CHIARA FATTA

LA TUTELA DELLA PRIVACY ALLA PROVA DELL'OBBLIGO DI *DATA RETENTION* E DELLE MISURE ANTITERRORISMO

SOMMARIO: 1. La « situazione normativa » della conservazione dei dati: una premessa. — 2. (*segue*) Dalla direttiva 2002/58/CE sulla riservatezza dei dati alla « controriforma » antiterrorismo del cd. « pacchetto Pisanu »: gli artt. 123 e 132 del Codice della *privacy* e le loro successive modifiche. — 3. L'intervento del legislatore comunitario sul profilo specifico della conservazione dei dati per la repressione dei reati: la direttiva 2006/24/CE, la giurisprudenza della Corte Europea dei Diritti dell'Uomo e il Garante europeo. — 4. (*segue*) Le reazioni a livello nazionale.

* Nelle more della pubblicazione delle presenti osservazioni, il Governo ha provveduto, con il D.Lgs. 30 maggio 2008, n. 109, a completare il procedimento di attuazione della direttiva 2006/24 (con il conseguente venir meno della disciplina « sospensiva », contenuta nel decreto legge cd. « milleproroghe » e relativa legge di conversione del febbraio scorso), da cui è derivata una nuova modifica (a pochissimo tempo da quella operata con la ratifica della convenzione sul crimine informatico, in vigore dallo scorso 5 aprile) dell'art. 132 del Codice della *privacy*, con riguardo sia ai tempi di conservazione, sia alla procedura di acquisizione dei dati medesimi nel processo penale.

Con riferimento al primo dei profili summenzionati, resta fermo il periodo di conservazione di 24 mesi per i dati del traffico telefonico, da cui però si escludono quelli relativi alle chiamate senza risposta, per le quali viene introdotto il comma 1-*bis*, che stabilisce un periodo di conservazione obbligatoria di soli trenta giorni e che rappresenta l'unica previsione del nuovo art. 132 non ancora in vigore, prescrivendo il regime transitorio una *vacatio* di ulteriori tre mesi dall'entrata in vigore del decreto legislativo medesimo. Relativamente ai dati del traffico telematico, il termine di conservazione di sei mesi viene prolungato a dodici. In entrambi i casi si specifica che la decorrenza dei predetti termini parte « dalla data della comunicazione » e, novità più rilevante della riforma, viene soppresso il contestato meccanismo del « doppio binario », che consentiva il raddoppio dei termini di conservazione dei dati del traffico, sia telefonico sia telematico, per i reati *ex* art. 407, comma 2, lettera *a*), del codice di procedura penale, nonché di delitti a danno di sistemi informatici e telematici.

Quanto alle modifiche procedurali (comma 4 e 4-*bis*) così come per il trattamento dei dati (comma 5), basti qui ricordare come venga espunto dal disposto dell'art. 132 il riferimento ai casi, ormai abrogati, di conservazione « prolungata » per i delitti più gravi. A prima lettura, può dunque notarsi che se le criticità maggiori della precedente disciplina (« doppio binario » e conservazione dei dati relativi alle chiamate senza risposta) sono state eliminate, resta tuttavia il fatto che il legislatore italiano si è limitato ad una « ripulitura » della disciplina nazionale di tutto l'eccedente le prescrizioni comunitarie, senza un significativo incremento di garanzie per la tutela della vita privata.

1. La « situazione normativa » della conservazione dei dati: una premessa.

La problematica della conservazione dei dati personali è tornata di vibrante attualità a seguito di alcuni interventi legislativi[1], che ne hanno ancora una volta modificato ed integrato la disciplina, andando ad incidere su uno dei profili maggiormente « sensibili », cioè quello dei tempi di conservazione dei dati stessi.

Val la pena di sottolineare preliminarmente come i predetti interventi costituiscano l'ultima tappa dell'allestimento della disciplina (evidentemente ancora incompiuta) della conservazione dei dati esterni delle comunicazioni telefoniche e telematiche, come punto di arrivo di una vicenda normativa, iniziata in sede di attuazione della direttiva comunitaria 2002/58/CE, sulla riservatezza dei dati delle comunicazioni elettroniche, sulla quale si è innestata, quale fonte di ulteriore (e delicata) complicazione, la normativa in materia di contrasto al terrorismo internazionale, a seguito dei noti tragici fatti dell'11 settembre 2001.

Una premessa su tale vicenda ci sembra infatti opportuna prima di prendere in esame le problematiche che il regime giuridico che ne è sfociato ha posto, soprattutto in tema di tutela della *privacy* e dei correlati profili di garanzia costituzionale.

In estrema sintesi, possiamo individuare due « blocchi » di intervento del legislatore in materia:

• Quello vero e proprio di disciplina della conservazione dei dati personali, in attuazione della normativa comunitaria recata dalla già citata direttiva 2002/58/CE, concretizzatasi in particolare nell'art. 132 del Codice della *privacy* e nella immediatamente successiva modifica dello stesso con d.l. 354/2003, convertito in l. 45/2004, e da ultimo con la l. n. 48/2008, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001;

---

[1] Si tratta della previsione, contenuta nel decreto-legge 31 dicembre 2007 248 (cd. « milleproroghe »), convertito dal Parlamento con la Legge 28 febbraio 2008, n. 31, della proroga di un anno della « sospensione dell'applicazione di tutte le disposizioni, di carattere primario, secondario o amministrativo, che prescrivono o consentono la cancellazione dei dati di traffico telefonico o telematico », con particolare riferimento al dettato dell'art. 132 del Codice della *privacy* (D.Lgs. 196/2003). Nello specifico, ai sensi dell'art. 1 della legge di conversione (recante modifiche all'art. 34, comma 1, lett. *a*), del d.l. n. 248/2007) detto termine è stato specificato, nel senso dell'applicazione della predetta disciplina derogatoria « fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008 ».

Il secondo recentissimo intervento sulla disciplina in esame è quello ad opera della l. 48/2008, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001. Si tratta del primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche, con l'obiettivo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata, che consenta di combattere il crimine informatico in maniera coordinata. Per una sintesi dei lavori parlamentari e del contenuto della Convenzione, cfr. D. De Sanctis, *I reati informatici nel D.Lgs. 231/01. Approvato il disegno di legge in Parlamento*, in *Teutas — Law & Technology Journal*, del 26 marzo 2008, all'indirizzo *www.teutas.it*.

• il praticamente contestuale intervento legislativo (ancora una volta « innescato » dal Governo, in via d'urgenza) in materia di contrasto al terrorismo internazionale, di cui al d.l. 144/2005, convertito nella l. n. 155/2005, cui ha fatto appunto seguito, da ultimo, la proroga dei termini previsti dalla predetta legge per la sospensione della disciplina della conservazione dei dati, con il citato d.l. 248/2007, convertito nella l. 31/2008.

In punto specifico di conservazione dei dati personali « ai fini di prevenzione, indagine, accertamento e perseguimento dei reati », resta poi sullo sfondo la nuova direttiva comunitaria 2006/24/CE (cd. « direttiva Frattini »), ancora in attesa di recepimento, pur essendo spirato il relativo termine il 15 settembre 2007.

Si è dunque per questa via pervenuti al vigente regime per la conservazione dei dati di traffico, con soluzioni diversificate in merito ai tempi di conservazione, a seconda che i dati siano relativi al traffico **telefonico** o **telematico**, anche se, in entrambi i casi, il periodo di conservazione massimo ammonta a sei mesi per i dati esterni del traffico da parte del fornitore del servizio, *facoltativamente* e a soli fini civilistici, *ex* art. 123, comma 2, del decreto legislativo 196/2003.

Passando alle ipotesi di conservazione *obbligatoria*, per quanto riguarda il traffico telefonico, i dati devono essere conservati per 24 mesi, per finalità di accertamento e repressione dei reati, ai sensi dell'art. 132, comma 1, del Codice della *privacy*, termine che il successivo comma 2 consente di prolungare a 48 mesi, per esclusive finalità di accertamento e repressione dei reati di cui all'art. 407, comma 2, lettera *a*), c.p.p., nonché dei delitti in danno di sistemi informatici e telematici.

I dati del traffico telematico devono invece essere conservati, per le finalità di accertamento e repressione dei reati, di cui all'art. 132, comma 1, del Codice della *privacy*, per sei mesi, prorogabili a dodici mesi per esclusive finalità di accertamento e repressione dei reati di cui all'art. 407, comma 2, lettera *a*), c.p.p., nonché dei delitti in danno di sistemi informatici e telematici. Un termine di conservazione obbligatorio di tre mesi (prorogabile a sei) è stato previsto dalla legge di ratifica della Convenzione di Budapest, « ai fini dello svolgimento delle investigazioni preventive previste dall'art. 226 delle norme di cui al decreto legislativo 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati »[2].

Sia per i dati di traffico telefonico, sia per quelli di traffico telematico, il d.l. 248/2007, convertito con la l. 31/2008, ha previsto la conservazione obbligatoria fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE e comunque non oltre il 31 dicembre 2008, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore, con la sospensione dell'applicazione dell'art. 132 del Codice della *privacy*.

