ALLEGRA STRACUZZI

DATA RETENTION: IL FATICOSO PERCORSO DELL'ART. 132 CODICE PRIVACY NELLA DISCIPLINA DELLA CONSERVAZIONE DEI DATI DI TRAFFICO

1. Premessa introduttiva[1].

Prima di entrare nel merito giuridico vero e proprio, ritengo necessario inquadrare il tema, di cui ci occupiamo oggi, nella prospettiva che gli compete e dare atto, se pur brevemente per ragioni di tempo, della dimensione socio-politica ed economica che, gran parte delle scelte normative riguardanti il settore dell'IT in generale e quelle relative alla privacy in particolare, vengono ormai ad assumere nella società contemporanea. Farò quindi una piccolissima premessa « storica » che ci dia modo di evidenziare, anche se per sommi capi, « dove siamo » dal punto di vista giuridico e soprattutto « dove stiamo andando ».

Negli ultimi quindici anni, lo sviluppo delle nuove tecnologie ha indotto e portato tanti e tali mutamenti negli ordinamenti giuridici nazionali e sovranazionali da rappresentare, a mio avviso, una sorta di vero e proprio passaggio ad una nuova « Era » giuridica.

Si può dire che, soltanto venti anni fa, il mondo del diritto rappresentava, per quanto riguarda la regolamentazione degli effetti dell'uso della tecnologia nella società, una sorta di « prateria selvaggia ». Non esistevano norme idonee e ci si muoveva timidamente per analogia (naturalmente solo in ambito civilistico), per cercare di estendere l'operatività delle

[1] I paragrafi 1, 2 e 3.1 di questo lavoro, riportano il testo della relazione « *Data Retention: lo stato dell'arte della normativa nazionale in materia di conservazione dei dati relativi al traffico telefonico e telematico* », presentata al Convegno Assintel « *Data Retention, privacy e criminalità* » del 16 gennaio 2006.

norme « tradizionali » alla nuova realtà: ad esempio la tutela del diritto d'autore al software, o il riconoscimento dell'efficacia di riproduzione meccanica (*ex* art. 2712 c.c.) al documento elettronico.

La prima normativa specifica risale al 1992 ed ha attribuito, appunto, la tutela d'autore al software (D.Lgs. 518/92). Successivamente e per tutti gli anni '90, si è sviluppata un'attività normativa sempre più intensa e diffusa, (es. '93 reati informatici, '96 privacy, '97 firma digitale, '99 banche dati ecc.) che ha allargato notevolmente l'ambito di intervento, via via che venivano in evidenza gli effetti dell'uso della tecnologia, sulla vita sociale ed economica della collettività. Si tenga conto anche del fatto che, per collettività, deve intendersi naturalmente un contesto sociale non più nazionale ma globale e che gli interventi normativi, per quanto riguarda il nostro spazio giuridico di riferimento, hanno ormai generalmente una matrice comunitaria, a cui fa seguito il recepimento in ambito nazionale, da parte degli Stati membri. Negli anni 2000 la produzione normativa è definitivamente esplosa, insieme allo sviluppo di Internet e dell'Information Technology in generale, per cui stiamo assistendo, da qualche anno, allo sviluppo di quella che definirei: « fase delle nuove codificazioni ».

Oggi l'ordinamento giuridico nazionale non è più costituito « soltanto » dai 4 codici tradizionali e da una miriade di leggi di vario genere, ma anche da una serie, in costante aumento, di nuovi codici: il codice privacy ('03), il codice delle comunicazioni elettroniche ('03), il codice della proprietà industriale ('05), il codice dell'amministrazione digitale ('05), il codice del consumo ('05) ecc.

L'aspetto rilevante è dato dal fatto che questi nuovi codici non si limitano a riorganizzare la propria materia, coordinando le leggi precedenti, ma contengono al loro interno l'enunciazione di principi che sono, in realtà, di rilevanza costituzionale, come ad esempio e per avvicinarci al nostro tema: il diritto alla protezione dei dati personali ed il principio di necessità nel trattamento dei dati (artt. 1 e 3 del codice privacy) o il diritto all'uso delle tecnologie (art. 3 codice amministrazione digitale).

Il diritto alla protezione dei propri dati e quello all'uso delle tecnologie da parte della P.A., sono dunque nuovi diritti del cittadino contemporaneo ma, se gli analizziamo con attenzione, essi si rivelano essere le due facce di una stessa medaglia: da un lato il diritto di pretendere l'uso della tecnologia, dall'altro il diritto ad essere protetti dai rischi che tale uso comporta.

In altri termini si deve essere consapevoli del fatto che, in questi anni, si sta inequivocabilmente disegnando un nuovo e diverso assetto nei rapporti cittadino-Stato, come riflesso dell'evoluzione in corso nella società, dovuta al passaggio da cartacea-nazionale a tecnologica-globale.

Le scelte che si stanno compiendo (ripeto, ormai fondamentalmente a livello comunitario e poi « a cascata » a livello nazionale) contribuiscono a definire il concetto di quella che chiamerei la nuova « democrazia tecnologica », indicandone il relativo « tasso ». La partita che si sta giocando, riguarda quindi non solo il nostro presente, ma anche le condizioni dei futuri rapporti tra cittadini e Stati, fino ad influenzare gli equilibri tra le superpotenze.

