Il diritto alla Privacy
e la lotta contro il terrorismo internazionale
dopo l'11 settembre 2001

Il termine Privacy

Radici

- concetto di origine anglosassone (nato nel 800)
- inizialmente riferito solo alla sfera della vita privata: diritto alla segretezza e all'intimità della propria vita privata (concetto di libertà negative)

Oggi

- diritto al controllo sui propri dati personali
- capacità di una persona (o di un gruppo di persone), di impedire che le informazioni che la riguardano diventino note ad altri, inclusi organizzazioni ed enti, qualora il soggetto non abbia volontariamente scelto di fornirle

- La Privacy oggi concerne diversi ambiti come
  - il giornalismo (→ diritto della cronaca),
  - la sanità (banche dati genetiche),
  - le comunicazioni elettroniche e Internet
    - utilizzo di tecnologie:
      - la tracciabilità dei cellulari,
      - la relativa facilità a reperire gli indirizzi di posta elettronica delle persone,
      - la raccolta "clandestina" di dati personali via Internet da parte di grandi aziende al fine di poter ottimizzare la vendita dei loro prodotti ("Adware"/"Spyware")
  - *la lotta contro il terrorismo internazionale, specialmente dopo l'11 settembre 2001.*

La tutela della privacy a livello dell'UNIONE EUROPEA

Punti di riferimento indispensabili per gli stati membri dell'Unione europea sono due direttive che concernono la tutela di dati personali.

La prima è la **Direttiva 95/46/CE** *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati.*

Prevede gli standard minimi da rispettare e da applicare per gli stati membri, per quanto riguarda il primo pilastro dell'Unione europea (Comunità europee). Per quanto riguarda gli altri due pilastri (Politica estera e di sicurezza comune/ Cooperazione di polizia e giudiziaria in materia penale) vige il modello intergovernativo.

La seconda è la **Direttiva 2002/58/CE** *del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche),* aggiunta alla direttiva del 1995. Questa direttiva ha obbligato gli stati membri ad applicare misure per, tra l'altro, vietare le intercettazioni telefoniche e nell'internet (e-mail). Tuttavia, lo scenario del terrorismo internazionale spinge anche stati membri dell'Ue come Italia e Germania ad elaborare atti legislativi che permettono allo stato di far uso proprio delle tecniche sopra descritte, dando via libera alle forze di polizia, nonché ai servizi segreti.

Dal 22 dicembre 2003 l'Unione europea ha una figura centrale, istituzionalizzata in materia. Il **Garante europeo per la protezione dei dati** è l'olandese Peter Johann Hustinx.

Inoltre, l'articolo 8 della **Carta dei diritti fondamentali,** proclamata a Nizza il 7 dicembre 2000, prevede esplicitamente la tutela della privacy, traendo ispirazione dall'art. 8 della CEDU (1950).

ITALIA: La tutela della privacy nella legislazione italiana

La **Costituzione Italiana**, pur non contenendo un riconoscimento esplicito del diritto della privacy, fornisce vari fonti di diritto per la tutela della privacy in generale e per quanto riguarda i vari rischi dopo l'avvento del terrorismo islamistico internazionale.

Il primo articolo rilevante è l'articolo 2 cost. la quale interpretazione ha permesso alla Corte costituzionale di ritenere costituzionalmente protetti vari diritti della personalità, attraverso varie sentenze, tra cui anche quello alla privacy (sent. 139/1990).

Nella seconda parte della costituzione (Diritti civili) si trovano tre articoli che rendono più esplicita la tutela della privacy:
Art. 13 e 14 parlano rispettivamente dell'inviolabilità della libertà personale e dell'inviolabilità del domicilio. Pongono un limite al tentativo dell'ordinamento di violare in modo arbitrario la sfera del proprio spazio personale tramite ispezioni, perquisizioni, sequestri che possono avvenire solo nei casi e modi previsti dalla legge (riserva di legge), per atto motivato dell'autorità giudiziaria (tranne i casi di necessità e urgenza indicati tassativamente dalla legge).

Art. 15 concerne l'inviolabilità della libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione.

