuale e fisico all'interno del dipartimento »[107].

Con queste premesse, dunque, non sorprende apprendere che il *Cyber Security Enhancement Act*[108] — secondo alcuni redatto addirittura prima dei fatti dell'11/9/2001 — miri in particolare a favorire la piena collaborazione dei *Provider* con le autorità di pubblica sicurezza, fino a rendere il loro rifiuto pressoché impossibile qualora queste ultime possano « credere in buona fede » nell'esistenza di un reato[109]. Peraltro, una tale « richiesta di collaborazione » diventa ora esperibile non solo per le autorità giudiziarie, ma anche per un qualunque organo facente parte di un'amministrazione — federale, statale o municipale —, comprendendo dunque non solo i servizi di polizia, ma anche categorie di soggetti tra le più disparate, come direttori scolastici, lettori universitari, centri di malattie contagiose o impiegati di una biblioteca municipale.

Il Dipartimento della Difesa ha intanto avviato un nuovo progetto, il *Total Information Awareness*, pubblicizzato come un'ulteriore forma di applicazione delle nuove tecnologie alla lotta al terrorismo: lo scopo ultimo consisterebbe nel porre in relazione banche dati diverse, come gli archivi creati da istituti di credito, agenzie assicurative o società di autonoleggio, per smascherare eventuali cospirazioni terroristiche. Anche in questo caso, dunque, quello che colpisce è l'approccio indiscriminato che muove il provvedimento, tale per cui le indagini realizzate non prendono l'avvio da un effettivo pericolo imminente per la collettività: un rischio indeterminato o una minaccia virtuale sono condizioni sufficienti per giustificare le ricerche, con una assoluta inesistenza di controlli giudiziari, sia a priori che a posteriori dell'iter procedurale[110]. Non si rende infatti necessario al-

---

[106] *Ibid.*

[107] D. Mccullough, *La cyberterreuer et les paranoïaques professionells*, ZDNet.Fr/Actualités, 29 marzo 2003, *op. cit.* in J.-C. Paye, op. cit., p. 27.

[108] H.R. 3482 CSEA.

[109] J.-C. Paye, *La fine dello Stato di diritto*, op. cit., p. 28.

[110] Electronic Frontier Foundation Action Center, http://action.eff.org/site/

cun mandato per avviare le investigazioni, né sussistono obblighi di informarne giudici o altri organi istituzionali: l'unico dovere consiste nel dare informazioni al Dipartimento di Giustizia dopo tre mesi dall'avvio delle indagini. Inoltre, le misure di controllo finiscono per risultare del tutto svincolate dalle specifiche categorie di reati che ufficialmente esse intendono combattere: un semplice utilizzo di mezzi informatici anche solo per la comunicazione di un reato consente infatti il ricorso alle tecniche di sorveglianza elettronica, sebbene la minaccia che si prospetta non rischi in alcun modo di arrecare danni ad infrastrutture telematiche. In altre parole, sia le tipologie di illecito perseguite che le categorie di soggetti potenzialmente sanzionabili risultano del tutto svincolate dalle finalità che il provvedimento intende ufficialmente perseguire, ovvero l'impiego delle tecnologie informatiche da parte di organizzazioni terroristiche per finalità eversive. L'effetto ultimo di tutto questo si traduce in una potenziale sorveglianza assolutamente indiscriminata di qualunque uso fatto di un computer connesso alla Rete, qualora un componente di una delle categorie di soggetti autorizzati lo ritenga necessario.

Tutte le azioni preventive e difensive rispetto ad un attacco informatico sono coordinate da una speciale struttura, il *National Infrastructure Protection Center*, istituito non da una legge ma da un decreto governativo, e del tutto irresponsabile sul piano penale o civile per le informazioni raccolte[111]. Secondo alcuni, il Governo di Washington si sarebbe in questo modo trasformato in una sorta di « poliziotto globale della Rete »[112], in particolare attraverso il diritto unilateralmente attribuito al Dipartimento della Giustizia statunitense di perseguire presunti pirati informatici — ma non solo loro, come detto — qualunque sia la loro nazionalità ed il luogo in cui il reato viene posto in essere: le leggi del Congresso diventerebbero così universali nella misura in cui la maggior parte del traffico mondiale su Internet passa per gli Stati Uniti, dovendo pertanto sottostare alle regole della loro giurisdizione[113].

III.1. Le reazioni alla reazione: oltre il *Patriot Act*.

Come era lecito attendersi, l'impatto del *Patriot Act* sull'ordinamento statunitense è stato talmente eclatante che le reazioni al provvedimento non potevano essere da meno: probabilmente anche a causa del progres-

PageServer?pagename=ADV_homepage (3 gennaio 2007).

111 A. Ramasastry, *The Cyber Security Enhancement Act's Good faith disclosure exemption: A Serious Threat to Individual Privacy*, 28 marzo 2002, in *http://writ.corporate.findlaw.com/ramasastry/20020328.html* (3 gennaio 2007).

112 J.-C. Paye, *La fine dello Stato di diritto*, op. cit., p. 30.

113 Emblematico, da questo punto di vista, l'episodio della Somalia, rimasta scollegata per due mesi dalla Rete: dal novembre 2001 al gennaio 2002, infatti, gli Stati Uniti hanno costretto l'unico *Internet Provider* del Paese, *Somalia Internet Company*, e la principale impresa di telecomunicazioni, *Al-Barakaat*, ad interrompere le proprie attività, in quanto inserite in una lista di organizzazioni sospettate di finanziare il terrorismo. Solo con l'ingresso nel mercato informatico di un nuovo operatore, *NetXchange*, è stato possibile riaprire alla Somalia le porte del *Web*. La vicenda è riportata in Reporters Sans Frontières, *Internet en liberté surveillée*, op. cit., p. 7.

sivo ridimensionamento del consenso mostrato dall'opinione pubblica nei confronti del provvedimento, soprattutto per via delle considerevoli ingerenze che questo ha comportato in materia di garanzie costituzionali, gli organismi istituzionali — con le corti in primo piano, come spesso è accaduto in situazioni emergenziali nella storia degli Stati Uniti — hanno gradualmente iniziato a far uso delle proprie prerogative, sollevando negli specifici ambiti di competenza interrogativi sempre più pressanti sulla legittimità della norma in questione, e operando per porre fine a quelle che, ai loro occhi, figuravano come forme illegittime di esercizio del potere politico.

