

---

ANDREA DE PETRIS

---

## L'APPROCCIO GIURISPRUDENZIALE ALLA TUTELA DELLA PRIVACY INFORMATICA: CAPACITÀ INNOVATIVA E TRADIZIONE COSTITUZIONALISTICA

---

**SOMMARIO:** 1. Il rapporto tra Privacy e Sicurezza in ambito informatico. — 2. USA. — 3. Portogallo. — 4. Spagna. — 5. Francia. — 6. Germania. — 7. Conclusioni: uno sguardo all'Italia e le prospettive future.

---

### 1. IL RAPPORTO TRA PRIVACY E SICUREZZA IN AMBITO INFORMATICO.

---

La questione del rapporto tra Privacy e Sicurezza ha acuito profondamente la sua rilevanza in conseguenza degli eventi dell'11 settembre 2001: gli attentati terroristici di New York e Washington, a cui sono seguiti quelli di Madrid (2003) e Londra (2005), hanno indotto le forze di sicurezza di ordinamenti nazionali e sovranazionali a rivedere le priorità nell'esercizio delle funzioni di tutela della sicurezza collettiva di fronte alla minaccia del terrorismo internazionale organizzato su scala mondiale.

Anche l'Unione Europea ha ritenuto opportuno intervenire in proposito, con provvedimenti che regolano le procedure di raccolta e trattamento dei dati personali per fini di sicurezza. In particolare, a livello europeo si sono recentemente registrate due misure di considerevole rilevanza in materia: una proposta di decisione quadro del Consiglio UE sulla protezione dei dati personali trattati nell'ambito del cosiddetto « III pilastro » (cooperazione giudiziaria e di polizia), ed il principio di disponibilità sancito dal « Programma de L'Aja » (ossia l'obbligo per gli Stati membri di rendere reciprocamente disponibili i dati raccolti a livello nazionale per finalità di giustizia e polizia).

Nella Conferenza delle *Authorities* europee di garanzia della protezione dei dati personali dei Paesi membri dell'Unione tenutasi il 10-11 maggio 2007 a Larnaka (Cipro), i Garanti hanno emanato tra l'altro una dichiarazione nella quale si ribadisce che la decisione quadro del Consiglio UE, nel momento in cui limita l'applicazione dei principi ai soli dati oggetto di scambio fra gli Stati, e non la estende anche ai trattamenti degli stessi dati effettuati a livello nazionale, rischia di introdurre una protezione dei dati personali « a due velocità » nell'ambito del III pilastro, laddove invece occorre garantire uniformità di tutele a livello nazionale e sovranazionale nel trattamento dei dati raccolti per finalità di giustizia e polizia<sup>1</sup>.

---

<sup>1</sup> Nella dichiarazione citata la Conferenza delle *Authorities* europee segnala al-

cuni principi-guida a cui il Consiglio dell'UE dovrebbe attenersi nel momento in

Quello che va sottolineato, rispetto all'approccio adottato sia dalla regolamentazione europea che ai rilievi mossi a riguardo dalle autorità garanti della privacy europee, è che l'ambito di disciplina riguarda prevalentemente le modalità di raccolta dei dati personali, all'interno del più generale contesto relativo alle misure di tutela della sicurezza collettiva: si tratta, cioè, di dati il cui conseguimento è espressamente richiesto da un provvedimento emanato appositamente per consentire l'ottenimento di quei dati. Questo presuppone una perfetta individuazione dell'ambito, dei soggetti e della tipologia di dati da sottoporre a controllo e da raccogliere. Una tale condizione, tuttavia, non è realizzabile in ambito telematico e soprattutto informatico: come dimostrano alcuni esempi di misure normative finalizzate al controllo di dati presenti nella Rete, infatti, la possibilità di scindere nettamente l'oggetto del controllo dal contesto informatico complessivo risulta in verità un'operazione difficilmente realizzabile, in primo luogo per ragioni tecniche<sup>2</sup>. Se questa sperequazione non sembra essere chiara agli occhi di molti legislatori nazionali e sovranazionali intervenuti dal 2001 ad oggi a regolare la materia in questione, molto più avveduti a riguardo sembrano essere gli organi giurisdizionali di volta in volta chiamati a verificare la legittimità dei provvedimenti normativi emanati dai primi. Con una serie di sentenze di grande rilievo, giudici ordinari e costituzionali di diverse latitudini hanno mostrato un orientamento tendenzialmente comune in merito al problema del riequilibrio tra sicurezza collettiva e privacy in ambito informatico, costringendo in molti casi il potere legislativo a ripensare i contenuti delle norme inizialmente promulgate.

Scopo principale di questo scritto è quello di fornire, attraverso l'analisi di alcuni casi nazionali particolarmente rilevanti sotto il profilo qui indicato, una breve ma attenta ricostruzione delle vicende giurisdizionali relative al tema in oggetto, per verificare similitudini, differenze e linee evolutive della giurisprudenza dedicata alla tutela della riservatezza telematica ed informatica a fronte della minaccia alla sicurezza pubblica proveniente dal terrorismo internazionale. Il lavoro si conclude tentando una valutazione dell'attuale disciplina vigente in Italia in materia di tutela della privacy a livello informatico e telematico alla luce delle linee-guida individuate attraverso lo studio dei suddetti casi giurisprudenziali, con l'intento

---

cui definirà la versione finale della decisione quadro, tra cui: 1) Limitazione delle finalità: necessità di definire chiaramente le finalità che consentono una legittima opera di raccolta dati nell'ambito delle attività del III Pilastro, eliminando la clausola generica ed indefinita «e per ogni altra finalità»; Categorie di informazioni: l'elaborazione di alcune categorie di dati è proibita, a meno che non ricorrano speciali condizioni e comunque in presenza di adeguate garanzie previste dalle legislazioni nazionali (art. 8 Direttiva UE, Art. 6 Convenzione 108); Categorie dei soggetti titolari dei dati: reintrodurre una adeguata distinzione in merito; Informazione dei

soggetti titolari dei dati: devono essere forniti di adeguate disposizioni, inclusa l'identità dei controllori di informazioni, i possibili contenitori ed il fondamento giuridico del trattamento dei dati. Ogni restrizione in materia deve essere precisa e limitata

<sup>2</sup> Per una descrizione ancora estremamente efficace, per quanto non più recentissima, del problema 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: 10 agosto 2008).

di estrapolare indicazioni utili per individuare approcci efficaci per la gestione futura del problema qui considerato.

## 2. USA.

Il primo e senza dubbio più eclatante caso relativo al tema oggetto del presente lavoro è quello conseguente all'emanazione del c.d. *USA PATRIOT Act* (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, noto anche con gli acronimi «USAPA» e «PAct»)<sup>3</sup>, emanato il 26 ottobre 2001 da parte del I Governo di George W. Bush<sup>4</sup>.

Il *Patriot Act* ha esteso l'applicabilità di quattro differenti metodi tradizionali di indagine, già previsti dalla disciplina investigativa, nel contesto virtuale, 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<sup>5</sup>, a meno che le condizioni ivi previste non vengano comunque rispettate.

<sup>3</sup> Pub. L. n. 107-56, 115 Stat. 272 (2001). Cfr. il testo integrale del provvedimento in: <http://www.epic.org/privacy/terrorism/hr3162.pdf> (10 agosto 2008).

<sup>4</sup> Per una più ampia ricostruzione della vicenda si consenta di rinviare a A. DE PETRIS, *Il Patriot Act e le libertà digitali*, in questa *Rivista* 2007, 599-647.

<sup>5</sup> «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

Come si vede, gli effetti del provvedimento sono ampie ed articolate, offrendo numerosi spunti di riflessione che di seguito vengono riassunti per sommi capi:

a) il PAct non introduce norme assolutamente nuove in materia di indagine delle comunicazioni tra privati, ma si limita in larga misura ad estendere l'applicabilità anche ad investigazioni penali tradizionali di un regime di *intelligence* che, fino alla sua entrata in vigore, risultava esperibile solo per indagini di carattere internazionale, in cui gli indagati sono agenti di governi stranieri (così disponeva il FISA - *Foreign Intelligence Surveillance Act*, provvedimento di riferimento in materia, emanato nel 1978 ed emendato successivamente<sup>6</sup>). Le problematiche che derivano da questa commistione tra sorveglianza esterna ed interna sono molteplici e facilmente immaginabili. Senza descriverli dettagliatamente in questa sede, basta ricordare che le finalità della prima (repressione dello spionaggio straniero) giustifica una serie di deroghe alle tradizionali garanzie costituzionali non ammissibili nel secondo contesto (lotta al crimine interno, sia pure di matrice terroristica).

b) Il PAct introduce un nuovo regime di intercettazione per le comunicazioni telefoniche e telematiche, derivato appunto dal FISA: tuttavia, mentre la disciplina originaria aveva come punto di riferimento essenzialmente i dati ottenibili attraverso la sorveglianza del traffico telefonico, la sua estensione anche al traffico informatico comporta una serie di problematiche giuridiche derivanti sia dal diverso contesto tecnologico, sia dalla diversa natura del dato trasmesso. Porre esattamente sullo stesso piano i due ambiti, pertanto, 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 dal PAct ha prodotto.

c) Il § 214 del PAct estende l'applicabilità di un'ordinanza di *Pen Register* o di *Trap and Trace* (*Pen/Trap Order*). Il nuovo regime permette di accedere ai numeri di telefono in entrata e in uscita da una determinata utenza telefonica con vincoli giurisdizionali molto più blandi, a scapito del rispetto delle più elementari garanzie costituzionali.

d) Il § 216 estende 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

---

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 RUFFIA, *Costituzioni straniere*

*contemporanee*, Giuffrè, Milano 1994<sup>6</sup>, p. 19.

<sup>6</sup> La versione attualmente in vigore è disponibile in: <http://www4.law.cornell.edu/uscode/50/ch36.html> (10 agosto 2008).