Attraverso le considerazioni che seguono, si ripercorrerà più nel dettaglio questa evoluzione normativa[3], esaminandola alla luce delle disposi-

[2] Art. 10 della Legge 18 marzo 2008, n. 48, recante Modifiche all'art. 132 del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, che ha aggiunto al disposto dell'art. 132 i commi da 4-*ter* a 4-*quinquies*.

[3] Il seguente schema, proposto da G. MARCOCCIO, *Convention on cybercrime: novità per la conservazione dei dati*, in *Interlex* del 10 aprile 2008, all'indirizzo *http://www.interlex.it/675/marcoccio7.htm*, ci pare una sintesi efficace della descritta si-

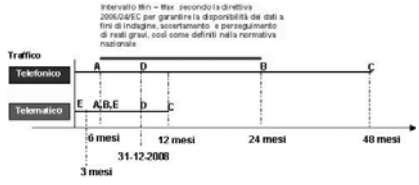
zioni costituzionali e della giurisprudenza costituzionale, nonché delle indicazioni del Garante per la protezione dei dati personali, a livello nazionale e comunitario, con particolare attenzione all'equilibrio che si dovrebbe raggiungere tra le contrapposte (ma entrambe bisognose di tutela) esigenze della *privacy* e della repressione dei reati, per quanto gravi, come il terrorismo.

2. (*segue*). Dalla direttiva 2002/58/CE sulla riservatezza dei dati alla « controriforma » antiterrorismo del cd. « pacchetto pisanu »: gli artt. 123 e 132 del Codice della privacy *e le loro successive modifiche*.

Indicate le coordinate essenziali del percorso, che si intende qui effettuare, non si può ora che « partire dall'inizio », ossia dall'art. 15 della direttiva 2002/58/CE, a cui ha dato attuazione l'art. 132 del Codice della *privacy*, il quale affronta lo spinoso problema del possibile conflitto tra il principio, sancito dall'art. 123 del medesimo Codice, per cui di regola i dati relativi al traffico telefonico devono essere cancellati o comunque resi anonimi al termine della comunicazione, ed il contrapposto interesse pubblico alla sicurezza nazionale, la repressione dei reati in particolare, nell'annosa lotta tra esigenze della *privacy* e della sicurezza, che sembra destinata a non trovare una soluzione[4].

La normativa comunitaria in questione riflette pienamente quello che è l'approccio « normale » del legislatore comunitario alla questione del bilanciamento tra *privacy* e sicurezza, diritto del singolo e interessi pubblici, ossia il rinvio alla discrezionalità dei legislatori nazionali dell'individuazione del punto di equilibrio tra gli interessi in gioco, pur nel rispetto delle garanzie minime, previste dalla CEDU e dalla direttiva stessa[5].

tuazione della *data retention* nella normativa italiana, allo stato attuale.



[4] Si è infatti sottolineato come il problema pur non nuovo, ha acquisito nel tempo sfumature diverse, soprattutto a causa dell'evoluzione tecnologica, che, con particolare riguardo ai cd. « dati esterni » di traffico, ha consentito di passare dalla mera acquisizione di riferimenti temporali e locali all'individuazione di un vero e proprio profilo della persona. Cfr. in proposito G.E. Vigevani, *Articolo 132*, in AA.VV., *Codice della privacy — Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Tomo II, Milano, 2004, 1668.

[5] Si veda, in particolare, il considerando n. 11 della direttiva 2002/58/CE, per cui « la presente direttiva, analogamente alla direttiva 95/46/ CE, non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se ne-

In particolare, il succitato art. 15 prevede la possibilità per gli Stati membri di consentire la conservazione dei dati, per un periodo di tempo limitato e solo nel caso in cui tale deroga alla regola generale della cancellazione[6] costituisca « misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica ».

L'elemento innovativo, di cui la direttiva in esame è portatrice rispetto agli interventi precedenti del legislatore comunitario sul tema[7], è costituito dalla previsione di una esplicita autorizzazione alla *data retention*, che, pur nell'ambito di limiti piuttosto restrittivi in termini di tempo e finalità, non è rimasta esente da critiche già in sede di approvazione della direttiva, dove si lamentava l'arrendevolezza del Parlamento europeo di fronte all'intenzione del Consiglio « di inserire il riferimento, ritenuto tanto pericoloso quanto più generico, alla conservazione obbligatoria dei dati da parte degli operatori telefonici e dei fornitori di accesso ad Internet »[8], nonché il conflitto con la Convenzione Europea dei Diritti dell'Uomo e con la Carta di Nizza.

L'art. 132 del Codice della *privacy*, che recepisce la direttiva 2002/58, nasce pertanto in un clima già acceso dall'appena accennato dibattito sulle norme comunitarie e, per così dire, « a scanso di equivoci », il legislatore delegato comincia con lo stabilire la regola generale della cancellazione (o principio di non conservazione), in ossequio all'allora vigente art. 9 della l. 675/1996, principio che transiterà poi nel disposto dell'art. 123 del Codice stesso e che costituisce, secondo l'interpretazione della dottrina[9] una specificazione della più generale tutela della personalità *ex* art. 2 Cost.

Il principio guida è dunque quello della cd. *data protection* (in contrapposizione alla *data retention*), per cui il soggetto interessato ha diritto a non vedere diffondere all'esterno aspetti della propria vita privata, nella specie i dati relativi alle proprie comunicazioni telefoniche.

---

cessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo », specificando tuttavia come « tali misure [debbano] essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali ».

[6] Il riferimento va, in particolare agli artt. 5, 6, 8, paragrafi 1, 2, 3, e 4 e 9, relativi rispettivamente alla riservatezza delle comunicazioni, all'obbligo di cancellazione dei dati relativi al traffico quando non sono più necessari ai fini della trasmissione di una comunicazione, alla possibilità, che il fornitore di servizi deve offrire all'utente chiamante, di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata e linea per linea, e ai limiti al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, in particolare il consenso dell'interessato.

[7] Ci si riferisce all'art. 14 della Direttiva 97/66/CE e all'art. 13 della Direttiva 95/46/CE, di cui l'art. 15 della Direttiva 2002/58/CE è in gran parte riproduttivo, con riferimento ai limiti previsti per la deroga.

[8] Puntualizza la questione, G.E. VIGEVANI, *Articolo 132*, cit., 1675, con riferimento alla Dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) e ai lavori del Gruppo di lavoro per la protezione dei dati personali, istituito dall'art. 29 della Direttiva 95/46/CE.

[9] Cfr. G.E. VIGEVANI, *Articolo 132*, cit., 1681.

Nella sua versione originaria, che sarà destinata a vivere soltanto sulla carta, l'art. 132 faceva salvo il disposto (mai mutato) dell'art. 123, comma 2, che prevede la mera facoltà in capo al fornitore di conservare i dati, per sei mesi e per soli fini civilistici (fatturazione), mentre imponeva un obbligo di conservazione di trenta mesi per i soli dati di traffico telefonico, ai fini della repressione dei reati.

Come già si accennava, tuttavia, il legislatore si è immediatamente trovato nella necessità di riformare la predetta disciplina, a causa di diverse criticità, prima fra tutte l'esclusione dei dati relativi al traffico telematico, nonché la riduzione eccessiva del periodo di conservazione, rispetto a quello quinquennale della disciplina previgente, *ex* art. 4 del D.Lgs. 171/1998.

Pertanto, ancora prima che il Codice della *privacy* entri in vigore (il 1º gennaio 2004), con il d.l. 354/2003, la disposizione viene modificata nel senso della dilatazione dei tempi di conservazione dei dati di traffico e dell'imposizione dell'obbligo di conservazione anche ai gestori dei servizi di comunicazione elettronica.

Fatto sempre salvo il comma 2 dell'art. 123, infatti, l'obbligo di conservazione ai fini della repressione dei reati viene confermato a trenta mesi, rinnovabili, però, nel caso si tratti di reati *ex* art. 407, comma 2, lettera *a*), del codice di procedura penale, nonché di delitti a danno di sistemi informatici e telematici. In questo modo, viene adottata una disciplina « a doppio binario », che, seppur solo nel caso dei delitti più gravi (e si noti come questa volta, siano ricompresi tra questi i reati telematici, prima neppure considerati), riporta il periodo di conservazione a cinque anni.

Neppure tale novellata versione dell'art. 132 rimane però esente da riprensioni, non mancando chi ritenga eccessivo l'obbligo quinquennale di conservazione, soprattutto in rapporto ai costi eccessivi che ne derivano, senza contare le problematiche procedurali, connesse alle modalità di acquisizione dei dati[10].