III.2. Il ruolo dei giudici.

Emblematica rispetto allo specifico rapporto tra sicurezza e libertà digitale, esaminato in questa sede, è la vicenda del pronunciamento della *United States District Court Southern District of New York*[114], con cui i giudici hanno valutato il citato § 505 dell'USAPA[115] in contrasto con i requisiti costituzionali sanciti dal Primo e dal Quarto Emendamento, e ciò nonostante nella sentenza si riconosca che « la sicurezza nazionale » costituisce « un valore supremo ed indiscutibilmente una delle più alte finalità per le quali si istituisce un Governo sovrano »[116]. Al valore della « sicurezza nazionale » i giudici hanno contrapposto nell'occasione un altro principio ritenuto di eguale rilevanza, ovvero la « sicurezza personale », intesa come garanzia di fronte a possibili imposizioni da parte del Governo che limitino irragionevolmente diritti fondamentali riconosciuti e protetti dal *Bill of Rights*[117]. Richiamandosi ad una posizione a più riprese ribadita anche dalla Corte Suprema, secondo la quale « uno stato di guerra[118] non può essere considerato un assegno in bianco per il Presidente quando si ha a che fare con i diritti dei cittadini della nazione » e « persino il potere di guerra non rimuove le limitazioni costituzionali a salvaguardia di libertà essenziali »[119], la Corte federale di Distretto di New York ha quindi stabilito come in un Paese democratico sia compito del potere giudiziario veri-

[114] Cfr. *John Doe v. John Ashcroft*, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).

[115] V. *supra*, Par. II.3.6.

[116] *John Doe v. John Ashcroft*, cit.

[117] Cfr. in proposito P. Torretta, « *Diritto alla sicurezza* » *e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, *op. cit.*, p. 464, che in particolare parlando di una concezione multidimensionale della sicurezza osserva come la legislazione d'emergenza, nell'intento di proteggere la dimensione positiva del diritto alla sicurezza da parte dell'Esecutivo statunitense, abbia prevaricato la componente negativa (tipica della nozione di libertà), « che, invece, nella sua accezione di sicurezza dei diritti e quindi giuridica, impedisce che interferenze dei pubblici poteri possano ledere la sfera di libertà dei cittadini ».

[118] Per una valutazione sull'ingerenza della legislazione di guerra sugli standard di tutela dei diritti costituzionali nell'ordinamento degli Stati Uniti v. F. Lanchester, *Gli Stati Uniti e l'11 Settembre 2001*, in www.associazionedeicostituzionalisti.it (3 gennaio 2007); T.E. Frosini-C. Bassu, La libertà personale nell'emergenza costituzionale, in A. Di Giovine (a cura di), Democrazie protette e protezione della democrazia, Giappichelli, Torino 2005, pp. 79 ss.; T.E. Frosini, *C'è un giudice (anche) a Guantánamo*, in *Diritto Pubblico Comparato ed Europeo*, n. 3/2006.

[119] Cfr. *Home Buildings & Loan Ass'n v. Blaisdell*, 290 U.S. 398, 426 (1934) ma soprattutto, anche per l'attualità della decisione, *Hamdi v. Rumsfeld*, 124 S. Ct. 2633, 2650 (2004).

ficare che tale bilanciamento venga realizzato nel modo più coerente e rispettoso degli equilibri costituzionali, per mezzo di un'analisi caso per caso della situazione, in modo da poter adeguatamente valutare di volta in volta a quale dei due principi concedere maggior peso, senza imporre assiologicamente criteri valutativi assoluti che non dovrebbero trovare spazio in un giudizio teso a conciliare due valori costituzionali di pari grado[120]. La decisione prosegue osservando come, sebbene un giudice debba sempre mantenere la massima attenzione verso l'esigenza espressa dal Governo di garantire la sicurezza nazionale — un principio che, ove se ne riscontrasse l'esistenza, potrebbe anche giustificare la temporanea sospensione di un particolare diritto costituzionale, abitualmente prevalente rispetto ad altre esigenze —, l'ultima parola in merito al bilanciamento da effettuare spetti comunque ai giudici, poiché solo in questo modo si potrà ripristinare quel sistema di *checks and balances* alla base del funzionamento dell'ordinamento costituzionale statunitense[121]. L'esperibilità, consentita dal § 505 dell'USAPA, di un provvedimento amministrativo — la *National Security Letter* — finalizzato al conseguimento di documenti su esclusiva iniziativa dell'Esecutivo, senza una pronuncia di convalida da parte dell'autorità giudiziaria[122] considerata fondamentale dalla Corte per la rivendicazione dei diritti sanciti dalla Costituzione, unitamente al fatto di avere imposto al destinatario di una NSL un assoluto divieto di rivelare quanto ricevuto, senza offrirgli la possibilità di chiedere assistenza legale per la tutela dei propri diritti se non attraverso una rischiosa contestazione del provvedimento[123], finiscono così per porre la norma impugnata in contrasto insanabile con i principi sanciti nel Primo e nel Quarto Emendamento. La vicenda, naturalmente, non si è esaurita

[120] V. in proposito anche la decisione *John Doe v. Alberto Gonzales*, 368 F. Supp. 2d 66, 82 (D. CONN. 2005), anch'essa riguardante il § 505 del *Patriot Act* e di cui si dirà più ampiamente fra breve.

[121] Nella motivazione della sentenza redatta dal Giudice federale Victor Marrero si legge: « la democrazia aborre la segretezza ingiustificata, riconoscendo che la pubblica consapevolezza assicura la libertà. Pertanto, un illimitato potere di indagine del Governo [che costituisce] in effetti una forma a se stante di segretezza, non può trovare posto nella nostra società. [...] Occultata sotto il mantello della segretezza, l'autoconservazione che in tempi di normalità permette al nostro Governo di praticare la censura e la segretezza può potenzialmente essere rivolta contro di noi come un'arma di distruzione di massa », cfr. *John Doe v. John Ashcroft*, cit., 519-520.