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. Il timore, quindi, è che sotto questi standard di garanzia 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 Internet, 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'ente 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 « *ihad.com* », seguito da « *bombs.com* », « *Osama.org* » e quindi « *ACLU* », 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 delle pagine visitate.

e) 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 e, quel che più conta, senza alcun controllo giurisdizionale della sua fondatezza, nemmeno a posteriori. Proprio per la mancanza di supervisione

da parte di organi giudiziari, le autorità di pubblica sicurezza interessate a pratiche investigative « disinvolute » tendono più facilmente a ricorrere al § 505 piuttosto che al § 215. La norma, che emenda profondamente il Titolo V del FISA, sostituendo 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 tangible things* »), includendo in questa categoria libri, giornali, documenti — compresi quelli in ambito medico, abitualmente protetti dal massimo grado di riservatezza —, 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. L'investigatore che domanda l'emissione di un provvedimento ai sensi del § 215 non deve motivare la richiesta, ma solamente limitarsi a 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 espresse dal Governo a suo carico.

f) Nel 1986 si ammise 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 dunque 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. 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 intervenire indisturbata tra le comunicazioni private di un numero incalcolabile di americani ». Inoltre, dal momento che il già citato § 216 dell'USAPA 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 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* » 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.

Era probabilmente inevitabile che un provvedimento di tale portata provocasse prima o poi una reazione dell'apparato giudiziario, notoriamente considerato un anello fondamentale della catena di *checks and balances* teorizzata dai *Founding Fathers* statunitensi<sup>7</sup>. Forse assai meno facilmente ipotizzabile era invece l'impeto di tale reazione rispetto allo specifico rapporto tra sicurezza e libertà digitale, e che di seguito viene ricostruito attraverso i pronunciamenti giurisdizionali più rilevanti sul tema.

In *United States District Court Southern District of New York*<sup>8</sup> i giudici di distretto hanno valutato il citato § 505 dell'USAPA<sup>9</sup> 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 »<sup>10</sup>. 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*<sup>11</sup>. Richiamandosi ad una posizione a più riprese ribadita

<sup>7</sup> Cfr. in prop. per tutti S.M. GRIFFIN, *Il costituzionalismo americano. Dalla teoria alla politica*, Il Mulino, Bologna 2003, in part. pp. 165-179.

<sup>8</sup> Cfr. *John Doe v. John Ashcroft*, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).

<sup>9</sup> V. *supra*, in questo par., punto e).

<sup>10</sup> Cfr. *John Doe v. John Ashcroft*, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).

<sup>11</sup> Cfr. in proposito P. TORRETTA, « *Diritto alla sicurezza* » e (altri) *diritti e libertà della persona: un complesso bilan-*

*ciamento costituzionale*, in A. D'ALOIA, (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano 2003, pp. 451 ss., (464), la quale parlando in particolare 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

anche dalla Corte Suprema, secondo la quale « uno stato di guerra<sup>12</sup> 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 »<sup>13</sup>, la Corte federale di Distretto di New York ha quindi stabilito come in un Paese democratico sia compito del potere giudiziario verificare 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 criteri valutativi assoluti che non dovrebbero trovare spazio in un giudizio teso a conciliare due valori costituzionali di pari grado<sup>14</sup>. 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'applicabilità, 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<sup>15</sup>. L'esperibilità, consentita dal § 505 dell'U-SAPA, 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<sup>16</sup> (considerata in verità fondamentale dalla Corte per la riven-

di sicurezza dei diritti e quindi giuridica, impedisce che interferenze dei pubblici poteri possano ledere la sfera di libertà dei cittadini ».

<sup>12</sup> Per una valutazione sull'ingerenza della legislazione di guerra sugli standard di tutela dei diritti costituzionali nell'ordinamento degli Stati Uniti v. tra gli altri F. LANCHESTER, *Gli Stati Uniti e l'11 settembre 2001*, in [www.associazionedeicostituzionalisti.it](http://www.associazionedeicostituzionalisti.it) (10 agosto 2008); 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 XXI ss.

<sup>13</sup> 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).

<sup>14</sup> 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.

<sup>15</sup> Nella motivazione della sentenza re-

datta 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.

<sup>16</sup> 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 legiti-



dicazione 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<sup>17</sup>, 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 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 (*John Doe v. Alberto Gonzales*)<sup>18</sup>, 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'esigenza contrapposta fosse consistita in un « *compelling state interest* »<sup>19</sup>; 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 verifica da parte dell'autorità giurisdizionale della fondatezza del provvedimento amministrativo producesse un'indebita violazione del Primo emendamento<sup>20</sup>; soprattutto, il Giudice ha rilevato la difficoltà di accertare la conformità alla legge dell'esercizio dei poteri conferiti dalla norma impugnata alle forze di sicurezza, e quindi di prevenire eventuali abusi<sup>21</sup>. 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* »<sup>22</sup>, in quanto

timità, 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?*, in *Duke Law & Technologies Review*, 2/ 2006, pp. 1-51.

<sup>17</sup> 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.

<sup>18</sup> Disponibile in: <http://www.supremecourt.us/opinions/05pdf/05a295.pdf> (10 agosto 2008).

<sup>19</sup> 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.

<sup>20</sup> 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.

<sup>21</sup> « 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.

<sup>22</sup> Nel diritto processuale statunitense un caso è considerato « *moot* » se ulteriori

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 stati inevitabilmente rivelati. 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<sup>23</sup>. Nel marzo 2006, a seguito dell'emanazione della legge di reiterazione di buona parte dell'USAPA, 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 la sentenza *Doe v. Gonzales*. L'Esecutivo ha inoltre tentato di persuadere i giudici di secondo grado a sospendere anche la sentenza del tribunale 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*<sup>24</sup>.

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<sup>25</sup>, 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<sup>26</sup>. 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 si-

---

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.

<sup>23</sup> Malgrado nel complesso possa essere interpretata come sfavorevole alle posizioni dell'Esecutivo, la deliberazione non 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 co-

me 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* (Oct. 2005), in: The Free Expression Policy Project, disponibile in: <http://www.fepproject.org/commentaries/patriotact-oct2005.html> (10 agosto 2008).

<sup>24</sup> N. TRIVEDI, *Section 215 of the USA PATRIOT Act and National Security Letters*, cit. La sentenza è disponibile in: <http://www.ctd.uscourts.gov/Opinions/090905JCH.DoeOP.pdf> (10 agosto 2008).

<sup>25</sup> *American Civil Liberties Union v. National Sec. Agency*, 438 F. Supp. 2d 754. La sentenza è disponibile in: <http://jurist.law.pitt.edu/pdf/aclunsa.pdf> (10 agosto 2008).

<sup>26</sup> « *Usa, giudice dichiara incostituzionali le misure antiterrorismo di Bush* », Repubblica.it, 17 agosto 2006.

curezza: richiamandosi a pietre miliari della storia giurisprudenziale, sia del periodo coloniale che di quello successivo alla fondazione degli Stati Uniti<sup>27</sup>, 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<sup>28</sup>. Aderendo alla catalogazione dei poteri presidenziali rispetto agli orientamenti del Congresso, mirabilmente descritta in un'opinione concorrente dal Justice Robert H. Jackson in *Youngstown Sheet & Tube v. Sawyer*<sup>29</sup>, la sentenza sostiene poi come, 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 abbia agito 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* »)<sup>30</sup> 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* »<sup>31</sup>, la decisione prescrive l'immediata obbligatoria conclusione del provvedimento di sorveglianza elettronica<sup>32</sup>. 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

<sup>27</sup> 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. Rumsfeld*, 542 U.S. 507 (2004);

<sup>28</sup> *American Civil Liberties Union v. National Sec. Agency*, cit.. A questo proposito, rigettando l'argomentazione dei « poteri impliciti » (« *inherent 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.

<sup>29</sup> Nell'occasione il Giudice Jackson aveva decretato che le materie che investono 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 po-

sto 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.

<sup>30</sup> *Ibid.*, 637.

<sup>31</sup> *American Civil Liberties Union v. National Sec. Agency*, cit.

<sup>32</sup> 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).

del ricorso — hanno comunque dichiarato che si opporranno a qualunque ulteriore tentativo di dilazione dell'attuazione della sentenza<sup>33</sup>. Di contro, esponenti dell'Esecutivo hanno espressamente manifestato l'intenzione di battersi affinché la decisione fosse ribaltata in successivi gradi di giudizio, poiché a loro parere una sua effettiva applicazione avrebbe indebolito gli apparati difensivi del Paese<sup>34</sup>.

### 3. PORTOGALLO.

Anche nell'ordinamento portoghese si sono registrate vicende in cui il potere giudiziario — nella fattispecie il Tribunale Costituzionale — è intervenuto a ridimensionare la portata di provvedimenti legislativi relativi alla tutela della privacy in ambito informatico.

Tipico in questo senso è l'*acórdão* n. 241, emanato il 29 maggio 2002 in regime di controllo concreto di costituzionalità<sup>35</sup>. La decisione risponde al ricorso inoltrato contro una deliberazione in cui l'art. 519 n. 3 al. b del Codice di Procedura Civile portoghese è interpretato nel senso che al giudice viene riconosciuta la facoltà di ordinare agli operatori delle compagnie telefoniche di fornire informazioni su dati personali (nello specifico: tabulati e fatturazioni di una linea telefonica) contenuti nei loro sistemi informatici. Rispetto a quanto disposto negli artt. 26 n. 1 (diritto alla tutela della riservatezza della vita privata) e 34 (inviolabilità della corrispondenza e degli altri mezzi di comunicazione privata, divieto di ogni ingerenza delle pubbliche autorità nelle telecomunicazioni e negli altri mezzi di comunicazione, fatte salve le eccezioni previste dalla legge penale, deroga al generale obbligo di collaborazione di tutti i cittadini portoghesi di collaborare per l'accertamento della verità consistente nel divieto di intromissione nella vita privata o familiare, nel domicilio, nella corrispondenza o nelle telecomunicazioni) della Costituzione portoghese, i giudici costituzionali riscontrano delle incongruenze nella norma impugnata. Analizzando il contenuto del ricorso, la motivazione della decisione del *Tribunal Constitucional* presenta tra l'altro un'analisi degli sviluppi delle tecnologie informatiche, con particolare riferimento ad Internet.