Infine, l'art. 21, il quale concerne la libertà di manifestazione del pensiero (in concreto: libertà di stampa, pubblicità ecc.) prevede, secondo la sent. 112/1993 della Corte Cost., in modo indiretto anche la tutela del diritto all'informazione: la libertà quindi "ricomprende tanto il diritto di informare, quanto il diritto di *essere informati* (…)". Pensiamo al valore di questa lettura per quanto riguarda il diritto dell'interessato di essere informato sul trattamento dei suoi dati sensibili anche per quanto riguarda le misure contro il terrorismo ("Legge antiterrorismo").

La giurisdizione italiana a regolare la privacy

In Italia solo nel 1996 è stata approvata una legge in grado di regolare la complessiva materia riguardo la tutela del diritto alla privacy. Si tratta della *legge n. 675 del 31 dicembre 1996* – "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", meglio nota come *Legge sulla privacy*, fatta per applicare la *direttiva 95/46/CE*. Questa legge:

- definisce i dati "sensibili", il "titolare" del trattamento, misure di sicurezza, diritti dell'interessato (come essere informato su, ricevere e accedere alle informazioni e chiederne la rettifica)
- prevede l'introduzione del *Garante per la protezione dei dati personali* il quale è un'autorità indipendente, un organo collegiale i quali membri sono eletti da ciascuno dei due rami del Parlamento. Svolge tra l'altro i compiti seguenti:
    - controllo dei dati,
    - segnalazioni,
    - ricorsi,
    - autorizzazioni,divieti ovvero blocco del trattamento di dati,
    - formulazione di pareri,
    - collaborazione su livello dell'Ue ecc.

Data la natura della materia costantemente in evoluzione e la necessità di applicare una nuova direttiva UE (2002/58 sulla riservatezza nelle comunicazione elettroniche), il *Decreto legislativo 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali",* meglio noto come *"Codice sulla Privacy",* abroga la vecchia "Legge sulla privacy" costituendo un Testo Unico sulla materia.

La legislazione italiana dopo l'11 settembre

La legge 15/12/2001 n. 438

In seguito agli attacchi di New York e Washington dell'11 settembre 2001, il Governo italiano ha reagito adottando il decreto legge 18/10/2001 n. 374 "Disposizioni urgenti per contrastare il terrorismo internazionale", poi convertito con legge 15/12/2001 n. 438, con il quale è stata introdotta nel nostro ordinamento la fattispecie di "terrorismo internazionale".

L'esigenza di provvedere urgentemente alla creazione di questa nuova ipotesi di reato trova fondamento nella carenza di una normativa penale volta a reprimere organizzazioni che, pur avendo sede nel territorio italiano, mirano a compiere atti di violenza a danno di altri Paesi.[1]

La legge prevede già l'estensione delle cosiddette intercettazioni preventive (art. 3) e giudiziarie ai delitti con finalità di terrorismo internazionale e le norme che rendono già possibili in specifici settori per esempio le perquisizioni di edifici e le operazioni "sotto-copertura[2].

L'esperto in materia Giovanni Modesti ritiene che ciò abbia portato alla creazione di una sorta di diritto penale internazionale attraverso il quale favorire, migliorare e rendere più efficace la cooperazione tra Stati nella lotta al terrorismo[3].

Il Pacchetto Pisanu/ la Legge Antiterrorismo (2003)

Dopo gli attentati di Londra del 07 luglio 2005, la situazione giudiziaria in materia è cambiata notevolmente anche in Italia. Il ministro dell'interno del vecchio governo centro-destra, Giuseppe Pisanu, è stato autore del *Decreto-legge 27 luglio 2005, n. 144,* convertito nella *Legge del 31 luglio 2005, n. 155* meglio nota come *"Legge antiterrorismo"*. Comprendendo 19 articoli, la legge non prevede soltanto provvedimenti come il fermo di polizia fino a 24 ore, colloqui investigativi anche senza avvocato, ma anche misure espressamente indicate per la raccolta di dati riguardo la comunicazione di tipo telefonico e telematico.