[122] Durante il giudizio i rappresentanti del Dipartimento di Giustizia hanno smentito il fatto che i destinatari di una *National Security Letter* non abbiano possibilità di ricorrere all'autorità giurisdizionale, pur ammettendo che la norma impugnata risulta di difficile interpretazione sul punto. In verità, come è stato sottolineato in precedenza, il § 505 prevede esplicitamente che tutti i soggetti coinvolti nel provvedimento di NSL siano tenuti al massimo riserbo in proposito: stando così le cose, non si vede come un soggetto destinatario di tale misura possa esserne informato, e quindi agire in giudizio contro la sua legittimità, prima di essere a sua volta oggetto di provvedimenti di polizia e giudiziari proprio sulla base delle informazioni eventualmente in tal modo conseguite dalle autorità responsabili delle indagini, così anche C.P. RAAB, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties?*, op. cit., p. 89.

[123] In realtà, proprio in considerazione dei rischi che un'azione legale del genere poteva comportare, il promotore della controversia ha scelto di mantenere l'anonimato, ricorrendo ad un nome di fantasia (John Doe) per quanto riguarda le generalità da fornire nel procedimento: « John Doe » è il nome fittizio che solitamente si adopera negli Stati uniti quando non si intendono fornire le effettive generalità di un individuo.

con tale decisione, avendo le autorità governative presentato appello contro la sentenza di primo grado.

Come già accennato, sempre rispetto alla costituzionalità del § 505 del *Patriot Act* è intervenuta una seconda sentenza presso una Corte federale del Connecticut[124], nella quale il giudice ha ritenuto che il divieto di informare altre persone sulla ricezione di una NSL da parte del destinatario poteva essere considerato legittimo solo laddove l'interesse contrapposto fosse consistito in un « *compelling state interest* »[125]; ciononostante, sebbene nel caso in esame dovesse ritenersi sussistente l'interesse del Governo a proteggere il Paese dalla minaccia terroristica, questo non ha costituito a giudizio della Corte prova sufficiente per dimostrare che il divieto citato fosse necessario per motivi di sicurezza nazionale. Anche in questa decisione, peraltro, è stato ribadito come l'assenza di una revisione da parte dell'autorità giurisdizionale della fondatezza del provvedimento amministrativo producesse un'indebita violazione del Primo emendamento[126]; soprattutto, il Giudice ha rilevato la difficoltà di verificare la conformità alla legge dell'esercizio dei poteri conferiti dalla norma impugnata alle forze di sicurezza, e quindi di prevenire eventuali abusi[127]. Il 20 settembre 2005 una Corte d'Appello federale del II Circuito ha deciso in prima battuta di mantenere in via temporanea quanto statuito dal Giudice di primo grado, osservando che, in caso contrario, il ricorso del Governo avrebbe dovuto essere dichiarato « *moot* »[128], in quanto l'identità del ricorrente nel giudizio di prima istanza — come detto, fino a quel momento celata sotto lo pseudonimo di « *John Doe* » — ed il contenuto della NSL ivi impugnata sarebbero state inevitabilmente rivelate. Ad ogni modo, riconoscendo una qualche fondatezza ai timori delle parti interessate che un'attesa eccessiva avrebbe impedito al caso di svolgere un ruolo rilevante nel dibattito sull'opportunità della reiterazione del *Patriot Act*, la Corte d'Appello ha poi provveduto a fissare un termine per lo svolgimento del processo[129]. Nel marzo 2006, a seguito dell'emanazione della legge di reitera-

---

[124] *John Doe v. Alberto Gonzales*, cit.

[125] In questo senso già *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984), che statuisce inoltre come i mezzi con i quali si sceglie di perseguire tale interesse devono essere i meno restrittivi della libertà di credo ed associazione tra quelli utilizzabili.

[126] Nell'intento di ribadire la legittimità della magistratura di assicurare un controllo sui poteri dell'Esecutivo, il Giudice Janet Hall ha precisato: « l'idea che il potere giudiziario dovrebbe abdicare alle proprie responsabilità decisorie in favore dell'Esecutivo ogni qual volta sorgano problemi in materia di sicurezza nazionale è estremamente pericolosa », *ibid.*, 15.

[127] « Le potenzialità per commettere degli abusi sono scritte nella stessa legge: alle persone che potrebbero effettivamente avere informazioni su abusi investigativi è preventivamente vietato di condividere queste informazioni con la collettività e con i titolari del potere legislativo che forniscono all'Esecutivo gli strumenti utilizzati per indagini in materia di sicurezza nazionale », *ibid.*, 26.

[128] Nel diritto processuale statunitense un caso è considerato « *moot* » (irrilevante) se ulteriori procedimenti giudiziari che lo riguardano possono non produrre effetti, di modo che la materia finisce per essere privata di rilevanza pratica: in un tale frangente, il caso deve essere respinto dall'autorità giudiziaria, in quanto secondo l'art. 3 della Costituzione degli Stati Uniti la giurisdizione delle Corti federali è limitata a « casi e controversie », per cui un'azione legale o un ricorso in appello rispetto a cui la decisione di una Corte non incide sulla condizione delle parti finisce per essere al di fuori delle materie di competenza della Corte stessa.

[129] Malgrado nel complesso possa essere interpretata come sfavorevole alle posizioni dell'Esecutivo, la deliberazione non

zione di buona parte dell'USAPA[130], che prevede tra l'altro un meccanismo di revisione giurisdizionale delle *National Security Letters* e dei loro ordini di esecuzione, l'Amministrazione Bush ed la Corte d'Appello hanno in ultimo convenuto di dichiarare concluso il ricorso governativo nell'appello contro *Doe v. Gonzales*. L'Esecutivo ha inoltre tentato di persuadere i Giudici di secondo grado a sospendere anche la sentenza della Corte del Connecticut, così che questa non potesse costituire un precedente nella controversia questione del rapporto tra libertà e sicurezza: i Magistrati hanno tuttavia respinto la richiesta, osservando che al Governo non dovrebbe essere concesso di ribaltare una sentenza sgradita semplicemente cambiando opinione e tentando di rendere nullo (« *moot* ») il caso; la citata revisione del *Patriot Act* ha inoltre offerto l'occasione agli stessi Giudici per dichiarare concluso anche il ricorso inoltrato dall'Esecutivo contro la sentenza di primo grado in *Doe v. Ashcroft*[131].