A parere dei giudici costituzionali, la segretezza delle telecomunicazioni gode di un trattamento costituzionale specifico che, sebbene non possa configurarsi in una inviolabilità illimitata, agisce comunque con ampia portata, ricomprendendo non solo il contenuto delle telecomunicazioni in quanto tali, ma anche il loro « traffico ». Pertanto, il divieto di ingerenza

<sup>33</sup> « 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.

<sup>34</sup> Il Procuratore Generale Alberto R. Gonzales, uno dei principali artefici pro-

gramma 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.*

<sup>35</sup> Disponibile in: <http://www.tribunalconstitucional.pt/tc/acordaos/20020241.html> (10 agosto 2008),

nell'ambito delle telecomunicazioni si estende a tutte le informazioni ad esse connesse, indipendentemente dal fatto se queste siano fornite o meno da operatori di tale settore. Secondo il Tribunale Costituzionale portoghese, dunque, anche le informazioni ottenute via Internet possono suscitare forme di ingerenza nelle telecomunicazioni.

La peculiarità della decisione qui richiamata consiste nell'affermazione secondo cui la privacy meriti di essere tutelata anche riguardo alle informazioni diffuse tramite Internet, a cui si affianca il monito secondo cui « *o que está em causa... não é a mera confidencialidade dos dados pessoais fornecidos às operadoras de telecomunicações... É a própria inviolabilidade das telecomunicações que está em causa, pelo que nunca a dispensa de confidencialidade poderia justificar a ordem de prestação de informações constantes dos sistemas informáticos de operadores de telecomunicações, maxime en processo de natureza cível* »<sup>36</sup>.

#### 4. SPAGNA.

Sia prima che dopo i gravissimi attentati di Madrid del 2003, la cui matrice è stata da più parti accomunata a quella integralista islamica responsabile degli attacchi statunitensi del 2001, la giurisprudenza costituzionale spagnola è stata chiamata a confrontarsi con il problema del bilanciamento tra sicurezza collettiva e tutela delle libertà fondamentali anche in ambito informatico.

Tra le decisioni più recenti del *Tribunal Constitucional* spagnolo rilevanti per il tema qui considerato si annovera la sentenza n. 183 emanata il 20 ottobre 2003<sup>37</sup>, che ha giudicato violato il diritto al segreto delle telecomunicazioni da parte degli atti giurisdizionali che avevano posto sotto controllo le telefonate dei ricorrenti senza alcuna indicazione utile alla valutazione della necessità, idoneità e proporzionalità del provvedimento in questione. Il problema centrale sottoposto alla valutazione dei giudici costituzionali spagnoli riguardava la capacità della norma legislativa, preventiva rispetto alla disposizione di intercettazione, di stabilire con sufficiente chiarezza le fattispecie nelle quali questo tipo di provvedimento restrittivo della libertà di comunicazione. La norma che disciplina le modalità di esecuzione delle disposizioni di intercettazione è l'art. 579 della *Ley de Enjuiciamiento Criminal*, il quale, a parere dei supremi giudici iberici, non disporrebbe delle caratteristiche di predeterminazione necessarie a porre il magistrato in condizione di emanare tale provvedimento: la norma impugnata, infatti, non individuerebbe i soggetti nei confronti dei quali può essere disposta l'intercettazione, né la natura dei reati che ne giustificano l'adozione, né il tempo massimo di durata e le possibili successive proroghe della stessa, mancando inoltre di indicare le previsioni in grado di assicurare che la registrazione sia trasmessa integra e inalterata all'autorità giudiziaria. Ciononostante, la sentenza non si spinge a decre-

<sup>36</sup> Citato in R. ORRÚ, *Vicende e attività del Tribunal Constitucional portoghese nel biennio 2001-2002*, in *Giurisprudenza costituzionale*, 5/2003, pp. 3387-3421 (3421).

<sup>37</sup> Il testo della sentenza è disponibile in: <http://www.tribunalconstitucional.es/jurisprudencia/Stc2003/STC2003-183.html> (10 agosto 2008).

tare l'automatica incostituzionalità della condotta degli organi giudiziari che si servano della norma in questione, disponendo provvedimenti di intercettazione delle comunicazioni telefoniche, fin quando siano comunque rispettate le garanzie giurisdizionali previste in materia<sup>38</sup>: più precisamente, il *Tribunal Constitucional* statuisce nel caso in esame che anche in mancanza di adeguata previsione legislativa, per trovarsi in presenza di una lesione di un diritto fondamentale è necessario che si riscontri una impropria attività da parte del giudice che violi direttamente la posizione giuridica costituzionalmente tutelata. Qualora, di contro, si abbia a che fare con un reato grave ed i giudici abbiano applicato il provvedimento restrittivo nei confronti di soggetti presumibilmente coinvolti nella fattispecie criminosa, valutando la sua necessità, idoneità e proporzionalità in senso stretto, non sarebbe possibile ravvisare una violazione del diritto interessato. Così, senza decretare l'annullamento della norma impugnata, né integrandola con una sentenza interpretativa — limitandosi ad invitare il legislatore a provvedere a riguardo —, i giudici costituzionali spagnoli statuiscano un orientamento giurisprudenziale che richiama tutti gli organi giudiziari a prestare la massima attenzione alle specifiche condizioni del singolo caso sottoposto alla loro valutazione nel momento in cui sono chiamati a disporre provvedimenti così invasivi della libertà di comunicazione<sup>39</sup>.

Lungi dallo stabilire una parola definitiva sull'argomento, la sentenza citata è stata seguita da una considerevole serie di ulteriori pronunciamenti negli anni a seguire, in particolare nel biennio 2005-2006, aventi ad oggetto soprattutto la difesa dell'inviolabilità delle comunicazioni telefoniche rispetto ad intercettazioni disposte dai pubblici poteri, confermando in larga misura la tradizionale giurisprudenza del *Tribunal Constitucional* già espressa nella decisione n. 183 del 2003.

Così, la sentenza n. 165 del 2005<sup>40</sup> ha decretato che, qualora le intercettazioni siano state ottenute illecitamente, in quanto emanate sulla base di meri sospetti, e laddove esse costituiscano la sola prova del reato, oltre al diritto alla segretezza delle telecomunicazioni risultano violati il diritto ad un equo processo e la stessa presunzione di innocenza.

Non molto tempo dopo il *Tribunal Constitucional* è tornato a pronunciarsi sullo stesso tema: la sentenza n. 136 del 2006<sup>41</sup> ha riconosciuto la violazione del medesimo diritto in quanto negli atti giurisdizionali impugnati mancavano l'indicazione della giustificazione delle intercettazioni eseguite — ovvero il carattere illecito degli eventi oggetto delle indagini, i quali non possono essere giustificati da semplici sospetti — e la motiva-

<sup>38</sup> A tal proposito i giudici costituzionali si richiamano alla precedente sentenza 49 del 1999, che aveva già stabilito il principio della non automatica incostituzionalità di disposizioni vaghe o incomplete in materia di limitazioni della libertà di comunicazione.

<sup>39</sup> Per un commento alla decisione cfr. F. CAAMAÑO DOMÍNGUEZ, *Doctrina del Tribunal constitucional durante el tercer cuatrimestre de 2003. IV. Derechos fundamentales*, in Rev. española de derecho

constitucional 2004, n. 70, 308 e, in lingua italiana. M. IACOMETTI, *La giurisprudenza del Tribunale Costituzionale spagnolo nel biennio 2003-2004*, in *Giurisprudenza costituzionale*, 5/2005, 4366-4368.

<sup>40</sup> Disponibile in: <http://www.tribunal-constitucional.es/jurisprudencia/Stc2005/STC2005-165.html> (10 agosto 2008).

<sup>41</sup> Disponibile in: <http://www.tribunal-constitucional.es/jurisprudencia/Stc2006/STC2006-136.html> (10 agosto 2008).

zione dell'idoneità, necessità (e non mera utilità) e proporzionalità del provvedimento invasivo della libertà di comunicazione.

Tra le pronunce più rilevanti in materia di difesa della segretezza delle comunicazioni rientra la sentenza n. 205 del 2005<sup>42</sup>, la quale ricostruisce le modalità secondo cui va interpretato il termine iniziale dal quale decorre il periodo previsto per le intercettazioni autorizzate da adeguato atto giurisdizionale. Riguardo al criterio applicabile per valutare il rispetto da parte delle forze di sicurezza del periodo di intercettazione, la Consulta spagnola ha stabilito che il giorno a partire dal quale si può legittimamente esperire il provvedimento è quello della data dell'atto giurisdizionale che ha autorizzato le intercettazioni, e non quello del loro effettivo inizio. Fare riferimento a quest'ultimo termine, infatti, comporterebbe una sospensione del diritto al segreto delle comunicazioni per il periodo intercorrente tra il giorno in cui il magistrato emani la disposizione autorizzativa delle intercettazioni e quello in cui le intercettazioni inizino ad essere materialmente eseguite. La sentenza in oggetto, riferendosi in primo luogo al giudice che riteneva legittimo utilizzare il secondo dei due criteri citati, indubbiamente più elastico e pratico sul piano processuale, ma nel contempo senza dubbio meno garantistico, stabilisce quindi che l'interpretazione e l'applicazione di una norma riguardante dei diritti fondamentali debba sempre avvenire in modo da assicurare quanto più possibile il loro effettivo rispetto. Nel caso in esame, secondo il *Tribunal Constitucional* l'interpretazione fornita dal giudice della norma in questione provocava una limitazione della portata del diritto alla segretezza delle comunicazioni, provocandone una sospensione per un periodo potenzialmente molto esteso, risultando pertanto illegittima<sup>43</sup>.