Basti ricordare, ad esempio, il « conflitto » che si è sviluppato, negli ultimi 10 anni, tra USA e UE, per le difficoltà di applicazione della normativa privacy adottata dalla UE, a fronte di una scelta viceversa, « non impositiva di norme », adottata dagli USA. Ciò rendeva (e rende tutt'ora) illecito il trasferimento di dati verso il territorio statunitense, in quanto

non sufficientemente garantista per la privacy degli interessati (cittadini UE), a meno che non vi sia il rispetto di condizioni specifiche, che non possono essere qui esposte per ragioni di tempo.

Questo tipo di problematiche e conflitti si erano posti già dal 1996, quindi ben prima dell'insorgere dell'emergenza terrorismo, scatenata dopo l'11 settembre 2001 e riflettevano appunto la diversa concezione del rapporto cittadino-Stato, accolta dalla UE e dagli USA.

Arrivando al tema di oggi, deve essere evidenziato che, al di sopra del problema dell'individuazione del numero dei mesi di conservazione dei dati, si è ormai fissato, sia a livello nazionale che comunitario, un principio rilevante e potenzialmente molto pericoloso, da trattare con estrema cautela: quello dell'obbligo di conservazione dei dati di riferimento di ogni comunicazione, telefonica e telematica, per finalità di accertamento e repressione dei reati.

Si noti che fino all'entrata in vigore del codice privacy (1º gennaio 2004), non esisteva un obbligo di conservazione dei dati di traffico nel nostro ordinamento.

In altri termini si è preso atto che, nell'attuale fase storica, se la tecnologia ha decuplicato la nostra capacità di comunicazione, ha anche notevolmente aumentato la possibilità di delinquere e la conservazione dei dati di traffico, risulta indubitabilmente essere uno strumento efficace ai fini dell'attività di accertamento e repressione dei reati.

La questione che si pone è: quanto l'uomo contemporaneo può essere disposto a pagare, in termini di perdita della propria riservatezza, quindi di libertà, per tutelare la propria sicurezza? In realtà il prezzo che stiamo già pagando è la perdita della possibilità di mantenere la totale riservatezza, ma per quanto tempo e con quali rischi?

Il punto di equilibrio tra privacy e sicurezza passa attraverso non solo e non tanto l'individuazione del numero massimo di mesi di conservazione, ma soprattutto la fissazione di regole che garantiscano ai cittadini che sui propri dati non vengano commessi abusi, ovvero trattamenti illeciti, siano questi conservati per 24, 36 o 48 mesi.

Il rischio infatti è altissimo ed una enorme e onerosa responsabilità viene a ricadere sugli operatori, che dovranno custodire immensi volumi di dati, garantendone la sicurezza. Questi si trovano in realtà tra « due fuochi ». Da un lato la magistratura che può richiedere dati, dall'altro i singoli interessati che possono contestare loro un trattamento illecito dei propri dati, in quanto effettuato ad esempio oltre i termini consentiti dalla legge e quindi senza consenso, o in modo non adeguatamente sicuro.

Non bisogna dimenticare che, ai sensi della normativa in materia di privacy, qualsiasi trattamento di dati (inclusa la mera conservazione) effettuato senza specifico consenso, al di fuori delle esimenti legislativamente previste (tra cui ad es. l'adempimento di obblighi di legge o l'esecuzione di obblighi derivanti da un contratto) è da considerarsi illecito.

Inoltre, pur nel rispetto dei tempi di conservazione previsti dalla legge, il Titolare (nel nostro caso il fornitore di servizi di comunicazione) risponde non solo della eventuale mancata adozione delle misure minime di sicurezza (artt. 33, 169 e All. B Codice), nonché di quelle che devono essere prescritte dal Garante per i trattamenti che presentano rischi specifici (artt. 17 e 167 Codice), ma può essere chiamato, in ogni caso, a risarcire gli eventuali danni, anche non patrimoniali, cagionati per effetto del trattamento, ai sensi dell'art. 2050 codice civile. L'art. 15 del Codice assimila

infatti l'attività di trattamento dati all'esercizio di attività pericolosa, di cui il Titolare deve rispondere « ...se non prova di aver adottato tutte le misure idonee ad evitare il danno ». Tali misure sono prescritte per qualsiasi Titolare, dall'art. 31 del Codice e, più specificamente per i fornitori di servizi di comunicazione elettronica accessibile al pubblico, dall'art. 32 del medesimo.

Allora diventa di fondamentale importanza, a garanzia di tutti noi cittadini/utenti, mettere gli operatori in condizione di adempiere all'obbligo di conservazione dei dati di traffico, nei tempi e modalità corretti, applicando le misure di sicurezza idonee.