Un duro colpo per le posizioni propugnate dall'Esecutivo in materia di sorveglianza elettronica è poi venuto dalla decisione di una Corte Federale del distretto di Detroit[132] che ha dichiarato incostituzionale il programma di intercettazioni privo di controlli giurisdizionali approntato dalla *National Security Agency* (NSA) nel 2001, con cui per sua stessa ammissione la Casa Bianca ha autorizzato l'intercettazione di centinaia di migliaia di telefonate e di e-mail di cittadini statunitensi[133]. Nella sentenza, emanata il 17 agosto 2006, il Giudice Anna Diggs Taylor conduce una vibrante requisitoria contro le recenti politiche perseguite dal Governo in materia di sicurezza: richiamandosi a pietre miliari della storia giurisprudenziale, sia del periodo coloniale che di quello successivo alla fondazione degli Stati Uniti[134], il Giudice Taylor ricorda in primo luogo come anche il Presidente sia una creatura della stessa Costituzione che ha prodotto il Primo ed il Quarto Emendamento, a suo giudizio violati dal citato piano di intercettazioni elettroniche segrete[135]. Aderendo alla catalogazione dei poteri presidenziali rispetto agli orientamenti del Congresso, mirabilmente descritta in un'opinione concorrente dal *Justice* Robert H. Jackson nella citata *Youngstown Sheet & Tube v. Sawyer*[136], la sentenza sostiene poi come,

ha mancato di suscitare critiche tra gli stessi oppositori delle NSL: Ann Beeson, uno dei legali della ACLU, ha descritto come « estremamente frustrante » la delibera, in quanto « il Governo può dire quello che vuole sul *Patriot Act*, ma non gente come i ricorrenti [nel dibattimento in oggetto], che hanno una conoscenza diretta dei suoi effetti », cit. in N. TRIVEDI, *Section 215 of the USA PATRIOT Act and National Security Letters: An Update*, *op. cit.*

[130] In proposito v. più ampiamente *infra*, in questo par.

[131] N. TRIVEDI, *Section 215 of the USA PATRIOT Act and National Security Letters: An Update*, *op. cit.*

[132] *American Civil Liberties Union v. National Sec. Agency*, 438 F.Supp.2d 754.

[133] « *Usa, giudice dichiara incostituzionali le misure antiterrorismo di Bush* », Repubblica.it, 17 agosto 2006.

[134] Tra cui *Entick v. Carrington*, 95 Eng. Rep. 807 (1765) (!);, 343 U.S. 579 (1952); *U.S. v. U.S. District Court*, 407 U.S. 297 (1992); *Clinton v. Jones*, 520 U.S. 681 (1997); *Hamdi v. Rumfseld*, 542 U.S. 507 (2004).

[135] *American Civil Liberties Union v. National Sec. Agency*, cit.. A questo proposito, rigettando l'argomentazione dei « poteri impliciti » (« *ineherent powers* ») del Presidente, invocata dai legali del Governo, il Giudice Taylor ribatte che « lo stesso Ufficio del Capo dell'Esecutivo è stato creato, con i suoi poteri, dalla Costituzione. In America non esistono sovrani ereditari e nessun potere che non sia stato creato dalla Costituzione. Pertanto, tutti i ''poteri impliciti'' devono derivare da quella Costituzione », *ibid.*, p. 40.

[136] Nell'occasione il Giudice Jackson aveva decretato che le materie che investo-

nel momento in cui le misure di sorveglianza elettronica vengono sottratte al necessario controllo giurisdizionale — sia pure speciale — della Corte FISA, previsto per legge, il Presidente agisca in palese violazione del *Foreign Intelligence Surveillance Act*, che rappresenta la consolidata prassi legislativa del Congresso in materia: pertanto, le sue potestà sono ridotte al minimo (« *at its lowest ebb* »)[137] e non possono essere considerate legittime. Ove si accogliessero le posizioni del Governo, e si ammettesse la legalità del programma di intercettazioni impugnato nella vicenda in oggetto, l'operato dell'Esecutivo risulterebbe immune dal controllo giudiziario: poiché « non è mai stata intenzione dei padri della Costituzione degli Stati Uniti di concedere al Presidente un tale illimitato controllo, soprattutto quando le sue azioni contrastano in modo così evidente con i parametri chiaramente enumerati nel *Bill of Rights* »[138], la decisione sancisce l'immediata obbligatoria conclusione del provvedimento di sorveglianza elettronica[139]. Le reazioni dell'Esecutivo non si sono fatte attendere: in primo luogo, il Governo ha convocato il Giudice Taylor per un'udienza in merito alla sua decisione il 7 settembre 2006, ciò che sospende gli effetti della decisione fino a quel momento; i legali della ACLU — che figura tra i proponenti del ricorso — hanno comunque dichiarato che si opporranno a qualunque ulteriore tentativo di dilazione dell'attuazione della sentenza[140]. Di contro, esponenti dell'Esecutivo hanno espressamente manifestato l'intenzione di battersi affinché la decisione sia ribaltata in successivi gradi di giudizio, poiché a loro parere una sua effettiva applicazione indebolirebbe gli apparati difensivi del Paese[141]. Quale sia stata poi la via effettivamente scelta dall'Esecutivo per rispondere alla decisione del Giudice Taylor si dirà tra breve[142].

---

no la potestà di agire dell'Esecutivo possono essere divise in tre categorie, a seconda se: 1) il Congresso abbia espressamente o implicitamente autorizzato l'atto del Presidente, 2) abbia taciuto sulla questione, o 3) abbia esplicitamente o implicitamente posto in essere atti incompatibili con l'iniziativa dell'Esecutivo. Gli atti rientranti nella terza categoria sollevano le problematiche più complesse, dal momento che un Presidente che intenda esercitare la propria autorità persino in presenza di una esplicita opposizione del Congresso finirà sempre per porsi in qualche misura in conflitto con il sistema costituzionale statunitense di pesi e contrappesi, cfr. *Youngstown*, 343 U.S., 636-638.

[137] *Ibid.*, 637.

[138] *American Civil Liberties Union v. National Sec. Agency*, cit.

[139] Significativamente, la decisione termina citando un suggestivo passo di una sentenza redatta dal *Justice* Warren, il quale nel 1967 osservava: « *Implicit in the term "national defense" is the notion of defending those values and ideas which set this Nation apart [...] it would be ironic if, in the name of national defense, we would sanction the subversion of [...] those liberties [...] which makes the defense of the Nation worthwhile* », *U.S. v. Robel*, 389 U.S. 258, 264 (1967).

[140] « È un altro chiodo nella bara dell'unilateralismo dell'Esecutivo », ha commentato Jameel Jaffer, uno dei legali della ACLU, accomunando la decisione a quelle emesse dalla Corte Suprema nel giugno 2004 in merito alla detenzione di « combattenti nemici » nella base militare di Guantánamo a Cuba, cfr. A. LIPTAK-E. LICHTBLAU, *Judge Finds Wiretap Actions Violate the Law*, in *New York Times*, 18 agosto 2006.