Anche la sentenza n. 26 del 2006 è tornata sull'argomento, offrendo tra l'altro un'attenta ricostruzione della giurisprudenza costituzionale in materia di provvedimenti restrittivi della segretezza delle comunicazioni: la decisione è tornata a criticare per imprecisione e genericità — già stigmatizzate nella citata sentenza n. 184 del 2003 — il contenuto dell'art. 579 della *Ley de Enjuiciamiento Criminal*, il quale pertanto è stato giudicato contrario alle esigenze stabilite in materia di intercettazioni sia dal dettato costituzionale che dalla Corte europea dei diritti dell'uomo<sup>44</sup>.

Cambia leggermente il contesto di riferimento nella sentenza n. 104 del 2006<sup>45</sup>, dedicata all'utilizzo delle intercettazioni per il perseguimento di reati connessi all'utilizzo di tecnologie informatiche. Nella fattispecie in oggetto i ricorrenti lamentavano una sproporzionalità tra il provvedimento di intercettazione telefonica e la natura dell'ipotesi di reato in conseguenza della quale era stata emanata, ritenuta di lieve entità rispetto alla rilevanza della misura investigativa emanata. In particolare, nel caso in oggetto le

<sup>42</sup> Disponibile in: <http://www.tribunal-constitucional.es/jurisprudencia/Stc2005/STC2005-205.html> (10 agosto 2008).

<sup>43</sup> Cfr. in prop. I. TORRES MUÑOZ, *Doctrina del Tribunal Constitucional durante el segundo cuatrimestre de 2005. V. Derechos fundamentales*, in *Revista española de derecho constitucional*, 2005, n. 74, 277 s.

<sup>44</sup> Cfr. in prop. I. TORRES MUÑOZ, *Doctrina del Tribunal Constitucional durante el primer cuatrimestre de 2006. V. Derechos fundamentales*, in *Revista española de derecho constitucional*, 2006, n. 77, 246.

<sup>45</sup> Disponibile in: <http://www.tribunal-constitucional.es/jurisprudencia/Stc2006/STC2006-104.html> (10 agosto 2008).

indagini vertevano su fatti relativi ad un reato contro la proprietà intellettuale commesso tramite il ricorso alle nuove tecnologie, capaci di permettere la riproduzione senza autorizzazione di compact disc musicali successivamente venduti in un sito *Web* sulla Rete. Sebbene la pena per il delitto in questione fosse di lieve entità, il Tribunale costituzionale ha ritenuto assolutamente adeguata alle necessità costituzionali la misura di intercettazione, dal momento che il reato in questione provocava pesanti ripercussioni in ambito sociale ed economico. L'utilizzo delle nuove tecnologie avrebbe infatti reso più semplice la commissione del reato, in particolare per la vendita del materiale musicale riprodotto. La sentenza ha inoltre riconosciuto tra le cause giustificative dell'utilizzo di dette misure d'indagine la sostanziale impossibilità di effettuare i rilevamenti necessari attraverso altri metodi di investigazione. L'importanza della sentenza citata si ravvisa dunque nel fatto che, accanto ai criteri già citati per valutare la legittimità dei provvedimenti di intercettazione (gravità della pena, natura del bene giuridico protetto, sua rilevanza sociale, commissione del delitto ad opera di organizzazioni criminali), con essa i giudici costituzionali hanno introdotto anche il criterio della rilevanza delle tecnologie informatiche, che facilitano l'esecuzione del reato e ne rendono più arduo il perseguimento<sup>46</sup>.

## 5. FRANCIA.

Anche in Francia la giurisprudenza costituzionale è stata chiamata a dirimere occasioni di contrasto tra provvedimenti di protezione della sicurezza collettiva e la tutela di varie forme di esercizio della libertà personale in vari ambiti, compreso quello informatico.

In particolare merita un richiamo in questa sede una decisione che abbraccia molti aspetti coinvolti dalla tematica qui considerata, di cui è opportuno descrivere, sia pur sommariamente, i diversi profili: all'inizio del 2006 il *Conseil constitutionnel* ha decretato la conformità all'art. 66 della Costituzione francese (prescrittivo del principio del *due process of law*) di disposizioni con cui i servizi speciali della gendarmeria e della polizia erano stati autorizzati a raccogliere sia i dati tecnici relativi alle comunicazioni elettroniche<sup>47</sup>, sia, in modalità automatica, dati connessi agli autoveicoli<sup>48</sup>.

Nella stessa sentenza, inoltre, i giudici costituzionali verificano la conformità della disposizione impugnata all'obbligo di osservanza della riservatezza della vita privata dei cittadini, la cui effettività potrebbe essere minacciata dalla possibilità delle forze di polizia di conseguire dati legati alle comunicazioni elettroniche e agli autoveicoli, per finalità di lotta al terrorismo. Sul punto la pronuncia cerca di coniugare le due esigenze, individuando un adeguato bilanciamento nella dichiarazione di legittimità di un sistema di sorveglianza e raccolta di informazioni che sappia tenere in debita considerazione i diritti costituzionali potenzialmente a rischio<sup>49</sup>.

<sup>46</sup> Così M. IACOMETTI, *La giurisprudenza del Tribunale costituzionale spagnolo nel biennio 2005-2006*, in *Giurisprudenza costituzionale*, 5/2007, 3839-3934 (3889).

<sup>47</sup> Cfr. dec. 2005-532 DC, in *Recueil des décisions du Conseil constitutionnel*, 19 gennaio 2006, 31 ss., cons. 8.

<sup>48</sup> *Ibid.*, cons. 16

<sup>49</sup> *Ibid.*, cons. 10, 18-21.



Infine, per quanto attiene alla libertà d'impresa, la sentenza citata ritiene che la disposizione sottoposta alla valutazione del *Conseil* tenga nella giusta considerazione anche diritti accessori rispetto alla più generale libertà personale, quale appunto la libertà d'impresa degli imprenditori attivi nel settore delle comunicazioni elettroniche<sup>50</sup>.

## 6. GERMANIA.

Rispetto ai suoi omologhi nazionali, il Tribunale costituzionale di Karlsruhe sembra essersi occupato più attivamente di aspetti particolarmente complessi ed attuali relativi al tema in oggetto — probabilmente « aiutato » da misure legislative che spingono al limite, e forse anche oltre, il rapporto tra sicurezza pubblica e difesa delle libertà fondamentali in ambito informatico.

Tra le molte decisioni intervenute recentemente in questo ambito si annovera per prima, in ordine di tempo, quella con cui con cui è stato rigettato il ricorso diretto di un componente delle « cellule anti-imperialiste »<sup>51</sup>, posto sotto sorveglianza speciale tramite l'utilizzo del sistema satellitare GPS (*Global Positioning System*), critico riguardo alla genericità della legge con cui si autorizzavano le forze di sicurezza a compiere misure di sorveglianza « con strumenti tecnici ». La sentenza ha riconosciuto conformi al dettato costituzionale in materia di libertà personale e riservatezza le investigazioni condotte attraverso il ricorso al citato sistema satellitare GPS. In particolare, i supremi giudici tedeschi hanno statuito come non sia necessario che la legge menzioni esplicitamente ogni singola tecnologia utilizzabile a fini di indagine, sebbene gli stessi giudici abbiano nel contempo considerato indispensabile che il legislatore adotti gli accorgimenti normativi atti ad evitare casi di sorveglianza indiscriminata ai danni dei cittadini<sup>52</sup>.

In un'altra pronuncia relativa a tematiche contingenti, il *Bundesverfassungsgericht* fa riferimento al diritto all'autodeterminazione informatica e all'inviolabilità del domicilio in un caso relativo alla tracciabilità dei collegamenti tra telefoni cellulari, e alla possibilità di utilizzo a fini processuali dei dati così raccolti. Sebbene tali dati, salvati sul disco rigido di un computer, e rinvenuti nel corso di una perquisizione, non siano tutelati dalla segretezza delle telecomunicazioni protetto dall'art. 10 della Legge Fondamentale, i giudici di Karlsruhe considerano violati i diritti individuali del ricorrente, poiché il provvedimento giudiziario che ha disposto la perquisizione risulta in contrasto con il principio di proporzionalità: in particolare, nel caso in esame le esigenze investigative non apparivano di una gravità tale da giustificare un intervento talmente invasivo delle libertà fondamentali garantite dal dettato costituzionale<sup>53</sup>.

<sup>50</sup> *Ibid.*, cons. 10.

<sup>51</sup> Organizzazione sovversiva di orientamento politico socialista/comunista e di fede islamica, responsabile alla metà degli anni '90 di una serie di attentati dinamitardi ed incendiari.