Che cosa comporta la "Legge antiterrorismo"? Vediamo alcuni articoli rilevanti rispetto alla privacy:

- L'art. 3 rende più facile l'espulsione degli stranieri – in modo più rapido –quando questi risultino pericolosi per la sicurezza nazionale. C'è chi osserva criticamente il rischio che l'

[1] Studi per la pace: Terrorismo internazionale: risposta dello stato italiano; 14 settembre 2002;
site: http://www.studiperlapace.it/view_news_html?news_id=terrorismo

[2] Il diritto di tutti – Rubriche: SICUREZZA E PRIVACY: CONFLITTO EVITABILE?; 2002;
site: http://www.giuffre.it/age_files/dir_tutti/archivio/fatti_1002.html

[3] Quaderni di Overlex; N. 3 – gennaio 2007; Giovanni Modesti;
site: http://www.overlex.com/quaderni/2007/3.pdf

acquisizione di dati di tipo personali da parte dell' intelligence comporta: non osserva solo la condotta, ma anche il pensiero.

- L'art. 4 prevede che i servizi segreti SISDE e SISMI possono effettuare, su autorizzazione del magistrato, delle intercettazioni "quando siano ritenute indispensabili per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale".

- L'art. 6 prevede la conservazione di dati di tipo telefonico e telematico fino a dodici mesi (c.d. data retention). Inoltre impone ai gestori che rilasciano le schede telefoniche l'acquisizione dei dati anagrafici e gli elenchi dei possessori delle schede da parte dei clienti.

- L. Art 7 impone ai gestori di luoghi pubblici forniti di strumenti di comunicazione elettronica (Internet Cafè, biblioteche ecc.) di chiedere la licenza al questore, di raccogliere i dati anagrafici dell'utente, ma anche di archiviare le sue operazioni per fini di prevenzione.

Giovanni Modesti ha un'opinione critica nei confronti di questa legge. Secondo lui porterebbe alla riduzione delle libertà, comporterebbe il rischio di criminalizzare gruppi etnici o religiosi e indebolirebbe delle garanzie costituzionali senza avere, di fatto, trasmesso più sicurezza ai cittadini. Basti pensare al tema della conservazione dei dati, la c.d. data retention, rispetto al quale il pacchetto-Pisanu è andato oltre quanto prescritto dalla direttiva dell'Ue, cioè conservando i dati telefonici e telematici per ***due*** anni, fino al 31.12.2007).

Sul sito web Shiny news[4] si trova un'altra lettura critica della legge. Gli autori pongono l'attenzione su aspetti più tecnici come le modalità di archiviazione di dati da parte di gestori pubblici non ben definite.

- Tempo di archiviazione
- Il problema del contenuto che "non può e non deve essere registrato in alcuna maniera".
- Altri punti importanti:
    - Consenso dell'interessato (cliente) non necessario (il rifiuto di trasmettere i propri dati comporta obbliga il titolare di non erogare il servizio)
    - Affidabilità del gestore: Archiviazione sicura? ecc.

Infine, si sostiene che il Pacchetto Pisanu, almeno in alcuni articoli rilevanti, non introduca tanto delle misure efficaci per combattere l'interscambio via mezzi di comunicazione elettronica da parte di possibili terroristi (i quali troverebbero facilmente delle vie per aggirare le limitazioni imposte), ma comporti delle misure ritenute eccessive e lesive nei riguardi di semplici cittadini e la loro sfera di privacy.

[4] Troppa apprensione genera confusione; Ottobre 2005
site: http://www.shinynews.it/diritto/1005-antiterrorismo.shtml
Antiterrorismo e privacy: connubio difficile?; Novembre 2005
site: http://www.shinynews.it/diritto/1105-antiterrorismo-2.shtml

Privacy e terrorismo in GERMANIA

La legge per combattere il terrorismo (2001)

Gesetz zur Bekämpfung des internationalen Terrorismus ("Terrorismusbekämpfungsgesetz")

Si tratta di una legge approvata in due tappe rispettivamente il 30 novembre 2001 e il 01 gennaio 2002.

Dato che è stato in vigore solo per 5 anni, il 10 gennaio 2007 è stato prorogato per ulteriori 5 anni, introducendo delle modifiche.