[141] Il Procuratore Generale Alberto R. Gonzales, uno dei principali artefici del programma di intercettazioni elettroniche, si è dichiarato convinto della costituzionalità del provvedimento, mentre il Deputato Repubblicano Peter Hoekstra, Presidente del *Intelligence Committee* della Camera dei Rappresentanti, ha commentato: « È deludente che un giudice si assuma la responsabilità di disarmare l'America in tempo di guerra », *ibid.*

[142] V. *infra*, par. III.3.

III.3. Le risposte della politica.

È stato in precedenza sottolineato come la provvisorietà delle restrizioni alla libertà personale sancite dal *Patriot Act* abbia costituito uno degli argomenti principali espressi a sostegno di un'approvazione in tempi rapidi del provvedimento, la cui temporaneità avrebbe dovuto nelle intenzioni dei suoi promotori bilanciarne l'eccezionalità, giustificandone l'adozione agli occhi dell'opinione pubblica[143]: alla fine del 2005, quando buona parte delle *sunset provisions* erano destinate a decadere ove non fossero state reiterate secondo le modalità previste dalla legge, il dibattito istituzionale sull'opportunità di un prolungamento delle limitazioni sancite dall'USAPA ha inevitabilmente raggiunto il suo apice. Dopo una prima fase in cui i due rami del Congresso hanno lavorato separatamente ad una nuova versione del provvedimento, senza peraltro raggiungere una posizione comune[144], si è proceduto a convocare una commissione che riunisse rappresentanti delle due Camere con la speranza di addivenire ad un compromesso sul punto. Le speranze dell'Amministrazione Bush di ottenere in tempi rapidi una reiterazione del *Patriot Act* subirono tuttavia una cocente delusione quando il 16 dicembre 2005 il prodotto della citata *Joint Conference Committee* fu respinto dal Senato, e questo malgrado il testo sul

[143] Cfr. *supra*, par. II.1.

[144] Ad aprire le attività di rielaborazione del *Patriot Act* è stata la Camera dei Rappresentanti, che il 21 luglio 2005 ha approvato l'« *USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005* » (H.R. 3199) con 257 voti a favore e 171 contrari (il testo del provvedimento è disponibile in *http://thomas.loc.gov/cgi-bin/query/D?c109:3:./temp/~c109WrJOaP::* (3 gennaio 2007). Per quel che concerne le libertà digitali, quella norma conteneva un emendamento proposto da Jeff Flake (Repubblicano eletto in Arizona) adottato con 402 voti favorevoli contro 26 contrari, che prevedeva l'obbligatorietà dell'approvazione personale da parte del Direttore dell'FBI di tutte le richieste di perquisizione ai sensi del § 215 riguardanti i dati in possesso di biblioteche o librerie, mentre rendeva definitivamente permanenti 14 delle 16 *sunset provisions* del *Patriot Act*. Un emendamento che mirava semplicemente a reiterare tali disposizioni, stabilendo la necessità di riesaminare dopo ulteriori quattro anni l'opportunità di una loro abolizione, fu sconfitto di misura (218 contrari e 209 a favore). Il 29 luglio 2005 è stata la volta del Senato di emanare una propria versione della norma di reiterazione del *Patriot Act* (S. 1389), che per quanto concerne il § 215 esigeva la dimostrazione di un effettivo fondamento per le richieste di provvedimenti ai sensi della norma citata, con un atteggiamento nettamente più orientato a favore di una concreta tutela delle libertà fondamentali potenzialmente coinvolte nel procedimento rispetto agli orientamenti presenti nell'omologo provvedimento della Camera dei Rappresentanti. Tale impressione veniva confermata anche da altre norme di dettaglio del S. 1389, come: 1) la possibilità per i destinatari di un provvedimento *ex* § 215 di consultare un legale e di impugnarne la legittimità di fronte ad una Corte FISA; 2) la necessità che il funzionario richiedente un provvedimento *ex* § 215 descrivesse dettagliatamente le informazioni ed i materiali ricercati: 3) l'obbligatorietà per il Dipartimento di Giustizia di presentare annualmente un rapporto con il numero di richieste di perquisizioni e sequestri inoltrate a biblioteche e librerie; 4) soprattutto, la reiterazione dell'intero provvedimento solamente fino al 2009 — in luogo di una sua approvazione definitiva, accolta invece nel progetto approvato alla Camera. Il S. 1389 si occupava anche del § 505 del *Patriot Act*, consentendo al destinatario di una *National Security Letter* di notificarne il contenuto ad un legale e, sia pure in un numero limitato di casi, di contestarne la legittimità in sede giurisdizionale. Da notare, comunque, come non rientrando tra le *sunset provisions* del *Patriot Act*, il § 505 non avesse comunque bisogno di ulteriori autorizzazioni per rimanere in vigore anche dopo il 31 dicembre 2005.

quale si era raggiunto l'accordo in commissione avesse tenuto conto del citato orientamento della Camera degli Stati, più incline a difendere le libertà fondamentali di quanto non facesse il progetto inizialmente elaborato dalla Camera bassa.

Il 22 dicembre successivo, ormai in prossimità di una sua scadenza definitiva, il Congresso aveva comunque provveduto ad accordare alla legge una « mini-proroga » di un mese, rinviando al 3 febbraio 2006 la discussione sulla sorte delle *sunset provisions*, per poi concedere una seconda autorizzazione temporanea di altri trenta giorni. La controversa vicenda ha quindi raggiunto un punto fermo nei primi giorni di marzo, quando i due rami del Parlamento statunitense hanno raggiunto un accordo, emanando separatamente leggi che rendono permanenti buona parte delle norme soggette a scadenza[145]. Per quel che rileva in questa sede, la nuova versione del *Patriot Act* costituisce certamente un passo indietro rispetto ai tentativi di miglioramento in termini di una maggiore attenzione alle libertà civili proposti soprattutto dal Senato nel confronto istituzionale esperito nella seconda parte del 2005, e conclusosi appunto con il mancato rinnovo del provvedimento nei tempi richiesti dall'Esecutivo. Un esempio particolarmente efficace è rappresentato dal § 215, che sebbene nell'ultima versione mantenga la sua natura provvisoria — essendo ancora prevista nel 2009 una nuova deliberazione in merito alla prosecuzione della sua validità — e continui a consentire ai destinatari di una richiesta di perquisizione o sequestro ai danni di un cittadino statunitense di consultare un legale — senza doverne preventivamente rivelare l'identità all'FBI — per contestarne la legittimità di fronte ad una *Foreign Intelligence Surveillance Act Court*[146], impone ora di attendere un anno dall'emissione del provvedimento prima di poter procedere in tal senso nella speciale sede giurisdizionale: in questo modo si congela il dibattito sulla regolarità di una disposizione pesantemente invasiva delle libertà personali di un cittadino nel momento più importante, quello della sua effettiva attuazione, dilazionando di ben dodici mesi qualunque possibile verifica giurisdizionale. Questa, qualora fosse effettivamente esperita e accogliesse le remore dei ricorrenti, si tradurrebbe fatalmente in una ben congegnata beffa a favore