<sup>52</sup> 2 BvR 581/01 del 12 aprile 2005, in

BVerfGE 112, 304, disponibile in: [http://www.bundesverfassungsgericht.de/entscheidungen/rs20050412\\_2bvr058101.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20050412_2bvr058101.html) (10 agosto 2008)

<sup>53</sup> 2 BvR 2099/04 del 2 marzo 2006, in BVerfGE 115, 166, disponibile in: <http://www.bundesverfassungsgericht.de/entsche>

Anche il *Bundesgerichtshof* ha avuto recentemente occasione di confrontarsi con il problema della conservazione dei dati personali di un utente di servizi telematici, risolvendo la questione con una decisione netta e severa a favore del ricorrente: l'occasione è venuta dalla *Verfassungsbeschwerde* di un 33enne di Münster, Holger Voss, contro T-Online, il *Provider* di Telekom, la principale compagnia telefonica tedesca. Nel 2002 Voss era stato sottoposto ad un procedimento giudiziario con l'accusa di aver espresso in un forum telematico giudizi di approvazione riguardo ad un reato penale, venendo al termine del giudizio assolto da ogni accusa: nel corso del processo era emerso come l'identificazione del ricorrente fosse avvenuta grazie alle informazioni sul suo conto raccolte e conservate dal suo *Provider*, T-Online, il quale dopo veementi proteste aveva chiesto l'intervento della magistratura. Sia il tribunale di prima istanza che la corte d'appello di Darmstadt avevano accolto le rimostranze di Voss, condannando T-Online alla cancellazione dei dati connessi al suo indirizzo di IP raccolti fino a quel momento, e riconoscendo l'illegittimità della sostanziale sorveglianza alla quale il *Provider* aveva sottoposto l'attività di navigazione on-line del suo cliente. L'Alta Corte federale tedesca ha quindi dichiarato irricevibile il ricorso di T-Online contro la decisione dei giudici di Darmstadt, che dunque è entrata in vigore a tutti gli effetti, obbligando la compagnia di servizi telematici ad adempiere alla disposizione della pronuncia impugnata. Sebbene valida solo nei confronti del ricorrente, si suppone che la decisione del *Bundesgerichtshof*<sup>54</sup> possa rappresentare una pietra miliare in materia di tutela dei dati personali in Rete per gli utenti residenti in Germania, tanto che alcuni studi di avvocati hanno approntato dei modelli di ricorso per tutti i cittadini tedeschi interessati a conseguire lo stesso risultato ottenuto da Voss<sup>55</sup>.

Introducendo un tema particolarmente attuale per le materie qui considerate, il *Bundesverfassungsgericht*, è stato chiamato a pronunciarsi sul ricorso a provvedimenti di intercettazione preventiva anche a livello sub-statale, dichiarando costituzionalmente illegittimi i controlli sugli apparecchi telefonici eseguiti per l'appunto preventivamente nel Land Bassa Sassonia, sulla base della legge sulla polizia del Land, giudicandoli in conflitto con l'inviolabilità della corrispondenza, non sufficientemente limitati nelle condizioni di utilizzo e non rispondenti al principio di ragionevolezza<sup>56</sup>. La legge in questione consentiva agli inquirenti di condurre intercettazioni su contenuti e dati di telefonate, fax, sms ed e-mail ove ravvisassero elementi, sia pure generici, che giustificassero il timore di un possibile compimento di reati particolarmente gravi. Abituamente i soggetti sottoposti a tali misure di indagine erano informati solo in un secondo momento dell'accaduto, ma in alcuni casi venivano mantenuti del tutto all'oscuro della vicenda. Il Tribunale costituzionale ha ritenuto che la norma impu-

idungen/rs20060302\_2bvr209904.html (10 agosto 2008).

<sup>54</sup> Aktz. III ZR 40/06, disponibile in: <http://www.kein1984.de/bgh-entscheidung.pdf> (10 agosto 2008).

<sup>55</sup> Cfr. tra gli altri T. KLEINZ, *BGH bestätigt Urteil zur Löschung von IP-Adressen*, 6 novembre 2006, in: <http://www.heise.de/newsticker/BGH-bestaetigt-Urteil-zur-Loeschung-von-IP-Adressen-/meldung/80614> (10 agosto 2008).

de/newsticker/BGH-bestaetigt-Urteil-zur-Loeschung-von-IP-Adressen-/meldung/80614 (10 agosto 2008).

<sup>56</sup> 1 BvR 668/04 del 27 luglio 2005, in BVerfGE 113, 348, disponibile in: [http://www.bundesverfassungsgericht.de/entscheidungen/rs20050727\\_1bvr066804.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20050727_1bvr066804.html) (10 agosto 2008).

gnata non operasse una distinzione sufficientemente adeguata tra i diversi possibili casi di reato grave, producendo una restrizione considerata eccessiva del diritto alla riservatezza, il quale — si precisa nella sentenza — va invece sempre tutelato anche in presenza di intercettazioni. Al di là del valore dei principi ribaditi in essa, la pronuncia si dimostra particolarmente rilevante anche per il fatto che, interessando l'intero territorio della Repubblica Federale, non si arresta alla situazione vigente in Bassa Sassonia, ma influenza in modo considerevole anche l'operato dei legislatori degli altri Länder, molti dei quali stavano approntando provvedimenti dello stesso tenore di quello sanzionato.

Come si vedrà poco oltre, peraltro, la materia alla base del ricorso in oggetto è poi tornata di lì a pochi mesi di stretta attualità, quando il Tribunale costituzionale ha dovuto esaminare la legittimità di una legge del Bund che autorizzava le forze di pubblica sicurezza federali a far uso degli stessi metodi di investigazione sanzionati in occasione del caso appena citato<sup>57</sup>. In questa occasione i giudici di Karlsruhe hanno pronunciato parole ancora più nette che nei pronunciamenti precedenti, in quella che molti considerano «la» sentenza di riferimento in materia di legittimità dei controlli di pubblica sicurezza in ambito informatico nel contesto giurisprudenziale tedesco: si tratta della decisione relativa alla cd. *Rasterfahndung* (lett.: «indagine a setaccio»<sup>58</sup>) un metodo già in uso durante la lotta all'eversione interna negli anni '70, ed ora utilizzato anche per le investigazioni sui fenomeni di terrorismo internazionale. Il metodo in questione consiste nel selezionare gruppi di persone attraverso banche dati pubbliche o private, facendo riferimento ad elementi che si suppone riguardino anche la persona che si intende effettivamente individuare. Di fatto, fissando dei criteri che solo *presumibilmente* si attagliano ai soggetti ricercati dalle forze dell'ordine, possono di fatto essere portati all'attenzione degli inquirenti anche profili di individui assolutamente estranei alle fattispecie di reato per le quali il metodo investigativo citato viene utilizzato, sollevando non pochi dubbi in merito al rispetto dei più elementari diritti costituzionali. Il Tribunale costituzionale tedesco ha dichiarato tale forma di indagine compatibile con il diritto all'autodeterminazione informatica del singolo individuo solo in caso di concreto pericolo per valori giuridici che richiedano la massima protezione, quali l'esistenza dello Stato o la vita e la libertà dei cittadini. Lo stesso metodo non è invece considerato ammissibile quale abituale strumento investigativo, né può considerarsi sufficiente, per giustificare l'impiego, l'esistenza di un indefinito pericolo di attentati terroristici<sup>59</sup>. Dunque, affinché la *Rasterfahndung* sia considerata ammissibile, i giudici di Karlsruhe stabiliscono nettamente i casi in cui ci si possa trovare di fronte alla straordinarietà di un «pericolo eccezionale», chiarendo nel contempo di essere pronti a censurare qualunque utilizzo di tale metodo di indagine per finalità investigative ordinarie. Molti hanno dunque interpretato queste disposizioni come un chiaro ammonimento nei confronti del legislatore ad evitare una regolamentazione troppo

<sup>57</sup> V. *infra*, in questo paragrafo.

<sup>58</sup> Così tradotto da F. PALERMO, *La giurisprudenza costituzionale tedesca nel biennio 2005-2006*, in *Giurisprudenza costituzionale*, 2007, 3973-4006 (3978).

<sup>59</sup> 1 BvR 518/02 del 4 aprile 2006, in BVerfGE 115, 320, disponibile in Rete in [http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404\\_1bvr051802.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html) (10 agosto 2008).

permissiva rispetto ad usi « disinvolti » della *Rasterfahndung*, rischiando, così facendo, di non tenere nella dovuta considerazione la proporzionalità tra la gravità del crimine perseguito e l'invasività dei metodi di indagine nell'ambito delle libertà fondamentali della persona<sup>60</sup>.

La decisione citata non ha comunque posto fine alle controversie in materia: nel febbraio del 2008 il Tribunale Costituzionale federale è stato nuovamente chiamato ad operare un complesso bilanciamento tra la tutela della sicurezza collettiva e la difesa dei diritti della personalità nel contesto informatico, emanando una decisione che con tutta probabilità è destinata a modificare profondamente l'approccio giurisprudenziale e, conseguenzialmente, legislativo alla trattazione della materia per il futuro: la rilevanza del pronunciamento è infatti tale da far ritenere che i principi stabiliti dai giudici di Karlsruhe non arresteranno i loro effetti all'interno dei confini della Repubblica Federale di Germania, ma potrebbero verosimilmente ispirare anche altri supremi organi giurisdizionali alle prese con problematiche dello stesso tipo<sup>61</sup>.

Nel caso in oggetto il *Bundesverfassungsgericht* è stato interpellato sulla base di una serie di ricorsi individuali presentati in via diretta da soggetti strettamente legati a vario titolo alla conduzione di attività sulla Rete: una giornalista componente della federazione regionale del NRW del partito « Die Linke », e tre avvocati.

L'oggetto dei ricorsi riguardava la presunta incostituzionalità di alcune disposizioni della Legge di Tutela della Costituzione del Land Nordreno-Vestfalia (*Verfassungsschutzgesetz Nordrhein-Westfalen*): in particolare, al Tribunale Costituzionale federale veniva richiesto di valutare sotto diversi profili la legittimità dell'art. 5 comma 2 nr. 11 della legge in questione, il quale testualmente recita:

« *L'autorità di tutela della Costituzione [del Nordreno-Vestfalia], in applicazione dell'art. 7 [della stessa legge] sulla raccolta di dati e notizie può utilizzare i seguenti provvedimenti come strumenti di informazione: [...] sorveglianza segreta (heimliches) ed indagini straordinarie di Internet, come in particolare la partecipazione sotto copertura alle sue strutture di comunicazione o la loro ricerca, nonché l'accesso segreto a sistemi informatici anche con l'utilizzo di strumenti tecnologici. Laddove tali provvedimenti costituiscano un'ingerenza nella segretezza della corrispondenza, postale e telematica, o per loro natura o entità vi si equiparano, questa è ammissibile solo in base alle condizioni della disciplina relativa all'art. 10 della Legge Fondamentale* ».