2. La conservazione dei dati di traffico e l'iter normativo dell'art. 132 del Codice Privacy.

Innanzitutto è necessario partire dal rilievo che nel nostro ordinamento, prima dell'avvento della normativa sulla privacy (l. 675/96 e correlate), una disciplina sulla conservazione dei dati di traffico era del tutto assente. Certamente gli operatori conservavano i dati a fini di fatturazione e successivamente in caso di eventuali contenziosi, ma i tempi di conservazione erano da considerarsi, dal punto di vista strettamente giuridico, del tutto discrezionali e lasciati all'iniziativa organizzativa dei singoli. In altri termini non vi era né un limite massimo di conservazione, previsto dalla legge, né soprattutto un obbligo minimo della medesima. È da ritenere ad esempio che qualsiasi operatore, una volta ottenuto il pagamento della fattura relativa al traffico (e si tratta della stragrande maggioranza dei casi), avrebbe potuto decidere di eliminare immediatamente i relativi tabulati[2], non avendo alcuna ragione, in quel caso, di attendere la scadenza del termine di prescrizione di cui all'art. 2948, comma 4, c.c.

In altri termini bisogna dire che la normativa in materia di privacy, se da un lato ha posto l'esigenza di limitare i tempi di conservazione dei dati, per tutelare la riservatezza degli individui, con ciò confliggendo con la necessità contraria di garantire l'accertamento e la repressione dei reati, dall'altro ha comunque progressivamente introdotto, nell'ordinamento giuridico, l'obbligo di conservazione dei dati stessi, a tali fini, prima inesistente.

Neanche la Legge 675/1996, stabiliva alcunché ai fini di una regolamentazione dei tempi e delle procedure relative alla conservazione di dati e all'acquisizione di tabulati in sede processuale. Il primo riferimento evidente venne stabilito con il D.Lgs. 171/98[3] che, regolando i rapporti privatistici tra fornitori ed utenti[4], stabiliva in via generale *l'obbligo per il fornitore della cancellazione* dei dati acquisiti, al termine della chiamata, salvo il trattamento finalizzato alla fatturazione (o ai pagamenti tra fornitori di reti in caso di interconnessione), « ...*consentito sino alla fine del periodo*

[2] Continuando a conservare la fattura a fini fiscali naturalmente.

[3] In G.U. n. 127 del 3 giugno 1998, attualmente abrogato dal D.Lgs. 196/03 (Codice privacy).

[4] Non vi era, infatti, alcun riferimento alla conservazione dei dati ai fini di repressione dei reati.

durante il quale può essere legalmente contestata la fattura o preteso il pagamento » (all'art. 4, comma 2). In mancanza di altri riferimenti, anche giurisprudenziali, tale termine è stato univocamente ricondotto alla disciplina della prescrizione quinquennale, di cui all'art. 2948 codice civile, che prevede, in particolare al comma 4, il termine prescrittivo di *5 anni*, per tutto ciò che deve pagarsi periodicamente ad anno o in termini più brevi[5].

La *finalità di accertamento e repressione dei reati* è stata introdotta dal Codice privacy (D.Lgs. 196/2003), con una norma apposita (art. 132), che ha stabilito *l'obbligo per i fornitori di conservare i dati relativi al traffico telefonico*[6] per un periodo non superiore a *30 mesi*, per le suddette finalità, a partire dall'entrata in vigore del Codice stesso (*1° gennaio 2004*). La conservazione avrebbe dovuto avvenire secondo modalità individuate con decreto del Ministero della Giustizia, di concerto con i Ministri di Interno e Comunicazioni e su conforme parere del Garante.

Tale norma si pone in ogni caso come deroga al principio generale, enunciato all'art. 123 del Codice[7], che conferma *l'obbligo di cancellazione dei dati di traffico* (tutti) « …quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, salvo il trattamento strettamente necessario per la fatturazione, ovvero per i pagamenti in caso di interconnessione. In questi casi è *consentito il trattamento non superiore a sei mesi*[8], a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

Già prima dell'entrata in vigore del Codice Privacy, anche a seguito dei risultati delle indagini sull'omicidio D'Antona[9], il legislatore è intervenuto a modificare il testo dell'art. 132, mediante l'emanazione del D.L. 354/03[10], ritenendo che il periodo di conservazione ivi stabilito fosse troppo esiguo, per garantire il corretto funzionamento dell'attività inquirente. Pertanto, con tale provvedimento d'urgenza[11], si è provveduto a riscrivere l'art. 132, stabilendo innanzitutto in capo al fornitore (comma 1) l'obbligo di conservazione di tutti i dati *di traffico* (da intendersi, in mancanza di

[5] Per quanto ci risulta, non vi è alcuna pronuncia che espressamente ricolleghi la prescrizione quinquennale ai canoni di fatturazione telefonica, ma a ben vedere, è disciplina perfettamente allineabile a quella del rapporto di utenza di distribuzione dell'acqua, per il quale è stabilita la prescrizione di 5 anni (Cass. 5 novembre 1979, n. 5730). La *decorrenza della prescrizione* coincide con il giorno di scadenza della prestazione e di emissione della fattura, essendo il credito divenuto liquido. Diversamente il termine di decorrenza degli interessi coincide con la scadenza del termine di pagamento della fattura, momento in cui il credito principale è anche divenuto esigibile (Cass. 16 luglio 1975, n. 2794).