---

[10] In proposito, la dottrina, se da un lato si è mostrata favorevole all'apertura ai dati del traffico telematico, dall'altro l'ha giudicata eccessiva, per i costi e la difficoltà di conservare per così lungo tempo una mole tanto consistente di dati, nonché per la difficoltà di individuare, nel complesso e peculiare universo telematico, quali fossero effettivamente i dati interessati dall'obbligo di conservazione. Cfr. L. DI PAOLA, *Art. 132*, in C.M. BIANCA-F.D. BUSNELLI (a cura di) *La protezione dei dati personali: commentario al D.Lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, 2007, 1594, che riporta le posizioni di G. BUSIA, *Così la riservatezza « guadagna » terreno*, in *Guida al dir.*, 2004, 58; F. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito di, tabulati, tracciamenti, intercettazioni, conservazione dei dati e dintorni)*, in *Cass. Pen.*, 2002, 2220; G. CAPOCCIA, *Tabulati telefonici: tanti dubbi sulla nuova normativa*, in *Cass. Pen.*, 2005, 291. Si vedano anche F. VEUTRO, *La conservazione dei dati relativi al traffico: una lettura diversa*, in *Interlex* del 12 febbraio 2004, all'indirizzo *www.interlex.it* e A. MONTI, *Dati del traffico: chi-conserva-cosa?*, in *Interlex* dell'8 gennaio 2004, all'indirizzo *www.interlex.it*.

In particolare, G.E. VIGEVANI, *Articolo 132*, cit., 1688, condivide l'estensione dell'obbligo di conservazione al traffico telematico, in ossequio al principio della « neutralità rispetto al mezzo » (di comunicazione), rilevando tuttavia i problemi di natura tecnica e quelli di tipo sostanziale, legati ai rischi di violazione dei diritti fondamentali, la libertà e segretezza di comunicazione *in primis*, puntualizzando come, nella comunicazione elettronica, sia più labile il confine tra dati esterni di traffico e contenuti. Nello stesso senso, S. VIGLIAR, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in questa *Rivista* 2003, 401 ss e V. GREVI, *Ma quei tabulati sono indispensabili*

A fronte dei predetti rilievi, la legge di conversione 45/2004, pur confermando l'obbligo di *data retention*, cerca di trovare un punto di equilibrio degli interessi in conflitto con l'introduzione di alcune novità significative.

Intanto, dopo aver fatto ancora salvo il disposto dell'art. 123, comma 2 (relativo, si ricorda, al profilo facoltativo e civilistico della conservazione dei dati), il nuovo art. 132 prevede la possibilità, per il fornitore di servizi, di conservare i dati relativi al traffico telefonico per 24 mesi, « per finalità di accertamento e repressione dei reati », periodo di tempo rinnovabile « per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, comma 2, lettera *a*), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici e telematici ».

Si nota dunque come torni il riferimento ai soli dati del traffico telefonico, mentre rimanga immutato quello ai reati telematici per il termine lungo di conservazione (cinque anni).

Dal lato processuale, si assiste poi ad una modifica significativa della procedura di acquisizione dei dati, in particolare con la previsione di maggiori restrizioni in capo all'imputato e alle parti private, nonché di previsioni poco chiare in ordine a chi competa in concreto l'acquisizione, a come procedere in caso di urgenza, in un quadro complessivo di appesantimento procedurale[11].

Anche se nel prosieguo ci sarà modo di riprendere tali problematiche, giova qui ricordare come i termini di conservazione da ultimo previsti siano stati immediatamente tacciati di incostituzionalità, determinando la rimessione alla Corte costituzionale di diverse questioni[12], attinenti so-

---

per le istruttorie, in *Il Corriere della sera* del 24 dicembre 2003, 16.

Particolarmente critici nei confronti della dilatazione dei tempi di conservazione e dell'utilizzo (improprio) della decretazione d'urgenza per la disciplina della materia, sono A. Lisi-M. De Giorgi, Tra *Data retention e Gattopardo*, in *Punto Informatico* del 14 gennaio 2004, all'indirizzo *www.punto-informatico.it*; G. Buttarelli, *Riservatezza ad alto rischio*, in *Il Sole 24 Ore* del 30 dicembre 2003.

Più nel dettaglio, sui problemi processualpenalistici, cfr. G. Fruganti, *Prime riflessioni sui profili applicativi della disciplina sull'acquisizione dei tabulati del traffico telefonico*, in *Arch. Nuova Proc. Pen.*, 2004, 367 ss.

[11] Le criticità procedurali vengono sottolineate da G. Capoccia, *Tabulati telefonici*, cit., 296 ss, che disapprova lo « sbilanciamento che si è realizzato in favore del difensore dell'imputato a detrimento del pubblico ministero e delle altre parti private », pur ritenendo, alla luce della giurisprudenza costituzionale, che la disciplina contenuta nella legge di conversione 45/2004 sia costituzionalmente legittima, in quanto frutto dell'esercizio ragionevole da parte del legislatore del suo potere discrezionale; M. De Bellis, *Brevi note sulla nuova disciplina dell'acquisizione dei tabulati telefonici*, *Cass. Pen.*, 2004, 1148 ss. e G.E. Vigevani, *Articolo 132*, cit., 1692, quest'ultimo maggiormente scettico sulla legittimità costituzionale del predetto intervento legislativo, che continuerebbe per di più a lasciare « una sensazione di provvisorietà » della disciplina della conservazione dei dati, sicuramente perfettibile.

[12] Cfr., in particolare, Trib. Roma, 23 dicembre 2004, in *Gazz. Uff.*, I Serie speciale, n. 9 del 2 marzo 2005, 53, che ha sollevato questione di legittimità costituzionale dell'art. 132 del Codice Privacy nella parte in cui esclude, decorso il termine di 24 mesi, l'acquisibilità e l'utilizzabilità dei dati di traffico telefonico per finalità di repressione dei reati diversi da quelli di cui all'art. 407, comma 2, lett. *a*), del c.p.p., per violazione degli artt. 2, 3, 13, 14, 24, 32, 42, 101, 104, 111, 112 Cost.

Più approfonditamente sul punto, si veda L. Di Paola, *Art. 132*, in C.M. Bianca-F.D. Busnelli (a cura di) *La protezione dei dati personali*, cit., 1587 ss.

Per la decisione della Corte, cfr. la sentenza 14 novembre 2006, n. 372, in *Giur. Cost.*, 2006, 3916, a commento della quale

prattutto al divario temporale 24-48 mesi, ritenendo il termine breve per i reati minori insufficiente, sia per i poteri acquisitivi del giudice, sia per le garanzie di difesa dell'imputato, che non vedrebbe neppure tutelata la propria riservatezza, essendo il fornitore obbligato a conservare comunque i dati per ulteriori 24 mesi, ma soltanto ai fini repressivi dei reati più gravi. Paradossalmente, avrebbe maggiore « spazio di manovra » l'imputato di reati più gravi, potendo accedere ai propri dati per 48 mesi, rispetto all'imputato di reati minori, con una evidente ed irragionevole disparità di trattamento.

È a questo punto, in un quadro normativo quanto mai incerto, che si innesta quello che si è qui chiamato « secondo blocco normativo », la riforma antiterrorismo del cd. « pacchetto Pisanu », di cui al d.l. 144/2005, convertito nella l. 155 dello stesso anno, che stravolge il predetto assetto, sotto un duplice profilo.

Da un lato, viene modificato nuovamente l'art. 132 con la previsione del « doppio binario » di conservazione, negli stessi termini (24-48 mesi), di cui alla l. 45/2004, pur con il riferimento ai dati del traffico, sia telefonico sia telematico, e con il recupero della meno gravosa procedura di acquisizione, di cui al d.l. 354/2003, e l'introduzione dell'auspicata procedura di urgenza.

Dall'altro lato, *ex* art. 6 del d.l. 144/2005, si prevede una sospensione generale dell'applicazione dell'art. 132 fino al 31 dicembre 2007, per l'esclusiva repressione dei reati di terrorismo, con il conseguente obbligo di conservazione di tutti dati esterni alle comunicazioni, anche se non soggetti a fatturazione.

La deroga alle limitazioni previste dal Codice della *privacy*, quale misura antiterrorismo coinvolge dunque anche i dati concernenti le cd. « chiamate senza risposta », nonché i dati relativi al traffico telematico, attraverso l'istituzione di una vera e propria disciplina autonoma, che ha destato comunque non poche perplessità, soprattutto (ancora una volta) in relazione ai profili procedurali di acquisizione[13].

Da ultimo, l'art 132 del Codice *Privacy* è stato nuovamente modificato da parte della legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, il cui art. 10, comma 1, inserisce, dopo il comma 4-*bis* dell'art. 132, i commi da 4-*ter* a 4-*quinquies*.

Le nuove disposizioni prevedono un nuovo ed ulteriore termine di conservazione dei dati di traffico, da tre a sei mesi, ai fini dello svolgimento delle indagini preventive di cui all'art. 226 del D.Lgs. 271/1989 (attuazione al Codice di Procedura penale) ovvero per finalità di accertamento e repressione di specifici reati. Si tratta, in particolare dell'introduzione del

si segnalano E. Bassoli, *Acquisizione dei tabulati Vs.* Privacy*: la* data retention *al vaglio della Consulta*, in *Dir. internet*, 3/2007, 240 ss e M. Pinna, « *Doppio binario* » *di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giur. Cost.*, 2006, 3929 ss. Quest'ultimo si sofferma criticamente sulla questione del divario temporale 24-48 mesi, che, secondo il giudice rimettente, rappresentava un pericolo per la riservatezza e che risulta invece pienamente inserito in un ragionevole bilanciamento dei valori, secondo la Corte.