La decisione del Tribunale Costituzionale federale accoglie vari aspetti dei ricorsi citati, rilevando alcuni profili di incostituzionalità della norma

<sup>60</sup> Per una panoramica delle opinioni espresse in dottrina sul tema cfr. W. BAUSBACK, *Fesseln für die wehrhafte Demokratie?*, in *Neue Juristische Wochenschrift*, 2006, p. 1922 ss.; U. VOLKMANN, *Grenzen der präventiven Rasterfahndung*, in *JuristenZeitung*, 18/2006, p. 906 ss.; G. KETTSTRAUB, *Rasterfahndung fällt durch das Raster des Grundgesetzes*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9/2006, p. 447 ss. In lingua italiana cfr.

V. BALDINI, *L'incostituzionalità della Rasterfahndung, ovvero, alla perenne ricerca di un (difficile...) equilibrio tra stato di diritto e « stato di prevenzione »*, disponibile in: <http://associazioneedicostituzionalisti.it/materiali/anticipazioni/rasterfahndung/index.html> (10 agosto 2008).

<sup>61</sup> BvR 370/07 del 27 febbraio 2008, disponibile in Rete in [http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227\\_1bvr037007.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html) (10 agosto 2008).

impugnata con un'argomentazione di natura profondamente innovativa rispetto alle precedenti pronunce relative a tematiche dello stesso genere. In particolare, i supremi giudici tedeschi ravvisano l'incostituzionalità delle pratiche di indagine consentite dalla disciplina impugnata (cd. *Online-Durchsuchungen* — lett.: perquisizioni online)<sup>62</sup> notando in primo luogo come per molti cittadini l'utilizzo di sistemi informatici abbia assunto una rilevanza fondamentale per l'estrinsecazione della loro personalità, giustificando tuttavia nel contempo anche il timore che ne conseguano nuove forme di minaccia alla tutela dell'identità individuale: la sorveglianza delle attività condotte attraverso tali sistemi, unita ad un esame dei dati rintracciabili sugli apparati informatici utilizzati, permettono infatti di ricostruire aspetti salienti della personalità di un soggetto. Da questa considerazione i giudici di Karlsruhe fanno discendere la necessità di approntare un'adeguata forma di protezione dei diritti fondamentali coinvolti, rilevando innanzi tutto che la tutela prevista dagli artt. 10 (segretezza delle telecomunicazioni) e 13 (inviolabilità del domicilio) della Legge Fondamentale, come pure la giurisprudenza prodotta finora dallo stesso *Bundesverfassungsgericht* in materia di protezione della personalità, non riescono ad offrire garanzie adeguate alle possibili ingerenze provenienti dallo sviluppo delle tecnologie informatiche.

Per quanto riguarda l'ambito di tutela della segretezza delle telecomunicazioni, si legge nella sentenza, questo coinvolge anche le comunicazioni esperibili tramite Internet, come ad es. i messaggi di posta elettronica: fin quando l'indagine si basa su un provvedimento con cui si rilevano contenuti e circostanze della telecomunicazione in corso sulla rete informatica, e si esaminano le informazioni che ne derivano, l'ingerenza in questione deve essere valutata esclusivamente sulla base dell'art. 10 I della Legge Fondamentale. L'ambito di tutela di questo diritto fondamentale, quindi, viene interessato indipendentemente dall'eventualità che, sotto un piano meramente tecnico, il provvedimento di indagine riguardi il tratto della rete informatica utilizzato o l'apparecchio finale impiegato per l'esperimento della telecomunicazione posta sotto sorveglianza. Pertanto, statuisce la pronuncia in oggetto, l'art. 10 comma 1 LF risulta l'unico parametro

<sup>62</sup> Da un punto di vista strettamente tecnico, per « Online-Durchsuchungen » si intendono attività di indagine condotte grazie all'utilizzo di specifici software (cd. *Trojans*), finalizzati all'individuazione ed all'esame di dati informatici. Tali programmi possono essere immessi clandestinamente in un determinato computer attraverso Internet, ed essere poi adoperati per spiare i dati salvati sul disco rigido o le applicazioni utilizzate dal terminale, il tutto senza che il proprietario o l'utente del computer « infiltrato » ne venga a conoscenza. Cfr. C. KELLER, *Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen*, R. Boorberg Verlag, Stuttgart et al. 2008, pp. 48-50; D. FOX, *Realisierung, Grenzen und Risiken der « Online-Durchsuchung »*, in *Datenschutz und Datensicherheit*, 31/2007, pp. 327-

834, disponibile in: <http://www.secorvo.de/publikationen/online-durchsuchung-fox-2007.pdf> (10 agosto 2008); K. LEIPOLD, *Die Online-Durchsuchung*, in *Neue Juristische Wochenschrift-Spezial*, 3/2007, pp. 135-136; U. BUERMAYER, *Die « Online-Durchsuchung »*, *Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme*, in *HRRS - Onlinezeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht*, 4/2007, pp. 154-166, disponibile in: <http://www.hrr-strafrecht.de/hrr/archiv/07-04/hrrs-4-07.pdf> (10 agosto 2008); M. HANSEN-A. PFITZMANN, *Online-Durchsuchung. Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme*, in *Deutsche Richterzeitung*, 8/2007, pp. 225-228, in: <http://www.heymanns.com/servlet/PB/menu/1226897/index.html> (10 agosto 2008).

di costituzionalità utilizzabile per valutare la legittimità di un provvedimento di autorizzazione ad una « sorveglianza delle fonti di telecomunicazione » nei casi in cui l'indagine sia limitata esclusivamente all'esame di dati provenienti da un'attività di telecomunicazione, e la sua osservanza va assicurata attraverso adeguati strumenti tecnici e giuridici.

Di contro, la tutela sancita dall'art. 10 comma 1 LF non si estende a contenuti e circostanze di una telecomunicazione che, dopo la sua conclusione, siano stati salvati in un ambito su cui esercita piena disponibilità uno dei partecipanti alla telecomunicazione stessa, fin quando quest'ultimo può assumere provvedimenti atti a difendere la riservatezza di tali dati da ingerenze occulte: è fin troppo chiaro, in questo passaggio, il riferimento dei giudici ai dischi rigidi dei personal computer, nei quali i dati relativi alle comunicazioni informatiche vengono immagazzinati e possono essere richiamati a piacimento dai loro proprietari o utilizzatori. Ancora, l'inviolabilità delle telecomunicazioni non trova applicazione nei casi in cui sia una pubblica autorità a sorvegliare le modalità di utilizzo di un sistema informatico in quanto tale, o ad esaminarne gli strumenti di memorizzazione dei dati. Da tutto questo consegue una lacuna nella protezione del diritto fondamentale alla segretezza delle telecomunicazioni nella forma attualmente vigente, che secondo i giudici di Karlsruhe va colmato con il ricorso alla generale tutela del diritto al libero sviluppo della personalità, sancito dall'art. 2 comma 1 LF — nel caso specifico interpretato come tutela dell'integrità e dell'affidabilità dei sistemi di comunicazione informatica. Infatti, si legge nella sentenza, nel momento stesso in cui un articolato sistema informatico diviene oggetto di misure di sorveglianza telematica, viene meno l'ostacolo che impedisce di spiare potenzialmente l'intero sistema nel suo complesso. Il potenziale pericolo che viene in questo modo a prospettarsi si estende ben oltre la semplice sorveglianza della singola telecomunicazione eseguita mentre il provvedimento di indagine è in atto: in particolare, nel corso dell'investigazione possono essere raccolti dati contenuti nei personal computer interessati dal provvedimento che non hanno alcuna relazione con l'utilizzo del sistema informatico posto sotto controllo.

Nemmeno la garanzia dell'inviolabilità del domicilio appare agli occhi dei giudici una tutela sufficiente ad escludere lacune nella protezione contro ingerenze in sistemi di comunicazione informatica. L'art. 13 comma 1 LF, infatti, non assicura al singolo una difesa completa contro le infiltrazioni nel sistema informatico da lui utilizzato, indipendentemente dalle modalità di accesso a cui è stato fatto ricorso, anche nel caso in cui questo sistema si trovi nella sua propria abitazione, in quanto l'accesso può avvenire a prescindere dalla collocazione fisica del sistema informatico indagato. Pertanto, una disciplina di tutela che sia legata ad uno specifico contesto spaziale — quale è la prescrizione di inviolabilità del domicilio — non è in grado di offrire una difesa appropriata da pericoli contro sistemi di telecomunicazioni: infatti, nel momento in cui l'attività di sorveglianza si serve del collegamento del computer del soggetto interessato ad una rete informatica, la protezione della sfera privata esperita dall'inviolabilità del domicilio resta sostanzialmente priva di efficacia.

Ancora, la sentenza ritiene che nemmeno la giurisprudenza finora sancita dal *Bundesverfassungsgericht* in materia di difesa del generale diritto al libero sviluppo della personalità individuale, in particolare riguardo alla protezione della sfera privata e del diritto all'autodeterminazione informatica, sia sufficiente a garantire un'adeguata tutela di un sistema in-

formatico: le esigenze di protezione di un utente di un sistema informatico non si limitano infatti a dati subordinati alla sua sfera privata. Anche il diritto all'autodeterminazione informatica non tiene conto adeguatamente delle minacce esistenti per la sfera della personalità dell'individuo. Un soggetto terzo che penetri in un sistema informatico del tipo qui considerato, infatti, è potenzialmente in grado di procurarsi una quantità di dati di estrema rilevanza sia per dimensioni che per significatività, senza essere vincolato da ulteriori provvedimenti di raccolta ed elaborazione di informazioni.