[6] Ovvero i dati concernenti i tabulati telefonici.

[7] Che ha sostituito l'art. 4 del D.Lgs. 171/98.

[8] Quindi con una notevole riduzione dei termini rispetto ai 5 anni previsti dal D.Lgs. 171/98.

[9] All'epoca non erano ancora in vigore le disposizioni del nuovo Codice Privacy, e pertanto si applicava la precedente disciplina del D.Lgs. 171/98 che, come sopra riportato, consentiva la conservazione per un periodo di 5 anni desumibile dai termini prescrizionali di cui all'art. 2948 c.c.

[10] In G.U. n. 300 del 29 dicembre 2003.

[11] *NB*: L'articolo 3 del Decreto-Legge 354/2003 e della relativa Legge di conversione 45/2004, ha un unico comma, che prevede la sostituzione integrale dell'art. 132 Codice Privacy. Per facilitare i riferimenti durante il prosieguo dell'analisi, ci si riferirà ai commi del nuovo art. 132.

altre indicazioni, sia come dati *telefonici* che *telematici*), per un periodo di *30 mesi*, per finalità di accertamento e repressione dei reati in generale, e, successivamente (comma 2), un *ulteriore* periodo di *30 mesi*, unicamente per finalità di accertamento e repressione dei delitti di cui all'art. 407, c, 2, lett. *a*)[12] del c.p.p., nonché dei delitti in danno di sistemi informatici o telematici[13].

La conservazione doveva essere subordinata all'adozione di particolari misure ed accorgimenti che garantissero la sicurezza dei dati (comma 5), da individuarsi con decreto del Ministro della Giustizia di concerto con il Ministro dell'Interno, con il Ministro delle Comunicazioni e con il Ministro per l'Innovazione e le Tecnologie, su conforme parere del Garante per la Privacy (comma 6).

In attesa dell'emanazione di tale decreto, una disposizione transitoria (modificativa dell'art. 181 del Codice privacy) stabiliva che, fino al 31 dicembre 2005, per la conservazione dei dati di traffico, doveva applicarsi il termine prescrizionale indicato all'art. 4, comma 2, D.Lgs. 171/1998, consentendo la conservazione per *5 anni*[14].

In sede di conversione del D.L. 354/2003, con la L. 45/2004[15], venivano apportate nuove modifiche alla disciplina. In particolare, venivano esclusi dall'obbligo di conservazione *ex* art. 132 Codice Privacy i dati concernenti il traffico telematico, essendo fatto esplicito riferimento ai dati relativi al solo *traffico telefonico*. Il periodo di conservazione dei dati veniva ridotto a *24 mesi* per finalità di accertamento e repressione dei reati in generale, ed a *ulteriori 24 mesi* per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, comma 2, lett. *a*)[16] del cpp, nonché dei delitti in danno di sistemi informatici o telematici[17].

Per quanto concerne la normativa transitoria, veniva eliminato il riferimento temporale al 31 dicembre 2005 e veniva introdotto al suo posto un *termine « mobile »*, individuato nella data in cui sarebbero diventate efficaci le misure e gli accorgimenti prescritti ai sensi dell'art. 132, comma 5, Codice Privacy[18].

---

[12] Ovvero strage, associazione a delinquere di stampo mafioso, rapina compiuta da persona facente parte di associazione mafiosa, sequestro di persona a scopo di estorsione, delitti commessi per finalità di terrorismo ecc.

[13] Ovvero accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, Intercettazione, impedi-mento o interruzione illecita di comunicazioni informatiche o telematiche, Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.

[14] L'art. 5 del D.L. 354/2003 aggiungendo la lettera *f*) all'art. 183, c. 1, Codice Privacy, salvava dall'abrogazione per il periodo di transizione l'art. 4, c. 2, D.Lgs. 171/1998.

[15] In *G.U.* n. 48 del 27 febbraio 2004.

[16] Vedi Nota 12.

[17] Vedi Nota 13.

[18] Ovvero la previsione in ogni caso di specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B); l'individuazione e la regolamentazione delle modalità di conservazione separata dei dati una volta decorso il termine di cui all'art. 132, c. 1, Codice Privacy; l'individuazione delle modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui all'art. 132, c. 1, Codice Privacy, l'utilizzazione dei dati sia consentita solo nei casi di cui all'art. 7 e all'art. 132, c. 4, Codice Privacy; l'indicazione delle modalità tecniche per la periodica distruzione dei dati,

Queste ultime misure, infine, avrebbero dovuto essere individuate non più da un decreto interministeriale, ma attraverso un provvedimento del Garante per la Privacy, sulla base del procedimento del *prior checking* di cui all'art. 17 Codice Privacy[19], secondo quanto desumibile dalla modifica del comma 5 e dall'eliminazione del comma 6, del precedente testo.

L'Autorità Garante non ha ancora[20] emanato il suddetto provvedimento, pertanto è da ritenere che la disciplina dettata dai « nuovi » commi 1 e 2 dell'art. 132, non sia diventata efficace, rimanendo operativo, per la conservazione del traffico telefonico, « ...il termine di cui all'art. 4, comma 2, del D.Lgs. 171/98 »[21].