[145] In particolare, il 2 marzo il Senato ha approvato il « *Usa Patriot and Terrorism Prevention Reauthorization Act of 2005* », mentre la Camera dei Rappresentanti ha fatto altrettanto la settimana successiva con il « *Usa Patriot Act Additional Reauthorizing Amendments Act of 2006* » (S. 2271), http://thomas.loc.gov/cgi-bin/query/D?c109:2:./temp/~c109Z3SM0S:: (4 gennaio 2007). Per quanto rileva in questa sede, il provveddimento modifica la normativa precedente in tre punti principali relativi a ai destinatari di un ordine *ex* § 215 del *Patriot Act* o di una *National Security Letter*: 1) è riconosciuto loro il diritto di ricorrere ad un giudice FISA per ottenerne la modifica o sospenderne le disposizioni relative agli obblighi di notifica di informazioni in loro possesso; 2) è eliminato l'obbligo a loro carico di notificare all'FBI o ad altre autorità di Governo l'identità del legale al quale si siano rivolti per avere assistenza relativa all'eventuale ricorso da presentare al giudice FISA; 3) le librerie che offrano anche servizi di accesso ad Internet sono esentate dal regime delle *National Security Letters*, a meno che non operino come *Internet Services Provider*.

[146] Come poc'anzi riportato, l'iniziale proposta di riforma del *Patriot Act* elaborata dal Senato vedeva proprio in questa disposizione una delle principali garanzie rispetto ai possibili abusi del § 215 da parte dei servizi di sicurezza; cfr. *supra*, nota 144.

dell'Esecutivo, comunque lasciato libero di utilizzare per un anno a proprio piacimento dati personali conseguiti in modo illegittimo[147].

III.4. Il *Patriot Act* oltre il « viale del tramonto ».

L'intensità con la quale sia a livello istituzionale che mediatico si è affrontato il tema del rapporto tra sicurezza e libertà digitali in occasione del dibattito sulla reiterazione delle *sunset provisions* del *Patriot Act* ha indotto alcuni ad esprimere posizioni fiduciose nei confronti della capacità dell'opinione pubblica statunitense di riprendere il controllo della situazione quando gli organi istituzionali sembrano aver abusato oltre i limiti consentiti delle loro prerogative: in particolare, la vicenda in questione costituirebbe la prova della necessità che « una risposta al terrore di questo tipo non può essere presa, senza l'avallo, immediato o comunque tempestivo, della società civile »[148]. La cautela mostrata dal Congresso al momento di affrontare il riesame di una disposizione profondamente invasiva delle libertà fondamentali degli individui sarebbe quindi l'effetto della pressione esercitata in tal senso da un'opinione pubblica nel suo complesso non più disposta a subire passivamente le intemperanze commesse dal « *Commander in chief* » in nome della salvaguardia della nazione[149]. A ben guardare, tuttavia, sussistono svariate ragioni che impediscono di condividere tanto ottimismo. L'argomentazione appena esposta parte infatti dall'assunto che l'elemento decisivo in tutta la vicenda delle restrizioni alle garanzie costituzionali statuite dal *Patriot Act* sia rappresentato dall'imprescindibilità di un avallo consapevole in tal senso da parte della società civile: in altre parole, ove i cittadini si fossero dimostrati solidali con le posizioni propugnate dall'Amministrazione Bush fin dall'indomani dell'11 settembre 2001, le limitazioni alle loro libertà personali avrebbero dovuto considerarsi legittime ed una loro eventuale reiterazione in sede parlamentare poco meno di un atto dovuto. Una tale posizione, tuttavia, tralascia di considerare le critiche espresse in varie sedi giurisdizionali in merito a molte delle disposizioni contenute nel *Patriot Act*, nonché alla generale impostazione scelta dal Governo nell'ambito della cosiddetta « guerra al terrore »[150]: quale effetto avrebbero dovuto produrre tali cen-

[147] Cfr. The Free Expression Policy Project, *Patriot Act Reforms Are Defeated*, in *http://www.fepproject.org/news/patriotactmarch2006.html* (3 gennaio 2007).

[148] Così R. Billé, « *Patriottismo* » *costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 154.

[149] « Gli Stati Uniti hanno sentito la necessità di reagire e hanno compreso che al pericolo del terrorismo non doveva in ogni modo affiancarsi il pericolo di un governo liberticida » [...] « I valori rimessi in discussione erano, pertanto, troppo alti e decisivi per la stessa sopravvivenza della democrazia perché non vi fosse un'inversione di tendenza da parte dell'opinione pubblica », *ibid.*, p. 153.

[150] Valga per tutti l'osservazione del *Justice* Sandra O'Connor in *Hamdi v. Rumsfeld*, secondo cui « uno stato di guerra non rappresenta un assegno in bianco (*a blank check*) in favore del Presidente, quando sono in gioco i diritti dei cittadini degli Stati Uniti », cfr. *Hamdi v. Rumfseld*, 542 U.S. 507, 536 (2004). Per un'analisi della sentenza *Hamdi* e delle altre legate al ricorso di alcuni detenuti del carcere militare statunitense di Guantánamo sia consentito rinviare a A. De Petris, *Guantánamo: un buco nero nella « terra della libertà »*, in *http://www.associazionedeicostituzionalisti.it/materiali/anticipazioni/guantanamo/index.html* (24 maggio 2007).

sure nei confronti dell'Esecutivo, qualora anche ad anni di distanza dai tragici attacchi terroristici del 2001 la maggioranza dei cittadini statunitensi avesse continuato a supportarne le draconiane politiche di sicurezza? Lo stridore di tali misure con lo spirito e la lettera del dettato costituzionale, ripetutamente sottolineato sia dalle Corti che da numerose organizzazioni ed associazioni libertarie statunitensi, sarebbe stato in questo caso meno aspro o, piuttosto, gli interrogativi espressi soprattutto in sede giurisdizionale sulla legittimità di detti provvedimenti avrebbero comunque conservato il loro vigore indipendentemente dagli orientamenti contingenti dell'opinione pubblica?