Ha introdotto una serie di misure per rendere più facile l'individuazione di persone sospettate di collaborare a crimini di natura terroristica ed estende le possibilità di accedere ai loro dati, specialmente dai servizi segreti che da quest'anno hanno visto addirittura aumentare le loro competenze in materia. D'altra parte – come già l'aggettivo *international* dimostra – prevede una collaborazione più stretta con i servizi (segreti) di altri paesi nel mirino di terroristi (specialmente gli Usa) e mira a riconoscere la natura internazionale, decentrata, "asimmetrica" del terrorismo.

Le misure in dettaglio:

- Integrazione del lavoro dei servizi segreti nella "individuazione e osservazione di intenzioni di tipo violento o preparatorie alla violenza"
- Intensificazione della collaborazione internazionale
- Integrazione di tratti biometrici nella carta d'identità
- Osservazione delle attività delle organizzazioni di concittadini stranieri
- Permesso al *Bundesamt für Verfassungsschutz* di accedere a dati della persona sospettata: dati del traffico di soldi per via postale o bancario, vigilanza di eventuali viaggi da parte della persona, della comunicazione telefonica e telematica.
- Riconoscimento di poteri simili agli altri 2 servizi segreti (*MAD* e *BND* il quale, prima solo operando all'estero, ha ricevuto il permesso di estendere le sue attività anche all'interno. Da quando la legge è stata prolungata, viene stabilito che "i diritti di informazione del *BND* e del *MAD* siano, in linea generale, equiparati al quelli del *Bundesamt für Verfassungsschutz*"[5].

Considerate le novitá importanti che queste prime misure adottate in Germania dopo l'11 settembre hanno comportato, il professore universitario Prof. Dr. Erhard Denninger già allora ha parlato di uno "spostamento di importanza dallo stato di diritto allo stato di prevenzione" *("Gewichtsverschiebung zwischen Rechtsstaat und Präventivstaat"* [6]*).*

[5] Stefan Lehmacher: Bürgerrechte unter Druck
site: http://www.zdf.de/ZDFde/inhalt/30/0,1872,3975582,00.html
[6] sito web della *Bundeszentale für politische Bildung*; 2002
site: http://www.bpb.de/publikationen/32OU0D,1,0,Freiheit_durch_Sicherheit.html#art1

La discussione sul dubbio valore costituzionale dello strumento della *Rasterfahndung*

La *Rasterfahndung* è uno strumento elaborato già negli anni 70 per contrastare in modo efficace il terrorismo della *RAF*. È un metodo che dovrebbe consentire alle forze dell'ordine di individuare persone che sono sospettate di crimini terroristici, attraverso la creazione di un profilo dettagliato, la raccolta di un numero elevato di dati personali di persone sospettate e un metodo complesso di confronto tra profilo e dati raccolti.

L' effettiva verifica della presunta colpevolezza avviene solo in un secondo momento attraverso indagini da parte delle forze dell'ordine. Metodo e impiego della *Rasterfahndung* comportano quindi inevitabilmente l'eliminazione della presunzione di innocenza. Dunque la creazione di una specie di griglia che dovrebbe essere efficace comporta inevitabilmente la raccolta di centinaia di dati di persone in verità innocenti. Dev'essere comunque detto che lo strumento della *Rasterfahndung* mira ad individuare proprio persone che sono paradossalmente caratterizzati da una buona condotta, un buon livello di adattamento e integrazione (per questo vengono chiamati *sleepers* o *Schläfer*: sembrano cittadini piuttosto normali prima di colpire in modo violento).

Lo strumento della *Rasterfahndung* è diventato oggetto di discussione subito dopo gli avvenimenti del 11 settembre 2001. Allora lo strumento è stato utilizzato per individuare possibili terroristi di fede islamica sul terreno della Repubblica Federale. Di conseguenza, vari enti come gli uffici anagrafe, le università statali, gli istituti tecnici superiori e il registro centrale degli stranieri sono stati costretti a fornire agli uffici di polizia dati riguardanti un profilo che doveva corrispondere a un uomo tra i 18 e 40 anni, di fede islamica, studente (attuale o in passato).