Qui corre l'obbligo di sottolineare un aspetto di notevole « fragilità » dell'impianto normativo, dovuto al fatto che *l'obbligo e la relativa liceità della « conservazione per finalità di accertamento e repressione dei reati » era stabilito esclusivamente dai commi 1 e 2 dell'art. 132*, non diventati « operativi ». In sostanza la dichiarata immediata applicabilità delle disposizioni sull'accesso e l'acquisizione dei dati, si fondava su una norma transitoria (l'art. 181, comma 6-*bis*, del Codice), che rimandava ad un *termine quinquennale facoltativo, stabilito a suo tempo, per esclusive finalità di fatturazione*.

Non si deve trascurare il fatto che il principio generale in materia resta sempre dettato dall'art. 123, comma 1, che impone l'immediata cancellazione dei dati di traffico, quando non sono più necessari ai fini della trasmissione, salvo le due deroghe specifiche sottoriportate.

Se si considera che l'art. 123, comma 2, del Codice, per le finalità di fatturazione, impone oggi un termine massimo di 6 mesi, salvo contestazioni in corso e che, per le finalità di accertamento e repressione dei reati, l'art. 132 impone una tempistica scadenzata da specifiche finalità e l'adozione di rigide misure di sicurezza, emerge evidente la contraddittorietà concettuale di una norma transitoria quale quella in esame. Laddove principi fondanti dell'impianto della normativa in materia di privacy sono quelli di « finalità, pertinenza e non debordanza », insieme al rispetto di opportune misure di sicurezza.

Appare allora naturale domandarsi se la norma transitoria, di cui all'art. 181, comma 6-bis, *dopo aver traslato* il termine quinquennale ad una finalità di trattamento diversa da quella originaria (dalla fatturazione — all'accertamento e repressione dei reati), fosse da considerarsi anche sufficiente a trasformarne la natura, da facoltà ad obbligo giuridico.

In altri termini, ponendosi dal punto di vista del fornitore, possono sorgere dubbi sull'effettività dell'obbligo di conservare per 5 anni e sulle possibili conseguenze di una risposta negativa ad un'eventuale richiesta dell'Autorità giudiziaria, nel caso di cancellazione avvenuta « prematuramente ».

Non solo ma non dobbiamo dimenticarci che una conservazione dei dati, oltre il termine di sei mesi di cui all'art. 123, se non prevista per legge ne-

---

decorsi i termini di cui all'art. 132, cc. 1 e 2, Codice Privacy.

[19] La conservazione dei dati di traffico viene così qualificata trattamento che presenta « rischi specifici » ai sensi del richiamato art. 17 Codice Privacy.

[20] Il Provvedimento è stato emanato il 17 gennaio 2008 (G.U. n. 30 del 5 febbraio 2008), cui è dedicato il prossimo paragrafo 6.

[21] Art. 181, comma 6-*bis*, Codice privacy, introdotto dalla L. 45/2004.

cessita del consenso degli interessati, in mancanza del quale risulta illecita e passibile di contestazione e richiesta di risarcimento danni da parte di questi ultimi.

3. Il decreto « Pisanu ».

3.1. *Le modifiche all'art. 132, la « sospensione » al 31 dicembre 2007 e la disciplina transitoria.*

A seguito degli attentati di Londra, il legislatore ha deciso di intervenire nuovamente sulla disciplina della conservazione dei dati, dettata dall'art. 132, ancorché, si ripete, non ancora operativa, con il D.L. 27 luglio 2005, n. 144[22] (c.d. decreto « Pisanu »), convertito nella Legge 31 luglio 2005, n. 155[23], che ha ulteriormente modificato tale norma, per quanto riguarda la tipologia dei dati, i tempi di conservazione e le modalità di acquisizione degli stessi.

Per quanto concerne la tipologia di dati, *si è tornati ad inserire i dati di traffico telematico*, pertanto la tempistica di conservazione risulta la seguente:

— Per finalità di accertamento e repressione dei reati, i dati relativi al *traffico telefonico* — inclusi quelli relativi alle *chiamate senza risposta* — sono conservati dal fornitore per *24 mesi*. Terminato tale periodo, gli stessi dati sono conservati dal fornitore per *ulteriori 24 mesi* per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, c, 2, lett. *a*)[24] del cpp, nonché dei delitti in danno di sistemi informatici o telematici[25],

— Per finalità di accertamento e repressione dei reati, i dati relativi al *traffico telematico* sono conservati dal fornitore per *6 mesi*. Terminato tale periodo, gli stessi dati sono conservati dal fornitore per *ulteriori 6 mesi* per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, c, 2, lett. *a*) del c.p.p., nonché dei delitti in danno di sistemi informatici o telematici.

— Rimane comunque esclusa la conservazione del contenuto delle comunicazioni.