[13] Per un approfondimento sul punto, v. G. Capoccia, *Tabulati telefonici*, cit., 298 ss.

cd. « congelamento dei dati per ragioni urgenti », con notevole incremento dei poteri delle forze di polizia e dei servizi segreti, seppur apparentemente limitato « a casi eccezionali ed urgenti », come appunto le indagini e le intercettazioni preventive sopra citate[14].

Tuttavia, almeno secondo i primi commentatori dell'intervento di ratifica, le cautele adoperate dal legislatore non paiono sufficienti, soprattutto in riferimento alla formula imprecisa, introdotta nell'art. 132 dal nuovo comma 4-*ter* e relativa all'« accertamento e repressione di specifici reati », che concretizza una « valvola di apertura » che appare irragionevole, in quanto contenuta in una norma di carattere eccezionale e suscettibile di ampliare (più che risolvere) le perplessità che già circondano la disciplina della *data retention*, in relazione alla quale sarebbe addirittura in corso una « schizofrenia interpretativa e normativa »[15].

Ciò che stupisce, in particolare, è come la disposizione sia passata indenne sia all'esame parlamentare (del Senato, in particolare, che era parso più attento al profilo della tutela della *privacy*) sia, e soprattutto, alle censure del Garante, che, come poco oltre si vedrà, ha condotto una strenua battaglia, affinché il legislatore provvedesse ad arginare i rischi per la tutela della vita privata, legati all'obbligo di conservazione dei dati[16].

---

[14] A prima lettura, si veda il commento alle nuove disposizioni di M. Cuniberti, G.B. Gallus, F.P. Micozzi e S. Aterno, all'indirizzo *http://www.giuristitelematici.it*, che sottolineano appunto come non vi sia certezza sull'eccezionalità dell'applicazione delle nuove disposizioni.

[15] Cfr. *ibidem*, dove si puntualizza che « l'apertura, appunto, ad ipotesi di reato non espressamente indicate significa poter applicare di fatto il comma 4-*ter* anche a reati diversi da quelli di cui alla convenzione sul cybercrime, diversi da quelli previsti dal 132 codice privacy e appunto specifici in quanto specificati a posteriori. Ciò non è proprio tranquillizzante sotto il profilo della chiarezza e della precisione normativa se si considera la portata internazionale della norma stessa in relazione ai rapporti che essa prevede con le autorità investigative straniere. La circostanza che non si tratta di una norma che stabilisce il potere di « acquisizione » fuori dai termini del primo comma dell'art. 132 bensì un potere meramente di « conservazione e protezione del dato » e tra l'altro con breve scadenza (sei mesi massimo), la circostanza che tutto ciò avviene vincolando al segreto assoluto (e punito) il gestore e con la massima indisponibilità del dato da parte dello stesso, la circostanza che i provvedimenti adottati ai sensi del comma 4-*ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida e in caso di mancata convalida, i provvedimenti assunti perdono efficacia, non è sufficiente per lasciare questa norma esente da dubbi e da critiche. Come non è sufficiente la circostanza che siamo in ambito di conservazione dei soli dati relativi al traffico telematico escluso il contenuto delle comunicazioni ».

[16] Così, *ibidem*. In particolare, « non è passata in aula parlamentare la modifica suggerita con una certa insistenza e riguardante la necessità di affidare la convalida del provvedimento di cui al comma 4-*ter* al giudice del luogo dell'esecuzione anziché al pubblico ministero. Trattandosi del luogo di esecuzione del congelamento dei dati ovvero del luogo dove i dati sono conservati dal gestore, e considerato che SE trattasi di indagini (intercettazioni) preventive *ex* art. 226 norme coord. è evidente non vi è alcun procedimento penale e quindi nessun PM competente in virtù di un'indagine assegnata, la convalida del provvedimento affidata comunque al pubblico ministero del luogo fa sorgere il legittimo dubbio di un facile e spesso ricorrente « involontario appiattimento » del PM a tutte le richieste delle forze di polizia di cui al comma 4 ter. Indubbiamente meglio sarebbe stato, viste anche le sopra richiamate (e se vogliamo più preoccupanti) richieste avanzate dalle autorità investigative straniere, l'intervento di un giudice per le indagini preliminari ».

3. L'intervento del legislatore comunitario sul profilo specifico della conservazione dei dati per la repressione dei reati: la Direttiva 2006/24/CE, la giurisprudenza della Corte Europea dei Diritti dell'Uomo e il Garante europeo.

Esclusivamente per « i dati generati o trattati come conseguenza di una comunicazione o di un servizio di comunicazione e non [...] i dati che costituiscono il contenuto dell'informazione comunicata »[17], il Parlamento ed il Consiglio europei decidono di disciplinare la cd. *data retention*, al fine di armonizzare le legislazioni nazionali, « considerevolmente differenti »[18], intervenute a limitare gli obblighi *ex* direttiva 2002/58/CE, ai sensi dell'art. 15, paragrafo 1, della direttiva medesima.

Viene adottata su queste basi la direttiva 2006/24/CE (cd. « direttiva Frattini »)[19], che ha dato vita a quella che è stata definita dalla stampa di settore « una delle più contestate normative sull'intercettazione delle comunicazioni [...] che consente ai singoli paesi di conservare i dati delle comunicazioni per un massimo di due anni »[20], che vieta la conservazione dei contenuti delle comunicazioni, ma che consente comunque ai singoli paesi di estendere la *data retention* per un indefinito « periodo limitato »[21].

Tali dubbi sono pienamente comprensibili, sol che si pensi a quanto previsto dalla vigente disciplina comunitaria, in materia di tutela dei dati personali, nonché alla « giurisprudenza » del Garante, con le quali la nuova normativa europea si pone in aperto contrasto, limitando formalmente a due anni l'obbligo di *data retention*, ma consentendo di fatto ai Paesi membri l'estensione discrezionale (per non dire arbitraria) di tale termine.

Proprio in punto di armonizzazione delle discipline nazionali degli Stati membri, in materia di protezione dei dati nell'ambito del terzo pilastro, il Garante europeo della protezione dei dati è intervenuto con tre fondamentali pareri[22] su un progetto di decisione quadro della Commissione,

---

[17] Ai sensi del Considerando n. 12 della Direttiva 2006/24/CE, « l'articolo 15, paragrafo 1, della direttiva 2002/58/CE continua ad applicarsi ai dati, compresi quelli connessi ai tentativi di chiamata non riusciti, di cui non è specificamente richiesta la conservazione a norma della presente direttiva e che pertanto non rientrano nel campo di applicazione della stessa, e alla conservazione dei dati per scopi, anche giudiziari, diversi da quelli contemplati dalla presente direttiva ».

[18] Parafrasando il considerando n. 5 in particolare, il successivo considerando n. 6 rileva che « le differenze giuridiche e tecniche fra le disposizioni nazionali relative alla conservazione dei dati ai fini di prevenzione, indagine, accertamento e perseguimento dei reati costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche, giacché i fornitori dei servizi devono rispettare esigenze diverse per quanto riguarda i tipi di dati relativi al traffico e i tipi di dati relativi all'ubicazione da conservare e le condizioni e la durata di tale conservazione ».

[19] Per un dettaglio sui contenuti della direttiva, cfr. S. Monteleone, *La tutela dei dati personali nelle comunicazioni elettroniche tra esigenze di* Data Protection *e obblighi di* Data Retention, in P. Costanzo, G. De Minico, R. Zaccaria (a cura di), *I « tre codici » della Società dell'informazione*, Torino, 2006.

[20] Cfr. l'articolo riportato su *Punto Informatico*, n. 2443 del 15 dicembre 2005, all'indirizzo *www.punto-informatico.it*, dal titolo *UE, via libera all'intercettazione di massa*.

[21] Articolo 12, paragrafo 1.

[22] Si tratta dei pareri del 19 dicembre 2005, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea C 47 del 25 febbraio 2006, del 29 novembre 2006, pubblicato

in cui si è evidenziata l'opportunità di adottare misure, seppur restrittive della riservatezza, al fine di repressione dei reati (del terrorismo in particolare) e la necessità di una disciplina uniforme in materia.

Tuttavia, secondo il Garante, la prima cautela in tale operazione deve essere quella della tutela dei diritti, in relazione alla quale, anzi, il Consiglio « deve comprendere che una protezione dei dati efficace va di pari passo con un'azione efficace dei servizi repressivi e giudiziari », come a dire che proprio l'accordo sul livello (alto) di tutela dei diritti è la chiave per il perseguimento di un altrettanto alto livello di cooperazione nel terzo pilastro. In particolare, il legislatore comunitario deve aver riguardo degli obblighi che gli derivano dalla legislazione comunitaria (direttiva 95/46/CE), dall'art. 8 della CEDU, nonché dalla Convenzione del Consiglio d'Europa n. 108, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981.

Cionondimeno le indicazioni del Garante non sembrano ottenere il risultato sperato, rilevandosi, in occasione dell'ultimo dei tre citati pareri, la « tendenza ad andare verso il minimo comune denominatore »[23] e non verso quell'ampio accordo/consenso di cui si diceva, fattore che spinge il Garante ad esprimere parere negativo sulla nuova proposta di decisione sulla protezione dei dati nell'ambito del terzo pilastro.