(La raccolta di dati alla fine si sarebbe rivelata inutile dato che non ha portato all'individuazione di *sleepers*.[7])

Su lamenta da parte di uno studente di origine marocchino di fede islamica che ha contestato la *Rasterfahndung*, la Corte Costituzionale ha infine dichiarato che l'utilizzo dello strumento comporti dei gravi rischi rispetto alla tutela della privacy dei cittadini. Sostiene che

- i dati acquisiti consentino in ogni modo ingerenze nella sfera dei diritti fondamentali delle persone interessate
- dato il valore prognostico incerto dei dati sia molto discutibile la sufficienza di legittimare un'ingerenza di questa intensità
- il fatto di essere entrati nella "griglia" già per sé possa costituire un pregiudizio nei confronti delle persone interessate
- lo strumento, in generale, comporti il grave rischio di sospettare un vasto numero di persone che in verità non stanno in alcuna relazione con una concreta condotta negativa.

Nella sua sentenza del 04 aprile 2006, la Corte infine dà retta alla lamentela dichiara che lo strumento della *Rasterfahndung* sia parzialmente incostituzionale e che

- sia intutilizzabile nell'ambito di una strategia di prevenzione
- debba far riferimento al parametro della "proporzionalità" intesa come adeguato bilanciamento tra la specie e l'intensità dell'ingerenza dei dati fondamentali

[7] Netzzeitung Deutschland: Wenig Zukunft für Rasterfahndung; 24.05.2006
site: http://www.netzeitung.de/deutschland/400775.html

- debba essere quindi utilizzato in presenza di un pericolo concreto, quando ci sono indizi effettivi della preparazione di atti terroristici.

In seguito, leggi hanno dato un nuovo regolamento per l'utilizzo della ***Rasterfahndung*** per garantire che possa essere utilizzata solo in presenza di un pericolo concreto (contro lo stato, la vita dei cittadini...).

L' *Antiterrordatei* (2006)

La cosiddetta *Anti-Terror-Datei* costituisce una banca dati integrata e centrale, usata sia su livello federale che regionale, in modo di permettere la collaborazione e lo scambio di dati tra non meno di 38 autorità che in passato hanno svolto compiti ben distinti tra loro, compresi le varie polizie, le varie polizie criminali e i 3 servizi segreti tedeschi (*BND, Verfassungsschutz, MAD*).

La legge dell'*Antiterrordatei* è stata approvata il 01 dicembre 2006 a seguito di un'intensa discussione (questa volta con un maggior coinvolgimento del pubblico) che si era infiammata dopo la minaccia posta dai tentati attentati a due treni a luglio '06 in Germania.

La banca dati concerne due tipi di dati.
Il primo è costituito dalla *Indexdatei*, una collezione di dati che possono essere utilizzati senza richiesta da parte di tutte le autoritá coinvolte. Riguardano nome, genere, data e luogo di nascita, cittadinanza/e, indirizzo, lingue, una foto e caratteri somatici.

Il secondo tipo è costituito dalla *Erweiterte Datei* che contiene dati strettamente personali (fede religiosa; numero di telefono, controcorrente bancario; località visitate, appartenenza a organizzazioni; macchina, permesso di utilizzo di mezzi di trasporto, abilità nell'uso di armi e esplosivi ecc.). Questi dati possono essere richiesti e scambiati solo in caso di pericolo imminente o di emergenza.

Il 30 marzo 2007 l'*Antiterrordatei* è stata elogiata dal ministro federale dell'interno, Wolfgang Schäuble, come strumento unico e incomparabile in tutto il mondo. In quella circostanza sono stati resi pubblici alcuni dati: Secondo le informazioni ufficiali, circa mezz'anno dopo l'approvazione della legge sarebbero stati raccolti già circa 15.000 dati concernenti un complesso di 13.000 persone delle quali la maggior parte risiede all'estero. Solo un quarto delle persone risiede in Germania; di queste, solo una piccola parte è ufficialmente ritenuta pericolosa[8].

Perquisizione clandestina online

Il 6 dicembre 2006, cinque giorni dopo l'approvazione dell'*Antiterrordatei*, il BKA (ufficio federale della polizia criminale) ha espresso la sua intenzione di ricevere permesso per poter effettuare perquisizioni "clandestine" online di computer di sospettati. Ha dichiarato di avere già a sua disposizione gli strumenti tecnici e organizzatori necessari, avendo anche istituito un organo di sorveglianza con il *Bundesverfassungssschutz*. Quest'ultimo aveva, nei limiti della legittimità, già da tempo utilizzato questo strumento, adottando metodi che sono analoghi a quelle utilizzati dai cosiddetti *hacker*.