Per quanto riguarda viceversa la reale operatività di tali norme, questa rimane subordinata all'attuazione delle misure di sicurezza, previste dal comma 5[26], rimasto inalterato, ma la cui operatività è stata demandata alla promulgazione di un regolamento (da adottarsi ai sensi dell'art. 17, comma 1, L. 400/1998), su proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri Interessati e sentito il Garante (art. 6, comma 4, D.L. 144/2005, convertito nella L. 155/2005), che ne definirà le modalità e tempi di attuazione[27].

---

[22] In G.U. n. 173 del 27 luglio 2005.
[23] In G.U. n. 177 del 1° agosto 2005.
[24] Vedi nota 12.
[25] Vedi nota 13.
[26] Ovvero il comma 5 dell'art. 132 Codice Privacy, volto al rispetto di determinate misure e accorgimenti a garanzia dell'interessato. L'art. 181, comma 6bis, non è stato modificato ed è da ritenersi vigente ed operante.
[27] Ci si potrebbe domandare se tale regolamento sia da intendersi sostitutivo

Pertanto, dal punto di vista dell'operatività della disciplina dell'art. 132, la situazione è analoga alla precedente, risultando immediatamente applicabili, come precedentemente osservato, soltanto le disposizioni attinenti all'accesso e all'acquisizione dei dati, così come modificate nei commi 3e 4-*bis*[28].

Probabilmente proprio in considerazione delle lacune ed incertezze rilevate sopra, il legislatore ha, in questa occasione, stabilito una *sorta di « obbligo provvisorio » alla conservazione*, prevedendo, all'art. 6, comma 1, che, dal 28 luglio 2005[29], e fino al 31 dicembre 2007, *è sospesa* l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono *la cancellazione dei dati di traffico telefonico o telematico*, anche se non soggetti a fatturazione. I dati, in assenza di particolari previsioni sulle modalità di conservazione[30], sono *conservati limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché dei servizi se disponibili, escludendo in ogni caso la conservazione del contenuto delle comunicazioni.*

Dal punto di vista della disciplina transitoria, la norma fa salve le disposizioni vigenti, che prevedono un periodo di conservazione ulteriore, con ciò lasciando intendere che, fino all'emanazione del Regolamento attuativo, debba applicarsi la disciplina transitoria di cui all'art. 181, comma 6bis, peraltro non toccato dalla novella. Pertanto, ferme restando le osservazioni espresse in precedenza, sembra da ritenersi *consentito conservare* i dati, anche successivamente a tale scadenza, per un periodo complessivo di *5 anni*, senza dover osservare a riguardo particolari misure o disposi-

---

del provvedimento del Garante, previsto dall'art. 17 del Codice, o se viceversa, come è più verosimile, saranno necessari entrambi per dare efficacia alla norma.

[28] Il comma 4 delle stesso articolo non viene modificato dal Decreto-Legge 144/2005, né dalla relativa Legge di conversione con modifiche 155/2005. Quindi il testo attuale risulta il seguente:

comma 3). Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera *f*), per il traffico entrante.

comma 4). Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera *a*), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

comma 4-*bis*). Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.

[29] Data dell'entrata in vigore del D.L. 144/2005, secondo quanto disposto dall'art. 19.

[30] La conservazione dei dati di traffico, come accennato in nota 19, è assimilabile alla tipologia di trattamento che presenta rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato di cui all'art. 17, Codice Privacy. Pertanto, la stessa Autorità Garante sarebbe dovuta intervenire tramite provvedimento per definirne le direttive guida su particolari misure e accorgimenti da seguire.

zioni[31], salvo le misure minime di sicurezza previste dal Codice per qualsiasi trattamento. I dati oggetto di tale disciplina transitoria dovrebbero essere esclusivamente quelli *telefonici*, considerando la lettera dell'art. 181 ed il fatto che il riferimento ai dati telematici sia stato previsto espressamente solo con l'introduzione dell'art. 6, comma 3, lett. *b*) e *d*), D.L. 144/2005, e relativa Legge di conversione.

Durante il periodo di sospensione non è stata purtroppo specificata la finalità di trattamento, se coincidente, come è probabile, con quella generale di accertamento e repressione dei reati, di cui al comma 1 dell'art. 132, o con quella più specifica di cui al comma 2. Il legislatore si è viceversa occupato della finalità dei dati conservati oltre i limiti previsti dall'art. 132, consentendone l'utilizzo esclusivamente per le finalità del Decreto Legge, ma facendo salvo anche l'esercizio dell'azione penale per i reati comunque perseguibili.

Disciplina transitoria sino all'emanazione del Regolamento di cui all'art. 6, comma 4, D.L. 144/2005, e relativa Legge di conversione n. 155/2005.

Dal momento che la disciplina dettata dai primi due commi dell'art 132, come più volte ripetuto, è in attesa di attuazione, in mancanza delle previsioni sulla modalità di conservazione, sulle tempistiche di adeguamento e sulla previsione dei costi, si rende necessario individuare la disciplina attualmente applicabile alle differenti situazioni ipotizzabili, con riguardo alla conservazione dei dati.

Nella seguente esemplificazione si pone l'attenzione sul rischio di trattamento oltre i termini consentiti e quindi illecito, partendo dal presupposto che venga osservato da tutti il termine quinquennale e tralasciando pertanto la questione della obbligatorietà o meno di tale termine.