La medesima fonte fornisce inoltre una particolare lettura del comportamento seguito dal Congresso al momento di decidere sulla proroga del *Patriot Act*, secondo la quale le resistenze espresse in sede parlamentare alla reiterazione del provvedimento — soprattutto da parte del Senato — non sarebbero state altro che la logica conseguenza dell'assenza di un espresso mandato in tal senso ad opera dell'opinione pubblica. In altre parole, il Congresso non avrebbe potuto fare altro che riflettere, attraverso le remore dimostrate in sede legislativa, l'inequivocabile clima sociale esistente in quel momento nel Paese riguardo al controverso tema del rapporto tra libertà e sicurezza. Al contrario, la successiva reiterata proroga dell'USAPA concordata dai due rami del Parlamento di Washington sarebbe solo il frutto di una riuscita azione di persuasione dell'Esecutivo sui senatori repubblicani più incerti, nell'intento di dimostrare alla nazione la coesione del partito del Presidente Bush su un tema scottante come la lotta al terrore[151]. Quello che non convince di una tale argomentazione è proprio la perentorietà con cui il Congresso ha mutato atteggiamento sul *Patriot Act* tra l'estate del 2005 e l'inverno del 2006: per quale motivo, infatti, gli « incerti » senatori repubblicani avrebbero dovuto dapprima sentire la pressione dell'opinione pubblica per poi, in un secondo momento, ignorarla in favore di una improvvisamente rivitalizzata disciplina di partito? Nello stesso periodo del « ripensamento » parlamentare non emergono indicazioni che facciano pensare ad un drastico cambiamento di orientamento da parte dell'elettorato statunitense rispetto al *Patriot Act* e, più in generale, alla spregiudicata linea del Governo in materia di « *War on Terror* »: al contrario, la crescente instabilità della situazione politica in Iraq ed Afghanistan, i due principali teatri della ormai ben nota « guerra preventiva » propugnata dalla Presidenza di George W. Bush, ha piuttosto incrementato lo scetticismo e la perplessità dell'opinione pubblica rispetto alle principali linee guida assunte dall'Esecutivo all'indomani degli attentati terroristici del 2001.

Alle argomentazioni di carattere speculativo si aggiungono poi elementi fattuali che contribuiscono a dimostrare come l'atteggiamento complessivo delle principali sedi istituzionali statunitensi — con la sola, sia pur rilevante eccezione di esponenti spesso particolarmente autorevoli del potere giudiziario — non abbia fatto registrare mutamenti sensibili sui temi esposti in questa sede. Il primo, inevitabile riferimento è per l'avvenuta approvazione delle misure di reiterazione del *Patriot Act* e di norme accessorie

---

[151] Così ancora R. BILLÉ, « *Patriottismo » costituzionale e libertà d'informazione: il caso statunitense*, op. cit., p. 154.

per la lotta al terrorismo, poc'anzi descritta[152]; altrettanto indicativo è il meno eclatante ma forse ancor più significativo *Real Security Act* emanato agli inizi di settembre 2006[153], la cui disposizione fondamentale per quanto rileva in questa sede è senza dubbio rappresentata dal § 2315, esplicativo dell'orientamento del Congresso riguardo alla sorveglianza elettronica (*Sense of Congress on Electronic Surveillance*). Esso esordisce con una serie di precisazioni da parte del Congresso, secondo cui: 1) le autorità governative degli Stati Uniti dovrebbero disporre del potere di mettere sotto sorveglianza elettronica qualunque conversazione telefonica in cui una delle parti coinvolte sia ragionevolmente ritenuta un membro o un agente di un'organizzazione terroristica; 2) in assenza di emergenze o di altre appropriate circostanze, la sorveglianza elettronica domestica dovrebbe essere sottoposta a controllo giurisdizionale allo scopo di proteggere la privacy dei cittadini americani osservanti della legge privi di legami con il terrorismo; 3) nel quarto di secolo trascorso dall'emanazione del *Foreign Intelligence Surveillance Act* (dunque nel periodo 1978-2003) la *Foreign Intelligence Surveillance Court* ha respinto l'istanza di autorizzazione ad un provvedimento di sorveglianza elettronica solo in cinque delle circa 19.000 richieste ricevute in tal senso. Il § 2315 prosegue con toni più prescrittivi, affermando che: 1) sia la Commissione scelta sull'*intelligence* del Senato che la Commissione permanente sull'*intelligence* della Camera dei Rappresentanti devono essere perfettamente informate sulla gestione e l'utilizzo del programma di intercettazione espletato dalla *National Security Agency* (NSA) in assenza di autorizzazioni giurisdizionali; 2) il Congresso dovrebbe modificare il *Foreign Intelligence Surveillance Act* del 1978 in modo tale da assicurare che il Governo possa espletare misure di sorveglianza elettronica su conversazioni telefoniche nelle quali è ragionevole ritenere che una delle parti coinvolte sia un membro o un agente di un'organizzazione terroristica; 3) la prescrizione secondo cui il Governo, in assenza di emergenze o altre appropriate circostanze, debba ottenere un'autorizzazione giurisdizionale prima di porre sotto sorveglianza elettronica una « *United States Person* »[154] dovrebbe rimanere in vigore al fine di proteggere la *privacy* degli americani osservanti della legge privi di legami con il terrorismo; 4) il Presidente non è al di sopra della legge e deve attenersi alle procedure instaurate dal Congresso per porre in essere misure di sorveglianza elettronica.

Nel complesso, la disposizione sembra voler riportare ordine nel caotico ambito delle intercettazioni elettroniche condotte dalle agenzie governative, dopo il difficile periodo di eccessi seguito alle vicende del 2001. Tra le varie affermazioni categoriche miranti a fissare chiaramente i confini delle potestà spettanti alle diverse figure istituzionali coinvolte, indubbia-

---

[152] V. *supra*, par. III.3.