Secondo il Tribunale Costituzionale federale, pertanto, il generale diritto della personalità più volte chiamato in causa deve intervenire a colmare le esigenze di tutela appena esposte e insoddisfatte dalla tradizionale interpretazione del diritto in questione, sancendo e garantendo un vero e proprio « diritto fondamentale all'integrità ed all'affidabilità dei sistemi di comunicazione informatica ». Tale diritto trova applicazione ogni qual volta la conduzione di attività di *intelligence* riguardi sistemi che, di per sé o a causa delle loro connessioni tecniche, possono contenere dati personali di un soggetto in misura e rilevanza tali da consentire, attraverso la raccolta e l'analisi di questi ultimi, di venire a conoscenza di aspetti significativi dell'esplicazione della sua personalità o di tracciare un quadro significativo della sua individualità.

La sentenza statuisce che l'incostituzionalità della norma impugnata deriva in primo luogo da una violazione del principio di proporzionalità: l'azione investigativa in questione permette infatti una penetrazione talmente ampia negli strumenti di raccolta di dati personali, che la loro ampiezza e eterogeneità rischia facilmente di eccedere lo scopo per il quale la misura di indagine è stata istituita. In questo modo si paventa una pervasività tale nella sfera più intima della personalità del soggetto indagato da poter essere considerata costituzionalmente legittima solo in casi particolarmente eccezionali, in cui il fondamentale valore dell'inviolabilità della dimensione individuale della persona può essere sacrificato in nome di valori giuridici (*Rechtsgüter*) particolarmente rilevanti, minacciati da pericoli di cui sia stata sufficientemente comprovata l'esistenza. Tra questi ultimi, la decisione menziona « l'integrità fisica, la vita e la libertà della persona, o valori appartenenti alla collettività che, se minacciati, coinvolgono i fondamenti o l'esistenza dello Stato, o i fondamenti dell'esistenza degli individui ». D'altro canto, i giudici di Karlsruhe precisano come a questo scopo non sia necessario dimostrare l'imminente probabilità di un pericolo concreto per i beni in questione, essendo piuttosto sufficiente ravvisare l'esistenza di una minaccia specifica a loro carico per giustificare il ricorso a misure di indagine invasive come quella consentita dalla norma impugnata. Nel contempo, tuttavia, gli stessi giudici tengono a sottolineare come un provvedimento di autorizzazione alla penetrazione segreta in sistemi informatici non possa sottrarsi alle più elementari garanzie previste dall'ordinamento giuridico per tutelare sul piano costituzionale gli interessi dell'indagato, a cominciare dal rispetto della riserva di giurisdizione e dall'adozione di un adeguato procedimento legislativo. La norma impugnata viene considerata carente sotto questo punto di vista, nel momento in cui, per autorizzare i servizi di sicurezza ad utilizzare gli strumenti di indagine citati, si limita a richiedere come unica condizione la presenza di elementi fattuali che giustifichino il sospetto di poter raccogliere informazioni relative ad azioni

eversive ed anticostituzionali — in questo mancando sia di esigere l'esistenza di circostanze sufficientemente rilevanti per legittimare le gravi ingerenze che il metodo investigativo in oggetto provoca, sia una preventiva verifica da parte di soggetti terzi indipendenti (*rectius*: l'autorità giudiziaria).

La decisione ravvisa inoltre la mancanza di adeguate disposizioni legislative atte ad evitare ingerenze nel nucleo costitutivo della sfera individuale privata, per il quale l'ordinamento prevede una tutela assoluta ed invalicabile. A tale riguardo, la sentenza non trascura la circostanza che, una volta poste in essere, le misure di indagine in questione consentono una penetrazione tale nei sistemi informatici da non poter permettere una conoscenza preventiva del contenuto dei dati raccolti, al fine di distinguere tra le informazioni legittimamente investigabili e quelle che, in quanto appartenenti al suddetto « nucleo individuale invalicabile », non possono al contrario essere oggetto di investigazione. Non potendo agire sulla fase preventiva, per le suddette ragioni di carattere tecnico che caratterizzano i sistemi investigati, il legislatore avrebbe dovuto necessariamente prevedere adeguati provvedimenti di valutazione a posteriori dei dati raccolti, assicurando la cancellazione immediata ed escludendo un eventuale recupero successivo a qualsiasi titolo di tutte le informazioni emerse nell'indagine che risultino appartenere alla seconda delle due sfere indicate — quella, per l'appunto, dei dati indisponibili in quanto direttamente connessi alla sfera intangibile della personalità individuale. Anche sotto questo profilo i giudici di Karlsruhe decretano l'incostituzionalità della norma impugnata, in quanto ritenuta non conforme alle esigenze descritte poc'anzi.

Per quel che rileva in questa sede, come già anticipato, l'elemento maggiormente degno di nota dell'intera vicenda si sostanzia senza dubbio nella creazione, di fatto, di un vero e proprio « nuovo diritto fondamentale » all'integrità ed all'affidabilità dei sistemi di comunicazione informatica non ancora previsto e pertanto non adeguatamente garantito dall'ordinamento costituzionale tedesco vigente. In altre parole, le forme di intervento nella sfera privata consentite dalle nuove forme di sorveglianza esigono la definizione di corrispondenti situazioni giuridiche soggettive di tutela, capaci di assicurare un'adeguata forma di protezione dei diritti costituzionalmente garantiti in capo ai soggetti interessati dai provvedimenti di sorveglianza. La circostanza che i giudici di Karlsruhe non si siano limitati a dichiarare la mera incostituzionalità della norma impugnata, ma abbiano avvertito la necessità di proclamare l'esistenza di un nuovo diritto fondamentale, non è ovviamente affatto secondaria: al contrario, proprio in questa differenza radicale dell'approccio scelto dalla sentenza si sostanziano la cautela e l'inquietudine con le quali il Tribunale costituzionale federale ha affrontato la questione.

La straordinarietà della pronuncia viene inoltre ulteriormente evidenziata da alcuni elementi fattuali di estrema rilevanza, che avrebbero potuto indurre i giudici di Karlsruhe ad optare per un sostegno alla tutela della sicurezza collettiva, a scapito delle garanzie costituzionali individuali, giustificando una tale decisione con la presenza di eccezionali condizioni emergenziali dovute alla minaccia proveniente dall'integralismo islamico, frequentemente invocate ad altre latitudini per giustificare ben altri orientamenti legislativi e giurisdizionali in materia. Tra le circostanze oggettive in questione si annovera, in primo luogo, l'ormai ben nota presenza nella



città di Amburgo per sei anni, dal 1993 al 1999, sotto le spoglie di studente universitario, di uno dei capofila del gruppo terroristico affiliato ad Al-Qaida materialmente responsabile degli attacchi terroristici a New York e Washington nel 2001, Mohammed Atta, capace persino di conseguire un diploma in pianificazione urbanistica prima di recarsi in Afghanistan per prepararsi agli attentati in un campo di addestramento talebano, e quindi spostarsi negli Stati Uniti; sempre da Amburgo, inoltre, sono transitati anche altri tre componenti del commando terrorista dell'11 settembre (Ramzi Binalshibh, Marwan al Shehhi e Ziad Jarrah), venuti per vie diverse in contatto con Atta proprio durante il loro soggiorno anseatico<sup>63</sup>. In secondo luogo, negli ultimi due anni per ben due volte il territorio tedesco aveva rischiato di divenire teatro di gravi attentati terroristici di matrice islamica: in un primo caso, il 31 luglio 2006, un doppio tentativo di far esplodere treni regionali a Coblenza e Hamm, nei pressi di Dortmund, organizzato da un gruppo di attentatori libanesi, di nuovo celatisi sotto le spoglie di studenti universitari — questa volta nell'ateneo di Kiel, in Schleswig-Holstein —, era stato sventato dalle forze di sicurezza tedesche in collaborazione con i loro omologhi di Beirut<sup>64</sup>; poco più di un anno dopo era stato il turno di tre sospetti terroristi di matrice musulmana integralista (due cittadini tedeschi convertiti all'Islam ed un cittadino turco-tedesco), arrestati il 5 settembre 2007 con l'accusa di pianificare attentati nell'aeroporto internazionale di Francoforte e nella base militare statunitense di Ramstein, in concomitanza con il 6° anniversario degli attacchi di New York e Washington<sup>65</sup>.

Sebbene, dunque, a differenza di Spagna e Gran Bretagna, la Germania non abbia fortunatamente ancora dovuto pagare pesanti bilanci in termini di vittime di attentati terroristici, gli eventi citati hanno indotto molti tra media ed esponenti politici — a cominciare dal Ministro federale degli Interni Wolfgang Schäuble (CDU), in questo appena tiepidamente contrastato dai partner di governo socialdemocratici, forse anche per via della sostanziale continuità mostrata in materia con gli orientamenti del suo predecessore Otto Schily (SPD) — ad assumere atteggiamenti più o meno apertamente allarmistici, tesi a paventare l'esistenza di un'articolata e complessa rete di cd. *Sleepers* (terroristi sotto copertura di insospettabili spoglie civili, aderenti all'estremismo islamico insediati segretamente in territorio tedesco in attesa di porre in atto azioni distruttive ed eversive), contro la quale sarebbe necessario intervenire con un massiccio ampliamento dei poteri investigativi dei servizi di sicurezza<sup>66</sup>.

<sup>63</sup> Sulla cd. «cellula di Amburgo» del commando terrorista dell'11 settembre 2001 cfr. *National Commission on Terrorist Attacks Upon the United States*, cap. 5.3., disponibile in: [http://www.9-11commission.gov/report/911Report\\_Ch5.htm](http://www.9-11commission.gov/report/911Report_Ch5.htm) (10 agosto 2008).

<sup>64</sup> Cfr. H. LAYENDECKER, *Netzwerk der Wirrwarrrs*, in *Süddeutsche Zeitung*, 21 agosto 2006, disponibile in <http://www.sueddeutsche.de/deutschland/artikel/209/83126/> (10 agosto 2008).

<sup>65</sup> *Terrorverdächtige in Deutschland festgenommen*, in *Süddeutsche Zeitung*, 5 settembre 2007, disponibile in <http://www.sueddeutsche.de/ausland/artikel/633/131400/> (10 agosto 2008).