I *dati che dovrebbero venire cancellati durante il periodo di sospensione*, *in quanto raccolti nei precedenti 5 anni*, non possono che essere *dati telefonici* e devono essere obbligatoriamente conservati sino al 31 dicembre 2007 — possono essere utilizzati unicamente per le finalità del D.L. 144/2005, salvo l'esercizio dell'azione penale per i reati comunque perseguibili, e devono essere di conseguenza cancellati al termine del periodo di sospensione.

I *dati acquisiti prima del periodo di sospensione e conservabili oltre il termine del 31 dicembre 2007*, in quanto i 5 anni scadono successivamente a tale termine, possono essere unicamente *dati telefonici* e dovranno essere cancellati allo scadere del quinquennio, a meno che non venga prima emanato il regolamento attuativo dell'art. 132, che renderà operativo il termine di 48 mesi.

I *dati acquisiti durante il periodo di sospensione della cancellazione* (28 luglio 2005-31 dicembre 2007), seguono la disciplina transitoria in attesa della promulgazione del Regolamento di cui all'art. 6, comma 4, Decreto-Legge 144/2005, e relativa Legge di conversione con modifiche. Possono essere *dati telefonici o telematici*. Nel primo caso potranno essere conservati, oltre la scadenza del termine di sospensione, fino allo scadere

[31] In mancanza del Provvedimento specifico del Garante, previsto dal 5° comma dell'art. 132.

del quinquennio, a meno che non venga prima emanato il regolamento attuativo dell'art. 132, che renderà operativo il termine di 48 mesi. Nel secondo caso potranno essere conservati oltre la scadenza del termine di sospensione, solo nel caso in cui venga prima emanato il regolamento attuativo dell'art. 132, che renderà operativo il termine di 12 mesi.

I *dati acquisiti successivamente al periodo di sospensione*. I dati acquisiti successivamente al 31 dicembre 2007, seguiranno la nuova disciplina dettata dall'art. 132, Codice Privacy, confidando in una tempestiva emanazione del suddetto Regolamento di attuazione. In mancanza è da ritenere che per i *dati telefonici* dovrà applicarsi la normativa transitoria più volte richiamata, mentre i *dati telematici* non potranno essere conservati a tali fini, rimanendo vigente soltanto la disciplina di cui all'art. 123.

3.2. *Gli obblighi a carico degli esercizi pubblici di telefonia e Internet o di gestori di circoli privati.*

Il decreto « Pisanu », recante misure urgenti per il contrasto del terrorismo internazionale, ha anche apportato integrazioni alla disciplina amministrativa degli esercizi pubblici di telefonia e Internet, prevedendo nuove disposizioni in materia (art. 7). È ivi previsto un obbligo generalizzato di licenza per chi è già esercente o intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono messi a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali per le comunicazioni, anche telematiche. Tali soggetti devono seguire specifiche regole nell'acquisizione dei dati degli utenti, nella conservazione di tali informazioni e nelle misure di monitoraggio e sicurezza, da adottare a protezione dei dati stessi e contro eventuali accessi non autorizzati, ai servizi messi a disposizione.

In particolare è stata prevista[32] l'emanazione di un decreto del Ministro dell'Interno, di concerto con il Ministro delle Comunicazioni e con il Ministro per l'Innovazione Tecnologica, sentito il Garante per la Privacy, per stabilire le misure tecnologiche e metodologiche da adottare nello svolgimento delle predette attività.

In data 16 agosto 2005 è stato adottato tale decreto[33], recante misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche, non vigilate, per comunicazioni telematiche, ovvero punti di accesso ad Internet utilizzando tecnologia senza fili. È stata anche promulgata una Circolare del Ministero dell'Interno[34], recante provvedimenti amministrativi e decreti attuativi previsti dagli artt. 7, 8 e 9 Decreto-Legge 144/2005, così come modificato in sede di conversione dalla Legge 155/2005.

Visto l'alto contenuto tecnico presente sia nel Decreto-Legge 144/2005 che nel Decreto ministeriale 16 agosto 2005 e nella Circolare 557/2005, è opportuno cercare di fare chiarezza sul significato di alcuni concetti tecno-

[32] Art. 7, comma 4.
[33] In G.U. n. 190 del 17 agosto 2005.
[34] Circolare del ministero dell'Interno del 29 agosto 2005, in sito ministero www.interno.it.

logici fulcro della normativa, e sull'eventuale correttezza nell'applicazione.

Ancora una volta la produzione normativa non è stata del tutto coerente con quanto effettivamente esistente allo stato della tecnica, come si osserverà una volta analizzata la legislazione di riferimento.

Pertanto, ricostruendo il quadro generale delle previsioni normative sopra riportate, emergono le seguenti considerazioni:

— *Soggetti.*

Le disposizioni si applicano in riferimento a chiunque abbia intenzione di aprire, o abbia già avviato l'attività, un pubblico esercizio o un circolo privato di qualsiasi genere, nel quale siano poste a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche[35]. Rientrano in questa categoria, dunque, non solo internet point e locali assimilati, ma anche « qualsiasi circolo privato ». Tale definizione lascia intendere che rientri nella categoria anche ogni forma di associazione non riconosciuta o comitato che, per propria natura, nasce come soggetto di diritto senza particolari formalità, con unica indicazione di operare per il raggiungimento di un fine comune.