Anche un altro organismo comunitario preposto, più nello specifico, alla tutela dei dati personali, il Gruppo di Lavoro « Articolo 29 »[24], ha sempre vigilato sulle garanzie della vita privata, stabilite dall'ordinamento comunitario (direttiva 95/46/CE) e dalla CEDU, attraverso l'adozione di raccomandazioni e pareri, spesso in aperto dissenso con le istituzioni comunitarie che, di fronte all'alternativa « più sicurezza e meno *privacy*, oppure viceversa »[25], a seguito dell'emergenza terrorismo *post* 11 settembre 2001, sono apparse evidentemente orientate verso la prima.

Già nel 1997, infatti, in relazione all'anonimato su internet, il Gruppo di Lavoro osservava che « il diritto alla riservatezza (articolo 8, della Convenzione europea dei diritti dell'uomo analogamente inserito nel diritto comunitario) è altrettanto importante quando si tratta di valutare la politica da adottare nei confronti di Internet [...] una delle maggiori minacce [al quale] è la capacità delle organizzazioni di accumulare un gran numero di informazioni sulle persone, in forma digitale, la quale si presta alla manipolazione, alterazione e comunicazione a terzi ad alta velocità »[26].

---

sulla Gazzetta Ufficiale dell'Unione Europea C 91/9 del 26 aprile 2007, e del 27 aprile 2007, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea C 139/1 del 23 giugno 2007, tutti reperibili sul sito ufficiale del garante, all'indirizzo *http://www.edps.europa.eu/EDPSWEB/edps/lang/ it/pid/1*.

[23] Cfr. il parere del Garante europeo del 27 aprile 2007, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea C 139/1 del 23 giugno 2007.

[24] Della Direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente sulla protezione dei dati e della vita privata. Le sue funzioni sono definite dall'art. 30 della Direttiva 95/46/CE e dall'art. 15 della Direttiva 2002/58/CE.

[25] Cfr. in proposito T. LOMBARDI, *Privacy e terrorismo, nuove parole al vento*, in *Punto Informatico*, n. 2613 del 21 settembre 2006, all'indirizzo *www.punto-informatico.it*.

[26] Cfr. la raccomandazione n. 3/97 del 3 dicembre 1997, *Anonimato su internet*, reperibile all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm*.

Tali rischi hanno indotto il legislatore comunitario ad adottare una disciplina *ad hoc*, in materia di protezione dei dati, la direttiva 95/46/CE appunto, secondo un *trend* per cui « i dati personali raccolti in qualsiasi situazione debbano limitarsi a quanto è strettamente necessario e attinente alla finalità in questione »[27], dato che qualsiasi informazione personale costituisce una potenziale minaccia alla riservatezza e deve pertanto essere conservata soltanto per finalità determinate e per il minor tempo possibile.

A seguito dell'adozione della direttiva, numerosi sono gli interventi del Gruppo di Lavoro, in relazione a problematiche specifiche, soprattutto attinenti alle comunicazioni elettroniche, in cui si pongono in evidenza le esigenze della vita privata avverso le intrusioni esterne, rinvenendo nell'art. 8 della CEDU, ed in particolare nei tre criteri fondamentali in esso stabiliti[28], il parametro per valutare la legittimità di tali ingerenze[29].

La conservazione dei dati di traffico, in particolare, viene tollerata soltanto per il tempo strettamente necessario alla fatturazione, risultando altrimenti « un'ingerenza nell'esercizio dei diritti fondamentali garantiti agli individui dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo »[30]. Per la legittimità della conservazione dei dati, inoltre, ci « deve essere una necessità dimostrabile, il periodo di conservazione deve essere il più breve possibile e la pratica deve essere chiaramente disciplinata dalla legge »[31].

Il sorgere dell'emergenza terroristica ha sollecitato, come si osservava sopra, l'intervento degli Stati membri all'adozione di normative in deroga alla generale disciplina di garanzia della *privacy*, nazionale e comunitaria, in ossequio a quel principio del « più sicurezza e meno *privacy* », che sembrava avere la meglio su quello opposto, che predilige la tutela della sfera privata.

In relazione a tali interventi, entra nuovamente in gioco il Gruppo di Lavoro, con un parere in merito alla necessità di un approccio equilibrato

---

[27] Cfr. la raccomandazione n. 3/97, cit.

[28] Si tratta di: una base giuridica, la necessità della misura in una società democratica e la conformità ad uno degli obiettivi legittimi enumerati nella convenzione, come integrati dalla giurisprudenza della Corte europea dei Diritti dell'Uomo e dalla Convenzione di Strasburgo n. 108 del 1981, in cui si prevede anche che un'ingerenza è tollerata unicamente se si tratta di una misura necessaria in una società democratica alla tutela degli interessi nazionali enumerati al suo art. 9, paragrafo 2 (si osservi che gli interessi nazionali enumerati nella convenzione 108 e nella convenzione per la tutela dei diritti dell'uomo non sono esattamente gli stessi), e se essa si limita unicamente al perseguimento di questo obiettivo.

[29] Si veda, in particolare, la Raccomandazione n. 2/99, adottata il 3 maggio 1999, in materia di intercettazioni, in cui il Gruppo di lavoro ha enumerato una lista di condizioni che la normativa nazionale deve soddisfare, per non incorrere nella violazione dell'art. 8 CEDU: « partendo dal principio che i dati relativi al traffico concernente gli abbonati e utilizzatori devono essere cancellati o resi anonimi subito dopo la fine della comunicazione, ne segue che gli scopi per cui i dati possono essere trattati, la durata della loro eventuale conservazione nonché l'accesso a tali dati sono rigorosamente limitati » (cfr. il paragrafo 9). Il documento è reperibile all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm*.

[30] Cfr. il parere n. 4/2001 del 22 marzo 2001, in relazione al progetto di convenzione sulla cibercriminalità del Consiglio d'Europa, reperibile all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm*.

[31] Il Gruppo di Lavoro richiama, in particolare, i lavori della Conferenza di Stoccolma del 2000 dei Garanti europei dei dati personali.

alla lotta contro il terrorismo, adottato il 14 dicembre 2001, in cui ha l'occasione di specificare come, pur essendo prezioso l'impegno delle società democratiche nella lotta al terrorismo, « in questa lotta, devono essere rispettate certe condizioni, che costituiscono anch'esse parte integrante della base della nostra società democratica », in particolare « assicurare il rispetto dei diritti fondamentali e della libertà dell'individuo », di cui quello alla protezione dei dati personali costituisce parte integrante[32].

Più marcatamente, in occasione della Conferenza di Cardiff del 9-11 settembre 2002[33], sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni, i Commissari europei per la protezione dei dati manifestano seri dubbi in ordine alla legittimità e legalità di misure che impongano l'« obbligo sistematico » di conservare i dati di traffico delle telecomunicazioni, per un periodo uguale o maggiore di un anno[34], ritenendo configurabile la violazione del già più volte citato art. 8 CEDU.

Sebbene l'adozione di normative nazionali, che prevedano la conservazione dei dati di traffico, sia infatti autorizzata dal disposto dell'art. 15 della Direttiva 2002/58/CE, esso pone, tuttavia, delle condizioni specifiche[35] a tale misura: un'archiviazione sistematica risulta pertanto « chiaramente sproporzionata e quindi inaccettabile comunque ».

Gli interventi più incisivi si concentrano poi nei pareri n. 1/2003, in punto specifico di conservazione dei dati di traffico ai fini di fatturazione, e n. 9/2004, sulla proposta di decisione quadro sulla conservazione dei dati di traffico al fine di repressione dei reati, ivi compreso il terrorismo.

In merito alla fatturazione, si puntualizza come il periodo massimo tollerabile di conservazione siano i sei mesi, fermo restando l'obbligo di cancellazione per i dati che non siano strettamente necessari allo scopo, nonché le eccezioni, consentite dal più volte citato art. 15 della Direttiva 2002/58/CE, le cui condizioni devono però essere scrupolosamente rispettate, per non incorrere in un'inammissibile violazione del diritto comunitario in materia di protezione dei dati personali.

Più in generale, sulla problematica questione della conservazione dei dati, ai fini di repressione dei reati, il Gruppo di Lavoro ripercorre tutta la sua « giurisprudenza », chiamando a conforto delle sue argomentazioni la consolidata giurisprudenza della Corte europea dei Diritti dell'Uomo, in ordine all'interpretazione dell'art. 8 della CEDU ed in particolare dei tre criteri stabiliti nello stesso.

---

[32] Cfr. il parere n. 10/2001 del 14 dicembre 2001, *sulla necessità di un approccio equilibrato alla lotta contro il terrorismo*, reperibile all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm*.

[33] V.la come riportata dal parere 5/2002, *Sulla dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni*, reperibile all'indirizzo *http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm*.