[153] Real Security Act of 2006, S. 3875, 7 settembre 2006.

[154] Si è scelto di mantenere l'espressione originale utilizzata dal Legislatore statunitense per lo specifico significato che questa possiede: la definizione ufficiale statuisce che « [*United States Person*] *means a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for a permanent residence, or a corporation which is incorporated in the United States which is not a foreign power* », cfr. 50 U.S.C. § 1801 (h) (4) (i).

mente in grado di conferire un aspetto meritorio all'iniziativa assunta nell'occasione dal Congresso, compare tuttavia una breve ma sintomatica formulazione: si tratta del riferimento all'»assenza di emergenze o altre appropriate circostanze» come condizione affinché permanga l'obbligo di un'autorizzazione da parte di un organo giudiziario per un provvedimento di sorveglianza elettronica. In generale, concedere al Governo la facoltà di intercettare conversazioni telefoniche o attività condotte in Rete da parte di privati cittadini in situazioni eccezionali, nelle quali ricorrere ad un intervento giurisdizionale rischierebbe di vanificare l'effettività del provvedimento di sorveglianza elettronica, non sembra scandaloso[155]: quello che lascia perplessi nella dichiarazione di intenti del Congresso, piuttosto, è la mancanza di una qualche definizione delle situazioni straordinarie o delle «altre appropriate circostanze» in grado di giustificare tale deroga al principio generale di una supervisione giudiziaria di tale ambito. In assenza di precisazioni a riguardo, il rischio che le condizioni emergenziali siano statuite unilateralmente dagli stessi organi chiamati ad avvalersi di tali deroghe, e che quindi si continuino ad attuare i provvedimenti di sorveglianza elettronica in un regime di eccezionalità dal quale resta esclusa qualunque forma di controllo esterno, può rappresentare più di una semplice ipotesi di scuola: per questo, fin quando il Congresso non provvederà a definire chiaramente le condizioni di accesso a questa «uscita di emergenza» (è il caso di dire) a favore dell'Esecutivo, sarebbe opportuno sospendere ogni giudizio in merito agli ipotizzati mutamenti in materia di sorveglianza elettronica nelle massime sedi istituzionali statunitensi.

Una riprova di quanto appena sostenuto viene dalla vicenda relativa alla legge di autorizzazione al programma di sorveglianza elettronica istituito dall'Amministrazione Bush all'indomani dell'11/9/2001 ed applicato sistematicamente fino a quando, nell'agosto 2006, una Corte Federale di distretto non ne aveva decretato l'incostituzionalità, imponendone l'immediata sospensione[156]. Invece di continuare la battaglia sulla legalità del provvedimento in ambito giudiziario, ricorrendo in appello contro la sentenza di primo grado, il Governo ha preferito la strada istituzionale — implicitamente indicata nella stessa decisione osteggiata dall'Esecutivo, nella parte in cui aveva ravvisato la principale ragione dell'illegittimità del programma di sorveglianza elettronica nel contrasto tra l'operato presidenziale e i consolidati orientamenti del Congresso in materia, stabiliti per legge —, imponendo alle Camere, come per il *Patriot Act*, un *tour de force* per arrivare in tempi rapidi all'approvazione di una norma che, attraverso la sanzione positiva dell'organo parlamentare, sanasse il deficit di costitu-

---

155 Al contrario, esiste una consolidata giurisprudenza in favore di tali deroghe, che vede tra i suoi principali punti di riferimento la decisione della Corte Suprema comunemente nota come il «caso Keith»: questa, pur considerando in via di principio l'autorizzazione giudiziaria una condizione imprescindibile per la legalità di un provvedimento di sorveglianza elettronica, nondimeno ammette che «standard differenti possono essere compatibili con il Quarto Emendamento, qualora siano ragionevoli sia in relazione alla legittima necessità del Governo di informazioni fornite dai servizi di *intelligence*, che riguardo ai diritti tutelati dei nostri cittadini», cfr. *U.S. v. U.S. District Court*, 407 U.S. 297 (1972), in part. 322-323.

156 Sui contenuti della decisione e le reazioni di sostenitori ed oppositori del provvedimento v. *supra*, par. III.2.

zionalità del provvedimento. Così, il 28 settembre 2006, ad appena quaranta giorni dalla citata decisione di incostituzionalità, la Camera dei Rappresentanti ha approvato con 232 voti favorevoli contro 191 contrari l'*Electronic Surveillance Modernization Act*[157] che conferisce al Presidente la facoltà di porre cittadini statunitensi sotto sorveglianza elettronica per novanta giorni senza una previa autorizzazione giudiziaria, come invece previsto finora dal *Foreign Intelligence Surveillance Act*, la norma vigente in materia[158]. Se da un lato è vero che il mancato *placet* del Senato sulla norma, il cui fulmineo processo di approvazione alla Camera ha fatto registrare infruttuosi tentativi di ridimensionamento del potere presidenziale di condurre intercettazioni elettroniche sia da parte Democratica che Repubblicana, ha frustrato le speranze del Presidente di sottoscriverne la versione definitiva prima della programmata sospensione delle attività parlamentari in vista delle elezioni di medio termine del novembre 2006, dall'altro sembra altrettanto corretto leggere nella tempestività con cui quanto meno un'ala del Congresso è intervenuta a copertura delle pecche dell'Esecutivo un'ulteriore smentita del presunto « nuovo corso » degli Stati Uniti in tema di sicurezza collettiva.

I futuri sviluppi del rapporto tra diritti e sicurezza nell'ordinamento statunitense appaiono al momento talmente incerti che azzardare previsioni in proposito non costituisce più di un pretenzioso esercizio di stile — tante sono le varianti in gioco capaci di produrre effetti decisivi in un contesto delicato come quello in esame. Assai meno azzardato, di contro, è ipotizzare che il tema in oggetto continuerà ad occupare ancora per molto i politici e le corti, non sono negli Stati Uniti. L'auspicio è che anche la dottrina séguiti a dedicare un'attenzione costante verso un argomento così determinante per la conformazione stessa del potere politico odierno.

---

[157] H.R. 5825, disponibile in *http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.5825.RFS:* (4 gennaio 2007).

[158] Cfr. E. LICHTBLAU, *House Approves Power for Warrantless Wiretaps*, in *New York Times*, 29 settembre 2006.