<sup>66</sup> Cfr. per tutti M. GEBAUER, *Große Koalition der Datenjäger*, in *Spiegel online*, 2 aprile 2007, disponibile in: <http://www.spiegel.de/politik/deutschland/0,1518,475253-2,00.html> (10 agosto 2008).

## 7. CONCLUSIONI: UNO SGUARDO ALL'ITALIA E LE PROSPETTIVE FUTURE.

Come è da tempo ben noto agli esperti del settore, i provvedimenti anti-terrorismo emanati in Italia all'indomani dell'11 settembre 2001 hanno provocato una massiccia azione di raccolta di dati personali, attraverso misure che per anni hanno costretto diversi operatori telematici ed informatici alla conservazione obbligatoria delle informazioni conseguite sui propri utenti. Altrettanto nota è la circostanza per cui, a quanto è dato sapere, malgrado le azioni di *intelligence* condotte negli ultimi anni non abbiano finora consentito l'individuazione di casi rilevanti di organizzazioni terroristiche insediate sul territorio nazionale, la sostanziale sospensione di alcuni diritti fondamentali riconosciuti ai cittadini italiani (quale quello alla cancellazione dei dati che li riguardano) a suo tempo giustificata proprio con l'esistenza di una grave « emergenza terrorismo », permanga in vigore. Alla fine del 2007, infatti, il Governo di centrosinistra allora al potere aveva rinnovato una delle più controverse misure del Decreto Pisanu — approvato come è noto dal precedente Esecutivo di centrodestra e fortemente criticato dall'opposizione dell'epoca —, quella sulla c.d. « *data retention coatta* », che obbliga operatori e fornitori all'identificazione degli utenti e alla conservazione dei dati delle loro comunicazioni: un provvedimento che molti hanno giudicato non soltanto un inutile ostacolo alla fruibilità dei servizi telematici ed informatici, ma anche — e soprattutto — una pesante violazione della privacy del cittadino.

Nomi e cognomi, data e ora della connessione, delle telefonate, dei fax, numeri e indirizzi dei coinvolti: secondo il citato Decreto Pisanu<sup>67</sup>, *tutto*, a parte il contenuto della comunicazione, andava conservato fino a dicembre 2007<sup>68</sup>. Attraverso l'inserimento dell'articolo 34 (« *Proroghe in materia di contrasto al terrorismo internazionale* ») nel provvedimento normativo noto come « *Decreto milleproroghe* »<sup>69</sup>, la scadenza della misura di sorveglianza delle TLC è stata posticipata di un anno, dunque al 31 dicembre 2008. La circostanza aveva provocato forti proteste e inquietudini, inducendo tra l'altro il Garante per la protezione dei dati personali a inviare una preoccupata lettera al Presidente della Camera ed al Ministro delle po-

<sup>67</sup> Decreto Legge 27 luglio 2005, n. 144, « Misure urgenti per il contrasto del terrorismo internazionale », convertito in legge con L. 31 luglio 2005, n. 155, entrambi pubblicati in G.U. n. 177 del 1 agosto 2005 e disponibili in <http://www.parlamento.it/leggi/051551.htm#decreto> (10 agosto 2008).

<sup>68</sup> Si noti, a questo riguardo, come la Commissione libertà civili del Parlamento Europeo avesse a suo tempo indicato tra sei e dodici mesi l'opportuno arco di tempo di validità di provvedimenti di « *data retention* » emanabili dai Governi degli Stati membri dell'Unione, considerati accettabili ma solo se contenuti nei loro termini di applicazione. A loro volta, i Garanti europei della privacy li aveva considerati in tutto e per tutto misure di intercettazione, e dun-

que caratterizzate da una netta straordinarietà sia nella portata che nella durata della loro validità. Sul tema cfr. *UE: si a sei mesi di intercettazione*, in <http://punto-informatico.it/1353863/PI/News/ue-si-sei-mesi-intercettazioni.aspx> (10 agosto 2008). Ancora degna di nota la circostanza per la quale il cd. Decreto Pisanu fosse già stato emanato prima del pronunciamento dell'Euro-parlamento che ammetteva la legittimità delle misure di *data retention*.

<sup>69</sup> *Rectius*: Decreto-legge 31 dicembre 2007, n. 248 « Proroga di termini previsti da disposizioni legislative e disposizioni urgenti in materia finanziaria », pubblicato in G.U. n. 302 del 31 dicembre 2007, disponibile in: <http://www.camera.it/parlam/leggi/decreti/07248d.htm> (10 agosto 2008).

litiche comunitarie dell'epoca, ribadendo le proprie perplessità riguardo ad un provvedimento che, a seguito della sua discussa posticipazione, aveva prolungato i termini di conservazione dei dati relativi al traffico telefonico ed alle attività condotte in Rete rispettivamente fino ad un massimo di otto e tre anni, a fronte di una direttiva comunitaria in materia (per ironia della sorte, trattavasi della direttiva 2006/24/CE, nota anche come « Direttiva Frattini », dal nome del suo promotore, l'allora Commissario europeo alla Giustizia, Libertà, e Sicurezza Franco Frattini, ora Ministro degli Esteri nel III Governo Berlusconi) che consentiva tempi di conservazione di dati telefonici ed informatici stabiliti da un minimo di sei mesi ad un massimo di due anni; la lettera invitava inoltre gli organi istituzionali citati ad adoperarsi per conseguire un rapido adeguamento della disciplina italiana alla normativa comunitaria, ribadendo ad ogni modo la perentorietà del 31 dicembre 2008 come termine ultimo per l'obbligo di conservazione dei dati personali degli utenti a carico dei gestori di servizi telematici e informatici<sup>70</sup>.

Anche per la normativa italiana, dunque, sembra essere afflitta dallo stesso dilemma emerso attraverso l'esame del Patriot Act. Come detto, infatti, il provvedimento intende mantenere nettamente separati gli elementi caratterizzanti di una comunicazione (autore, destinatario, tempi di collegamento, etc.) dal suo contenuto. Tuttavia, se una tale divisione si dimostra in qualche misura realizzabile in ambito telefonico, assai meno semplice appare il conseguimento dello stesso risultato nelle comunicazioni informatiche: come illustrato nel paragrafo dedicato alla situazione vigente negli Stati Uniti, in fondo essere a conoscenza di autore, destinatario e modalità di invio di un messaggio on-line o di attività di navigazione in Rete mette in condizione chi sorveglia — o semplicemente consente all'utente lo svolgimento di tale attività — di avere accesso in modo pressoché automatico anche al contenuto della mail o del « tracciato » dell'Internet Surfing. In ultima analisi, dunque, a dispetto di quanto possa essere disposto dalle discipline nazionali in materia, a fronte di una chiara regolamentazione dei casi in cui sia legittimo penetrare nelle telefonate o nelle attività di navigazione della Rete per qualsivoglia finalità autorizzata dalla legge, si ha l'impressione che, non solo nell'ordinamento italiano, l'osservanza di qualunque garanzia finalizzata a tutelare l'inviolabilità delle comunicazioni telefoniche ed informatiche sia lasciata alla buona volontà di chi gestisce il traffico di questi dati.

Le giurisprudenze ordinarie e costituzionali considerate in questa sede mostrano attenzioni e sensibilità diverse a riguardo, scegliendo di conseguenza gli approcci ritenuti più opportuni. Certo è che il tema continuerà a rimanere attuale a lungo, stante la « perdurante incombenza » delle minacce terroristiche (di qualunque matrice esse siano) da un lato, e la capillare diffusione delle telecomunicazioni nella quotidianità contemporanea dall'altro. Non è sempre altrettanto chiaro, di contro, quale possa essere l'orientamento più opportuno per conseguire l'adeguato bilanciamento tra sicurezza collettiva e rispetto delle libertà fondamentali dell'individuo.

<sup>70</sup> Cfr. comunicato stampa del Garante per la protezione dei dati personali, 15 gennaio 2008, disponibile in: [http://](http://www.garanteprivacy.it/garante/doc.jsp?ID=1479338)

[www.garanteprivacy.it/garante/doc.jsp?ID=1479338](http://www.garanteprivacy.it/garante/doc.jsp?ID=1479338) (10 agosto 2008).

Un buon punto di partenza, ad ogni modo, sembra potersi ravvisare — a parere di chi scrive — nell'approdo raggiunto dalla giurisprudenza costituzionale tedesca, quanto meno nella parte in cui questa riconosce, in modo assolutamente esplicito e fermo, la peculiarità della cd. realtà virtuale, ammettendo la necessità di approntare strumenti giuridici e normativi nuovi per regolamentare una « sfera dell'agire comunicativo » ancora inedita, le cui peculiarità tecnologiche finiscono inevitabilmente per trasmettersi sull'immanenza e la fruibilità dei diritti esercitabili in tale contesto. I reiterati interventi dell'organo di garanzia per la riservatezza dei dati personali sembrano, tra l'altro, voler portare all'attenzione dell'opinione pubblica e degli operatori del diritto l'urgenza del riconoscimento di questa particolare condizione: l'auspicio è che entrambe le categorie citate sappiano recepire in fretta tale monito.

Purtoppo, gli eventi di cronaca mostrano di andare nella direzione opposta, dal momento che con il cd. « decreto mille proroghe » emanato alla fine del 2008<sup>71</sup>, è stato tra l'altro deliberato il prolungamento della validità delle citate disposizioni del Decreto Pisanu in materia di sorveglianza delle telecomunicazioni a tutto il 31 dicembre 2009: ancora per quest'anno, quanto meno, niente di nuovo sul fronte digitale.

---

<sup>71</sup> Cfr. art. 11 del D.Lgs n. 207/2008, pubblicato sulla G.U. n. 304 del 31 dicembre 2008, « Proroga di termini previsti da

disposizioni legislative e disposizioni finanziarie urgenti ».