[8] Spiegel Online; 30.03.2007
site: http://www.spiegel.de/netzwelt/web/0,1518,474924,00.html

Il 14 dicembre del 2006 il Garante federale per la protezione della privacy, Peter Schaar, si è espresso in maniera decisamente negativa. Non sarebbe secondo lui in nessuna maniera possibile di paragonare una perquisizione clandestina via internet con una perquisizione domiciliare nella quale, in via generale, l'interessato sarebbe comunque presente e si tratterebbe quindi di un'azione di natura palese. Una perquisizione clandestina online sarebbe in contraddizione totale con il principio della tutela della sfera privata dell'individuo. Al contrario, la deputata del partito cristiano-democratico bavarese CSU, Daniela Raab, ha sostenuto che solo a febbraio 2006 un giudice inquirente della Corte federale avrebbe con una decisione acconsentito queste misure

La stessa Corte federale il 5 febbraio 2007 si è espressa contro l'utilizzo di questo strumento di indagine.

Chi però sperava che questo capitolo ora fosse chiuso, sbagliava. A giugno, il ministro federale dell'interno Schäuble ha ripreso il tema. Dato che però riconosce i limiti giudiziari posti dalla costituzione federale, ha espresso l'intenzione di adottare delle modifiche alla costituzione in modo di permettere allo stato e ai suoi organi di godere di più libertà nella battaglia contro il terrorismo internazionale. Secondo Schäuble, la costituzione dovrebbe essere adeguata alla realtà e alle necessità di oggi. Le proposte di Schäuble hanno finora provocato dure critiche da parte del partner di coalizione, il partito socialdemocratico tedesco (SPD) che non sembra voler sostenere il ministro.

La proposta fa parte di un complesso disegno di legge da parte del ministro. Questo disegno tra l'altro prevede il ritorno della ***Rasterfahndung***, il permesso al ***BKA*** di fare intercettazioni per fini preventive (finora non consentite) o il divieto ai sospettati di crimini terroristici di usare cellulari e di accedere a internet[9].

[9] Spiegel Online: archivio; 7.12.2006; 14.12.2006; 5.2.2007; 02.06.2007, 05.07.2007, 07.07.2007 parola chiave „Bundestrojaner"

La tutela della privacy negli STATI UNITI D'AMERICA

L' USA PATRIOT ACT (acronimo per *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)* è una legge federale statunitense approvata dal Congresso americano il 25 ottobre del 2001 e, avendo avuto una validità di 5 anni, prolungata, con alcune modifiche, il 9 marzo del 2006.

Comporta una serie di misure che fortemente rischiano di ledere il diritto alla privacy dei cittadini americani che è fissato nel 4°emendamento della Costituzione Americana del 1787 (*"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"* [10]*).*

Particolarmente contestati sono i punti seguenti:

- raccolta e conservazione di dati e informazioni,
- intercettazioni di comunicazioni di tipo telefonico e telematico,
- le facoltà riconosciute agli Isp di protocollare, raccogliere ed archiviare i dati di traffico online,
- la possibilità e l'autorizzazione delle varie autoritá di diversa natura giuridica (FBI; servizi segreti) di scambiare dati di tipo personale o sensibile tra di loro senza particolari vincoli, riconoscendo ai servizi segreti facoltà normalmente assegnate solo alle forze di polizia,
- perquisizioni clandestine di alloggi di sospettati.

Secondo la American Civil Liberties Union (ACLU), storica associazione americana che si occupa dei diritti civili, sono **212 milioni di Americani i cui dati sono finora stati raccolti** e contenuti in una banca dati

Una peculiarità del Patriot Act consiste nella pratica della ***National Security Letter (NSL)***. Si tratta di un metodo usato dal FBI di costringere aziende di trasmettere informazioni su clienti se sussiste un sospetto che riguarda la sicurezza nazionale anche in assenza di un indizio concreto. L'FBI non ha bisogno di un'autorizzazione da parte di un giudice. Le aziende non hanno il diritto di rendere pubblico il ricevimento della lettera e, visto la natura segreta del messaggio, sono minacciate di sanzioni penali nei loro confronti[11]..