[34] Nello specifico si tratta di « proposte che comporterebbero l'obbligo sistematico di mantenimento dei dati di traffico concernenti tutti i tipi di telecomunicazioni (ossia luogo, data, e numeri utilizzati per comunicazioni telefoniche, fax, posta elettronica, e altri usi di Internet) per un periodo di un anno o anche oltre, allo scopo di consentire la possibilità di accesso a tali dati da parte delle autorità di polizia e di sicurezza ».

[35] In particolare, « per un periodo limitato e qualora strettamente necessario, opportuno e proporzionato nell'ambito di una società democratica ».

La Corte è intervenuta, in particolare e già in epoca piuttosto risalente, a specificare il contenuto del secondo criterio della necessità della misura adottata in una società democratica, stabilendo che l'ingerenza nella vita privata deve rispondere ad un « pressante bisogno sociale », da soddisfare comunque a specifiche condizioni[36].

In particolare, a prescindere dalle limitazioni di oggetto (quali dati) e di tempo (periodo massimo di conservazione), ciò che emerge dai citati interventi del Gruppo e dalla giurisprudenza della Corte è che il problema fondamentale, attinente alla conservazione dei dati di traffico, è l'automatismo generalizzato di tale operazione, il conservare « tutto di tutti », anche di coloro che non sono imputabili di alcunché.

I legislatori nazionali, nel disciplinare il trattamento dei dati di traffico, hanno « l'obbligo di rispettare i principi di legalità, lealtà e finalità e proporzionalità in rapporto ad eventuali provvedimenti restrittivi », risultando necessaria (ancora parafrasando l'art 8 CEDU) non la semplice utilità della misura adottata, ma la sua « necessità sociale imperativa »[37].

Risulta pertanto necessario bilanciare l'esigenza di repressione dei reati con la tutela della riservatezza, nel rispetto di quelle condizioni, che si enumeravano sopra, derivanti dalla normativa comunitaria, dalla CEDU e dalle indicazioni della Corte europea dei Diritti dell'Uomo e del Garante, che inspiegabilmente nella direttiva 2006/24/CE non sembrano trovare adeguato riscontro, soprattutto con riguardo ai tempi previsti e a quella possibilità di proroga « limitata » (ma di fatto *ad libitum*?) prevista all'art. 12 del termine biennale già (troppo) ampio, consentito dal precedente art. 6.

4. (*segue*). Le reazioni a livello nazionale.

Se a livello sovranazionale la disciplina della conservazione dei dati, ai fini del perseguimento dei reati, suscita i dubbi appena considerati, le cose non sono andate meglio a livello dei singoli ordinamenti statali, dove la reazione delle Autorità garanti, delle Corti costituzionali e dei cittadini stessi si è mantenuta sulla linea della contrapposizione all'ingerenza dell'autorità di pubblica sicurezza nella vita privata, non importa se giustificata dalla lotta al terrorismo: da un lato, si sono contestate le discipline nazionali in materia di *data retention*, dall'altro si è censurata quella disciplina comunitaria, che avrebbe dovuto armonizzare e, nel contempo, porre

---

[36] Si tratta del paradigmatico caso *Klass contro la Repubblica Federale Tedesca*, Corte europea dei Diritti dell'Uomo, 6 settembre 1978, serie A n. 28, di cui rileva in particolare il passo in cui afferma che « ... les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voir de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelles mesures jugées par eux appropriées ». A questo, in relazione alla conservazione dei dati di traffico, si aggiungono i casi *Amann c. Svizzera*, n. 27798/95, *Rotaru c. Roumanie [GC]*, 4 maggio 2000, n. 28341/95, *P.G. et/and J.H. c.Regno Unito*, 25 settembre 2001, n. 44787/98, *Malone c. Regno Unito*, 2 agosto 1984, Serie A, n. 82; *M.M c. Paesi Bassi*, 8 aprile 2003, n. 39339/, da cui si ricava l'applicabilità dei criteri *ex* art. 8 CEDU anche a questo settore specifico.

[37] Cfr. in proposito G.E. Vigevani, *Articolo 132*, cit., 1678.

rimedio alle criticità degli interventi dei legislatori nazionali, soprattutto laddove un diritto fondamentale dell'individuo veniva posto in pericolo.

I casi più eclatanti in proposito si sono verificati in Irlanda ed in Germania, dove l'associazionismo impegnato sul fronte dei diritti civili, da un lato, e il Tribunale costituzionale, dall'altro, si sono contrapposti apertamente alla normativa nazionale sulla *data retention* e, soprattutto, all'intervento del legislatore comunitario in favore di tale misura.

Partendo dal Tribunale costituzionale tedesco, esso ha operato un intervento deciso avverso la *data retention*, in riferimento al profilo specifico delle investigazioni sistematiche sulle reti di *sharing* da parte delle *major*, che ha comunque costituito lo spunto per una riflessione più approfondita, in materia di diritti fondamentali.

L'impulso è stato una *class action*, intentata da utenti, esponenti politici e associazioni culturali, che ha portato alla dichiarazione dell'illegittimità costituzionale[38] di tale operazione, non essendo ammissibile una violazione incondizionata di massa della *privacy* degli utenti, senza il loro consenso preventivo.

Il Tribunale ha quindi stabilito i precisi confini entro cui la *data retention* può muoversi: in relazione all'ipotesi specifica del diritto d'autore, soltanto per richiesta delle forze di polizia e solo per casi determinati, quali la garanzia di sicurezza del paese, la repressione di minacce di sovvertimento dell'ordine e democratico e del terrorismo; in relazione agli altri ambiti della *data retention*, i dati delle comunicazioni possono essere ottenuti dalle forze di polizia solo ed esclusivamente per la repressione di reati gravi, nel caso in cui l'informazione sia assolutamente necessaria e non possa essere ottenuta in altro modo[39].

Ma la Corte è andata ben oltre la dichiarazione di illegittimità della previsione, contenuta in una legge del *land* Nord Reno-Westfalia, ampliando le proprie riflessioni alla dignità della persona e alla tutela dei suoi diritti fondamentali, inevitabilmente (ed intollerabilmente) compromessi da una conservazione indiscriminata dei dati personali, nella specie di traffico telefonico e telematico. Come si legge nella sentenza e come sottolineano i primi commenti alla stessa[40], il problema è in buona sostanza quello di un *trend* degenerativo dell'utilizzo dei mezzi forniti dallo sviluppo tecnologico, che, accompagnati da una disciplina legislativa di questo tipo, rischierebbero di trasformarsi da « tecnologie della libertà » in « tecnologie del controllo »[41].

---

[38] Questi gli estremi della decisione: Urteil del Estern Senats vom 27.2.2008 — 1 BvR 370/07 — 1 BvR 595/07, reperibile sul sito ufficiale del Bundesverfassungsgericht, all'indirizzo *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*. Per un (paradigmatico) caso analogo italiano, cfr. il provvedimento del Garante del 28 febbraio 2008, pubblicato sul sito ufficiale del garante, Bollettino del n. 92/febbraio 0008, doc. *web* n. 1495246, all'indirizzo *www.garanteprivacy.it*, cd. « caso Peppermint ».

[39] Per maggiori dettagli sul caso, v. l'articolo pubblicato su *Punto Informatico* del 21 marzo 2008, all'indirizzo *www.punto-informatico.it*, dal titolo *P2P, Logistep&C fermati anche in Germania*.

[40] Cfr. S. RODOTÀ, *I diritti e la barbarie*, in *La Repubblica* del 22 marzo 2008; l'articolo pubblicato su *Punto informatico* del 21 marzo 2008, cit.; K. GEHMLICH, *German court curbs data storage law*, in *Reuters* del 19 marzo 2008, all'indirizzo *www.reuters.com*.

[41] Cfr. S. RODOTÀ, *I diritti e la barbarie*, cit.

Con una lungimirante presa di coscienza di questo problema[42], la Corte ha compiuto un passo ulteriore rispetto alla dichiarazione di illegittimità, con la vera e propria creazione di un nuovo diritto della persona: « il diritto fondamentale alla garanzia della confidenzialità e dell'integrità del proprio sistema tecnico-informativo », quale espressione del multisfaccettato diritto della personalità, interpretato addirittura (si ritiene a ragione) una vera e propria sfida all'Europa stessa, quella dei « ministri degli Interni e di quei commissari europei che vogliono realizzare proprio le forme di controllo capillare ritenute incompatibili con la libertà della persona », contrapposta all'Europa della giurisprudenza della Corte europea dei diritti dell'uomo, l'unica in grado di salvarci da una imperante « barbarie »[43].

In relazione al caso irlandese, qui si è compiuto un passo ulteriore e diverso, essendosi censurata la *data retention*, proprio in quanto operata dall'Autorità di pubblica sicurezza, per finalità di repressione dei reati, a fronte dell'adozione di una disciplina a livello comunitario.

La direttiva 2006/24/CE è stata infatti impugnata di fronte alla Corte di Giustizia, con il sostegno di ben sedici organizzazioni internazionali (tra cui l'italiana ALCEI), dal *Digital Rights Ireland*, il gruppo impegnato sul fronte dei diritti civili digitali, che aveva in precedenza avviato un'azione nanti la Corte Suprema contro il Governo irlandese, il quale avrebbe « sfidato » la normativa comunitaria e nazionale, attraverso sistemi di sorveglianza di massa[44].

Le censure delle associazioni per la tutela dei diritti civili si sono poi estese anche all'Unione stessa, che avrebbe avallato le posizioni assunte dagli Stati membri, attraverso l'adozione della Direttiva 2006/24/CE. In particolare, viene invocato l'intervento della Corte di giustizia, al fine di riaffermare i principi sanciti dall'art. 8 della CEDU e dalla stessa normativa comunitaria a tutela dei dati personali, nonché dalla Carta dei Diritti fondamentali dell'Unione Europea (che, pur attualmente priva di concreta

---

[42] A onor del vero, va detto che la decisione dello scorso febbraio è solo l'ultima di una lunga serie, generata da una riflessione e da una « cultura sedimentata », inaugurata già nel 1983, con il riconoscimento del diritto all'autodeterminazione informativa, che ha influenzato il percorso successivo, in relazione a privacy e libertà. Ancora S. Rodotà, *I diritti e la barbarie*, cit. rileva come una tale cultura non sia presente nell'ordinamento italiano, con le conseguenze che si sono viste nella disciplina della *data retention* e dei poco incisivi interveti della Corte costituzionale.

[43] L'espressione è di A. Cassese, *Dalla barbarie ci salva l'Europa*, in *La Repubblica* del 5 marzo 2008, che richiama la recentissima sentenza della Corte di Strasburgo, sul caso *Saadi vs Italia* del 28 febbraio 2008, causa n. 37201/06, in tema di lotta al terrorismo, in cui essa « ha così autorevolemente avallato la tesi, sostenuta da vari procuratori italiani, per cui la lotta al terrorismo, pur se implacabile, va condotta sempre nel pieno rispetto delle regole ». La decisione è reperibile all'indirizzo *http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/*.

[44] L'azione è stata promossa il 6 luglio 2006 (causa C-301/2006) contro il Consiglio e il Parlamento europei. Per quanto concerne la normativa nazionale, si tratta dell'*Irish Criminal Justice (Terrorist Offences) Act* del 2005, che prevede un obbligo di conservazione dei dati di traffico telefonico e telematico di almeno 3 anni.

Per completezza e quale ulteriore « segnale positivo » per la tutela dei diritti individuali, va segnalata la recentissima lettera, in data 8 aprile 2008, inviata alla Corte di Giustizia da 43 ONG (compresa ancora una volta l'italiana ALCEI), relativa all'azione di annullamento della direttiva 2006/24/CE e che si pone esplicitamente in linea di continuità con l'iniziativa irlandese del 2006. Il testo integrale è reperibile all'indirizzo *http://www.vorratsdatenspeicherung.de/content/view/216/79/lang, en/#letter*.

efficacia vincolante, è stata firmata da tutti gli Stati membri), con l'obiettivo di rendere inefficace la direttiva in tutti i Paesi dell'Unione, impedendole di vincolarli a disposizioni contrarie ai diritti umani, peraltro a fronte di nessuna prova certa sull'efficacia delle misure previste, per fermare il terrorismo o il crimine organizzato[45].

Da parte sua, anche il Garante per la protezione dei dati personali italiano è più volte intervenuto a reprimere abusi nei confronti degli utenti (ciò in analogia alla su descritta linea tenuta dal Tribunale tedesco, peraltro proprio sulla scorta dell'esempio italiano), nonché a dettare disposizioni e direttive per gli operatori, ai fini della corretta applicazione delle disposizioni in materia di *data retention*.

Già a partire dall'entrata in vigore del Codice della *privacy*, infatti, il Garante è parso attivo su questo fronte, intervenendo con prescrizioni, volte ad indicare ai « fornitori di servizi di comunicazione elettronica che svolgono, su richiesta dell'autorità giudiziaria, attività connesse alle intercettazioni telefoniche » le misure, « la cui adozione risulta necessaria e allo stato congrua anche per tutelare i diritti dell'interessato », in particolare la protezione dei dati personali trattati[46].

Con il successivo « affastellarsi » delle modifiche all'art. 132 ed il complicarsi del quadro normativo, il Garante, nella relazione al Parlamento per il 2006, parla con toni allarmati di una « sindrome bulimica » nella raccolta ed archiviazione dei dati personali, fenomeno che trasformerebbe « anche l'Unione Europea in un universo dei controllati e spiati »[47] ed al quale sembra idonea a porre un freno la direttiva Frattini, soprattutto in ragione dei più brevi termini di conservazione previsti rispetto alla normativa nazionale.

Il persistente (e pressante) invito al recepimento della direttiva si trasforma in un vero e proprio « cavallo di battaglia » del nostro Garante, al fine di pervenire, da un lato, ad un'armonizzazione a livello comunitario della disciplina della conservazione dei dati, dall'altro, al tanto auspicato punto di equilibrio tra *privacy* e riservatezza, dal quale il legislatore italiano sembra essersi sempre più allontanato, con la dilatazione dei tempi di conservazione dei dati, soprattutto all'esito dei più recenti interventi di riforma.

A seguito della « controriforma » antiterrorismo ed in attesa dell'auspicato recepimento della direttiva comunitaria (peraltro a termini già spirati), il Garante è intervenuto con nuove prescrizioni tecniche sempre più stringenti sulla tenuta e la messa in sicurezza dei dati, affinché i fornitori esercitino la *data retention* obbligatoria *ex lege*, con il maggior riguardo possibile alla tutela della *privacy*[48].

---

[45] Per maggiori dettagli sul caso, v. gli articoli pubblicati su *Punto Informatico*, n. 2610 del 18 settembre 2006, all'indirizzo *www.punto-informatico.it*, dal titolo *UE, nuova offensiva contro il controllo di massa* e su *Interlex* del 25.09.2006, all'indirizzo *www.interlex.it*, dal titolo *Data retention e diritti fondamentali dei cittadini in Europa*.

[46] Cfr. il provvedimento adottato il 15 dicembre 2005, Bollettino del n. 67/dicembre 2005,, doc. web n. 1203890, il comunicato stampa del 20 settembre 2006, Bollettino del n. 75/settembre 2006, doc. web n. 1341009, e il caso deciso il 1º giugno 2006, Bollettino del n. 73/giugno 2006, doc. web 1296533, pubblicati sul sito ufficiale del Garante all'indirizzo *www.garanteprivacy.it*.

[47] Questa la sintesi di G. Marcoccio, Data retention, *la « Pisanu » dovrà fare i conti con l'Europa*, in *Interlex* del 23 luglio 2007, all'indirizzo *www.interlex.it*.

[48] Si tratta del provvedimento del 19 settembre 2007, recante *Misure e accorgi-*

L'adozione di un nuovo provvedimento da parte del Garante, a breve distanza dal precedente e con le medesime finalità di garanzia degli interessati[49], è stata suscitata dalla proroga, contenuta nel d.l. 248/2007, suscettibile di prolungare i termini di conservazione per un tempo (problematicamente dilatato) di otto anni per il traffico telefonico e quasi quattro anni per quello telematico.

Il provvedimento ha peraltro fatto seguito ad una lettera del Garante medesimo al Presidente della Camera dei Deputati ed al Ministro delle Politiche comunitarie, in cui esprimeva le preoccupazioni sul periodo di conservazione suddetto, ponendo « l'esigenza che il bilanciamento degli interessi coinvolti sia conforme alle prescrizioni della direttiva comunitaria in materia (la cosiddetta « direttiva Frattini »), e che la direttiva stessa, la quale prevede tempi di conservazione dei dati di traffico sia telefonico che telematico compresi tra un minimo di sei mesi ed un massimo di due anni, sia tempestivamente recepita ».

Resta tuttavia da chiedersi se il recepimento della Direttiva comunitaria potrà essere effettivamente risolutivo delle criticità rilevate in precedenza, a fronte delle perplessità che circondano la normativa comunitaria stessa e di cui le citate iniziative a livello nazionale si sono fatte rivelatrici.

A quest'ultimo proposito, nel nostro ordinamento non si sono tuttavia registrate reazioni contrarie ai contenuti della direttiva, né da parte del legislatore, né da parte degli « organi di garanzia » (Autorità Garante e Corte costituzionale): anzi, come visto, il Garante, dopo essersi mostrato decisamente critico verso la disciplina nazionale della *data retention*, ha accolto con favore quella comunitaria, sollecitando il legislatore ad un recepimento tempestivo della stessa, mentre il Giudice delle leggi non ha avuto ancora occasione di pronunciarsi sul punto, risultando mancante la disciplina di attuazione. Quando peraltro la Corte si è trovata di fronte ad una questione relativa alla conservazione dei dati, come regolata dalla normativa nazionale[50], si è orientata nel senso del più scrupoloso *self restraint* nei confronti della discrezionalità del legislatore, alla luce degli obblighi *ex* art. 28 della l. 87/1953.

Da parte sua, il Governo, delegato dalla legge comunitaria per il 2006[51] all'attuazione della direttiva 2006/24, ha approvato il 27 febbraio 2008 il relativo schema di decreto legislativo, sottoposto al parere della XIV Commissione il 1° aprile 2008, dal quale non traspare l'intenzione del legislatore di discostarsi dalle prescrizioni della direttiva medesima[52].