La pratica della NSL è stata abusata in tanti casi per fini tutt'altro che investigativi. Verso l'inizio di marzo 2007 una relazione di controllo da parte del ministero federale della giustizia ha evidenziato abusi in centinia di casi. In particolare, si è osservati che

- in 739 casi il FBI abbia ricevuto fatture di telefono e documenti simili persino senza aver espresso questa richiesta via NSL,
- che siano stati inoltrate delle NSL senza un'autorizzazione ufficiale di indagine da parte del FBI,
- vari sospetti si siano rivelati infondati,

[10] site: http://www.europarl.europa.eu/meetdocs/committees/temp/20010322/433524IT.pdf

[11] ZDF.de; „Sicherheit über alles"; 07.09.2006
site: http://www.zdf.de/ZDFde/inhalt/30/0,1872,3975582,00.html

- in almeno 2 casi la pratica sia stata abusata per ricevere informazioni su operazioni bancarie.[12]

La sopraccitata **ACLU** nel **2004** si è mossa contro le modalità della pratica. Un Isp (Internet Service Provider) ha ricevuto una NSL per motivi ritenuti infondati e si è rivolto all'organizzazione. Difendendo la sua causa davanti un tribunale newyorkese, l'associazione alla fine si può dire contenta: Il giudice dà retta al querelante e dichiara l'illegittimità parziale del Patriot act in quanto violerebbe il 4°emendamento della Costituzione americana[13].

Tuttavia, il 09 marzo 2006 l'USA PATRIOT ACT è stato **prolungato** per ulteriori 5 anni, introducendo delle modifiche. Visto l'abuso frequente della pratica della NSL, riconosce alle aziende la possibilita di far causa senza la minaccia imminente di sanzioni penali. D'altra parte comporta delle novità che aggravano il peso delle misure. Per esempio in futuro possono essere raccolte persino dati di biblioteche e informazioni raccolte nell'ambito sanitario. Inoltre, sia mittente che ricevente di comunicazioni elettroniche (email) possono essere raccolte e registrate da parte di aziende e istituzioni senza vincoli particolari.

Il sito web http://punto informatico.it riprende la delusione di tanti dopo l'approvazione dell'USA PATRIOT ACT II. "Non sono servite le proteste delle organizzazioni per le libertà civili, le prese di posizione della magistratura, le denunce dei giornali: alla fine il Patriot Act è stato rinnovato. Insomma, come ha sostenuto il repubblicano Dennis Kucinich, la legge è stata riformata superficialmente e non vi è stato nessun miglioramento che preluda ad una migliore salvaguardia delle libertà civili.[14]"

[12] SPIEGEL ONLINE; 09.03.2007
site: http://www.spiegel.de/politik/ausland/0,1518,470909,00.html

[13] ICTLEX : FBI e Patriot Act: un caso di accesso abusivo ai dati degli utenti Internet?; 01.12.2004; Andrea Monti
site: http://www.ictlex.net/index.php/2004/12/01/fbi-e-patriot-act-un-caso-di-accesso-abusivo-ai-dati-degli-utenti-internet/

[14] sito web „Punto informatico"; 09.03.2006;
site: http://punto-informatico.it/p.aspx?i=1430036

Dati passeggeri aerei e gli accordi in materia tra Ue e Usa

Un capitolo speciale riguardo il dubbio valore della tutela della privacy negli Stati Uniti concerne i cosiddetti dati passeggeri aerei dei voli transatlantici e le sue modalità di raccolta, conservazione e trattamento. Il termine americano di questo metodo introdotto con l'approvazione **dell'USA PATRIOT ACT** è *Passenger Name Record (PNR)*. L'autorità americana federale a prendersi cura della banca dati è il *Department of Homeland Security*.

Il **17 maggio 2004** la Commissione europea approva un primo accordo raggiunto tra l'Unione europea e gli Stati Uniti. Il Parlamento europeo si esprime contro l'accordo nella sua votazione. Dato che il suo voto non ha potuto influenzare la decisione presa e si è sentito trascurato nella presa di decisione, ha in seguito fatto ricorso presso la Corte europea. Sostiene, in linea con varie associazioni e garanti per la privacy, che la tutela dei dati personali non sia sufficiente, sia per quanto riguarda il numero e la natura dei dati raccolti che il dubbio trattamento di questi dati da parte delle autorità americane coinvolte.