---

menti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati, pubblicato sul sito ufficiale del Garante all'indirizzo *www.garanteprivacy.it*, a commento del quale si vedano le considerazioni di S. Bendandi, *Sicurezza e conservazione dei dati del traffico telefonico e telematico: le nuove prescrizioni del garante*, all'indirizzo *www.stefanobendandi.com*.

[49] Si tratta del provvedimento del 17 gennaio 2008, recante *Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati*. V.lo in *Interlex* del 14 febbraio 2008, con il commento di G. Marcoccio, *Dati del traffico: le nuove « misure » del Garante*, all'indirizzo *www.interlex.it*.

[50] Si tratta della sentenza 14 novembre 2006, n. 372, cit., in cui la Corte è peraltro apparsa avallare l'operato del legislatore, pur in presenza delle rilevate notevoli criticità.

[51] Legge 6 febbraio 2007, n. 13, pubblicata nella *Gazzetta Ufficiale* n. 40 del 17 febbraio 2007 — Supplemento ordinario n. 41/L.

[52] In particolare, la Commissione per le Politiche dell'Unione europea ha espres-

In attesa di conoscere la scelta definitiva del legislatore italiano, ci si può interrogare sulla motivazione dell'ossequio incondizionato alle prescrizioni del legislatore comunitario, difficilmente spiegabile, se non con la constatazione che, pur se connotata da molteplici criticità, la disciplina comunitaria, rispetto a quella nazionale, risulta comunque maggiormente « garantista » nei confronti dei diritti fondamentali[53].

Se questo è vero, è anche vero che ci si poteva forse orientare in un senso diverso (e più critico), soprattutto alla luce di una più risalente giurisprudenza della Corte costituzionale, che ha avuto modo di affermare con decisione la tutela della riservatezza delle comunicazioni, sia con riguardo ai contenuti[54], sia in relazione ai dati esterni delle stesse[55], attraverso

---

so parere favorevole, limitandosi ad un'osservazione in merito agli oneri finanziari del decreto e senza rilevare alcun profilo critico in relazione al suo contenuto, che appare in linea con la direttiva 2006/24 (e pertanto legittimo?). Il testo del parere è reperibile all'indirizzo *http://leg15.camera.it/_dati/leg15/lavori/bollet/200804/0401/html/14/allegato.htm*.

[53] Con particolare riferimento ai tempi di conservazione, si ricorda che troviamo un termine di due anni (per quanto non tassativo) contro un termine, stabilito dalla legge nazionale, che può complessivamente raggiungere gli otto anni.

[54] In particolare, l'occasione è stata quella del più generale problema delle intercettazioni telefoniche (degenerate al punto di creare un vero e proprio « caso » all'inizio degli anni Settanta), in relazione alle quali ha affermato come in tale operazione si debba « tendere al contemperamento dei due interessi costituzionali protetti onde impedire che il diritto alla riservatezza delle comunicazioni telefoniche venga ad essere sproporzionatamente sacrificato dalla necessità di garantire una efficace repressione degli illeciti penali », conseguendone « che il provvedimento di autorizzazione stabilisca anche la durata delle intercettazioni e che, quando una proroga si renda necessaria, se ne offra concreta, motivata giustificazione » (Cfr. Corte cost., 6 aprile 1973 n. 34, in *Giur. Cost.*, 1973, 316 ss, punto 2 del *Considerato in diritto*, con nota di V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, *ibidem*, 317 ss, il quale sottolinea la situazione di anarchia nella tutela del diritto alla riservatezza, creatasi negli anni precedenti la pronuncia della Corte, in cui Vassalli, *Morte della « privacy »*, in *Il Giorno* del 15 marzo 1973, constatava come « nel nostro beato Paese chiunque controllava chiunque, comunque e dovunque gli piacesse, in barba alla giustizia, in barba alla polizia, in barba alla Costituizone, in barba alla privacy dei cittadini, in barba allo Stato »).

Ancora e più nello specifico, « proprio perché la Costituzione riconosce un particolare pregio all'intangibilità della sfera privata negli aspetti più significativi e più legati alla vita intima della persona umana, le restrizioni alla libertà e alla segretezza delle comunicazioni conseguenti alle intercettazioni telefoniche sono sottoposte a condizioni di validità particolarmente rigorose, commisurate alla natura indubbiamente eccezionale dei limiti apponibili a un diritto personale di carattere inviolabile, quale la libertà e la segretezza delle comunicazioni (art. 15 della Costituzione) » (Cfr. Corte cost., 23 luglio 1991 n. 366, cit., punto 3 del *Considerato in diritto*).

[55] Si tratta della sentenza 11 marzo 1993, n. 81, in *Giur. Cost.*, 1993, 731, in cui, ancora in tema di intercettazioni, il Giudice delle leggi ha stabilito che « l'ampiezza della garanzia apprestata dall'art. 15 della Costituzione alle comunicazioni che si svolgono tra soggetti predeterminati entro una sfera giuridica protetta da riservatezza è tale da ricomprendere non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa ». In particolare, il compito di garantire l'applicazione del livello minimo di siffatti principi spetta al giudice, insieme alla valutazione sulla legittimità (e quindi ammissibilità) dell'acquisizione dei dati, ferma restando la discrezionalità del legislatore nello « stabilire più specifiche norme di attuazione dei predetti principi costituzionali ». Si veda, a commento (molto critico) della decisione, A. Pace, *Nuove frontiere della libertà di « comunicare riservatamente » (o, piuttosto, del diritto alla riservatezza)?*, in *Giur. Cost.*, 1993, 742 ss. Sulla stessa linea, pur con maggiore attenzione alla discrezionalità del legislatore,

un'interpretazione estensiva (peraltro non esente da vivaci reazioni in dottrina[56]) dell'art. 15 Cost., in combinato con l'art. 2[57].

Stando così le cose, non pare possibile sperare (almeno in tempi brevi) in un intervento, per così dire *ex auctoritate*, a garanzia della vita privata, e non resta che mantenere lo sguardo rivolto all'Europa, in attesa della risposta della Corte di Lussemburgo all'azione irlandese, non escludendo peraltro, anche da noi, un'iniziativa avverso l'attuazione nazionale della direttiva comunitaria, da parte dei singoli interessati di fronte alla Corte di Strasburgo (ancora una volta l'unica « via di scampo » alle violazioni della vita privata, per quanto « nobilmente » giustificate dalla lotta al terrorismo), nell'ideale prosecuzione di quella sfida agli abusi del legislatore nazionale e all'Europa « cattiva »[58], inaugurata dal giudice costituzionale tedesco.

---

cfr. Corte cost., 17 luglio 1998 n. 281, in *Giur. Cost.*, 1998, 2167.

[56] Per una « riflessione » sul punto si veda T. Croce, *Articolo 123*, in AA.VV., *Codice della privacy — Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Tomo II, Milano, 2004, 1526 ss e, ancora, A. Pace, *Nuove frontiere*, cit., 745, che non contesta l'esistenza del diritto alla *privacy* e la garanzia dello stesso, ma la loro riconduzione al parametro dell'art. 15.

[57] Cfr. in proposito Corte cost. 9 maggio 1985 n. 138, in *Giur. Cost.*, 1985, 986, con nota di A. Cerri, *Diritto di non ascoltare l'altrui propaganda*, *ibidem*, 987 ss; Corte cost. 1° agosto 1979 n. 98, in *Giur. Cost.*, 1979, 719, con nota di S. Bartole, *Transessualismo e diritti inviolabili dell'uomo*, *ibidem*, 1179 ss, e, in particolare Corte cost. 30 dicembre 1994, n. 463, in *Giur. Cost.*, 1994, 3985, in cui viene ribadita l'esistenza di « un diritto costituzionale — quello alla riservatezza delle proprie comunicazioni — che è stato riconosciuto da questa Corte come un diritto inviolabile ai sensi dell'art. 2 della Costituzione e, in quanto tale, restringibile dall'autorità giudiziaria soltanto nella misura strettamente necessaria alle esigenze di indagine legate al compito primario concernente la repressione dei reati (v. sentt. nn. 63 del 1994, 81 del 1993, 366 del 1991 e 34 del 1973) ».

[58] Si ricorda, quella dei « ministri degli Interni e di quei commissari europei che vogliono realizzare proprio le forme di controllo capillare ritenute incompatibili con la libertà della persona », così definita da S. Rodotà, *I diritti e la barbarie*, cit.

NORMATIVA COMUNITARIA IN BREVE

DECISIONE COMMISSIONE CE 21 maggio 2008, n. 2008/411/CE

Decisione della Commissione, del 21 maggio 2008, relativa all'armonizzazione della banda di frequenze 3 400-3 800 MHz per i sistemi terrestri in grado di fornire servizi di comunicazioni elettroniche nella Comunità.
[notificata con il numero C(2008) 1873]
(Testo rilevante ai fini del SEE)
(2008/411/CE)

(In* G.U.C.E. *L 144 del 4 giugno 2008)

(Il testo integrale è reperibile sul sito Internet *www.fondazionecalamandrei.it/comunitaria/49.rtf)*