Infatti, da fine maggio 2004 ad oggi il *Department of Homeland Security* riceve fino a 34 dati personali dalle compagnie aeree contenenti nome, data e luogo di nascita, indirizzo, numeri di telefono, indirizzi email, numero della carta di credito ecc., ma anche preferenze riguardo il cibo (consumato in aereo), dato spesso contestato perché probabile indizio alla fede religiosa dell'interessato.

Il **22 novembre 2005** la Corte europea si esprime contro all'accordo raggiunto un'anno e mezzo prima dando retta quindi al Parlamento europeo che ha fatto ricorso e invitando entrambi le parti a mettersi di nuovo d'accordo.

Il **06 ottobre 2006** Ue e Usa raggiungono una nuova intesa provvisoria, che è in vigore fino al 31 luglio 2007, obbligando entrambi le parti a discutere di un accordo definitivo. Il commissario europeo per la giustizia, Franco Frattini, promette di tutelare la privacy dei passeggeri al massimo possibile, obbligando il *Department of Homeland Security* a rendere più difficile l'accesso ai dati da parte delle varie autorità americane. D'altra parte l'accordo prevede il permesso ufficiale di accesso ai dati da parte del FBI, ma anche che l'accesso ai dati da parte di una serie di altre autorità coinvolte diventi più facile.
Nel frattempo gli Stati Uniti hanno, pur agendo in una sfera di dubbia legittimità, continuato a raccogliere i dati passeggeri con le stesse modalità.

Verso fine giugno 2007 Ue e Usa raggiungono un'intesa definitiva, in vigore fino al 01 agosto 2007. Il 23 luglio il Consiglio dei ministri europeo approva l'accordo che sarà in vigore per 7 anni. Prevede una riduzione dei dati raccolti (da 34 a 19) che sarà però contrapposta da un aumento della durata di conservazione delle informazioni: da tre a 15 anni in complessivo. I primi sette anni questi dati conservati saranno di natura "attiva" , quindi facilmente accessibili alle autorità coinvolte.

Per gli 8 anni restanti i dati avranno carattere "inattivo" dotati di modalità di accesso più rigide. Per quanto riguarda i dati "sensibili"(riferiti alla razza, alle opinioni politiche e religiose o alla salute e alla vita sessuale di una persona) il dipartimento di sicurezza Usa, secondo l'accordo, non ne farà uso se non in casi in cui sono in gioco vite umane[15]. In prima linea si trattta dei dati contestati riguardo le preferenze di cibo[16].

[15] ANSA; 13.07.2007
site: http://www.ansa.it/infrastrutturetrasporti/notizie/fdg/20070713165728502/20070713165728502.html
[16] SPIEGEL ONLINE; 13.07.2007

Prima dell'accordo Michael Chertoff, segretario americano per la Sicurezza del territorio nazionale, ha minacciato di aggravare le modalità di viaggio costringendo i viaggiatori di registrarsi online fino a 48 ore prima del viaggio e di compilare una scheda informativa.

Il nuovo accordo tra Ue e Usa è tuttavia contestato. Secondo i critici dell'accordo, la riduzione di dati raccolti in futuro da 34 a 19 sarebbe in verità solo di natura teorica visto che si è scoperti che tante definizioni di dati ora hanno una natura più generica, offrendo quindi la possibilità di raccogliere più dati quando "ufficialmente" se ne raccoglie solo uno per volta (es.: numero e informazione generale sulla sedia nell'aereo contenuti entro lo stesso punto).

Il giorno dopo il ministro federale tedesco dell'interno **Schäuble propone la creazione di una banca dati passeggeri nello spazio dell'Unione europea**. Una banca dati di questo tipo trarrebbe ispirazione dal modello americano e raccoglierebbe i dati dei passeggeri aerei che si muovono all'interno dell'Unione europea.

http://www.spiegel.de/reise/aktuell/0,1518,494337,00.html