Ex art. 5, Decreto 16 agosto 2005, sono esplicitamente *esclusi* dall'applicazione della normativa, i rivenditori di apparecchi terminali o altri prodotti elettronici per le attività di prova, svolte sotto la diretta vigilanza degli addetti alle dimostrazioni, l'offerta di servizio fax attraverso la normale rete telefonica, l'accesso alle reti telematiche attraverso apparati che utilizzano SIM/USIM sulla rete di telefonia mobile, rilasciate ai sensi dell'art. 55 del decreto legislativo 1º agosto 2003, n. 259[36], come modificato dall'art. 6, comma 2, Decreto-Legge 144/2005 e relativa Legge di conversione.

È in questo senso controversa la qualificazione giuridica, ai fini dell'applicazione della presente normativa, dei locali aperti al pubblico, quali alberghi, pensioni, residence, probabilmente anche università e biblioteche[37], che consentono il collegamento alla rete telematica attraverso l'utilizzo sia di postazioni messe a disposizione dell'utente, sia attraverso le predisposizione di una presa di rete, alla quale si possa collegare l'utente, con mezzi propri. La normativa sembra essere chiara, ed anche la conve-

[35] Art. 7, c. 1 D.L. 144/2005, così come modificato in sede di conversione dalla L. 155/2005 e Art. 1, c. 1, decreto 16 agosto 2005.

[36] Era infatti già previsto nel Codice delle comunicazioni elettroniche che (art. 55, c. 7) ogni impresa fosse tenuta a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno, gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che sono identificati al momento dell'attivazione del servizio. Con il Decreto 144/2005 e relativa Legge di conversione, è stato previsto che prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica, le imprese debbano adottare tutte le necessarie misure, affinché venga garantita l'acquisizione e la corretta conservazione dei dati della persona che procede all'acquisto. Pertanto l'identificazione dell'utente e l'associazione col numero di telefono mobile avviene al momento del rilascio della SIM/USIM card da parte del fornitore di servizi.

[37] Sulla stessa linea sono da considerarsi rientranti nella categoria tutte le strutture, pubbliche o private che possono, secondo logica, mettere a disposizione dei propri clienti-utenti collegamenti alla rete telematica, quali, ad esempio, campeggi, bed and breakfast, centri multimediali, librerie, centri di ricerca universitari, ecc.

nienza della logica, in quanto si parla di « apparecchi terminali », e tali non possono, dunque, essere considerati i telefoni posti in ciascuna camera, ma soltanto gli apparecchi che consentono un servizio di connessione, diverso da quello della semplice comunicazione vocale (infatti, la *ratio* della normativa in esame non riguarda la telefonia vocale). In considerazione di ciò, la Circolare 557/2005 afferma che anche gli esercizi che già sono obbligati alla identificazione del cliente, *ex* art. 109 del T.U. delle leggi di Pubblica Sicurezza[38], sono comunque soggetti ai nuovi obblighi di identificazione e registrazione, laddove vengano offerti, alle persone ospitate, servizi di connessioni alle reti telematiche, anche se gratuite. Pertanto, gli esercenti attività recettive dovranno seguire tutti gli obblighi di identificazione e conservazione di cui alla normativa in esame, con la possibilità, nel caso in cui vengano messe a disposizione dei clienti non più di tre apparati terminali per la comunicazione, di usufruire della semplificazione di cui all'art. 1, comma 4, Decreto 16 agosto 2005, ovvero registrazione su supporto cartaceo[39]. Alla luce di quanto osservato, dunque, agli esercenti attività ricettive dovrebbero applicarsi tutti gli obblighi derivanti dall'art. 7 del Decreto antiterrorismo. Per le realtà non rientranti nella categoria di attività recettiva — che come biblioteche e università sono per lo più di natura pubblica — non viene specificato nulla. È conveniente pertanto ritenere che anche per atenei e strutture simili aperte al pubblico, dovrebbero essere predisposte regole per l'osservanza delle misure di identificazione e registrazione previste per le attività sopra riportate[40]. A supporto di questa tesi, soccorre la previsione di cui all'art. 3, comma 2, decreto 16 agosto 2005, che annovera nella categoria di postazione non vigilata (per quanto riguarda credenziali di accesso ad uso plurimo) proprio centri di ricerca, università ed altri istituti di istruzione[41].

Come ulteriore specificazione, l'art. 3 dello stesso decreto stabilisce (comma 1) che le disposizioni dell'art. 1, con esclusione di quella di cui al comma 1, lettera *c*), si applicano anche nei confronti dei fornitori di apparecchi terminali utilizzabili per le comunicazioni telematiche collocati in aree non vigilate[42], esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale[43]. Queste « zone recettive » consentono l'ac-

[38] Ovvero la disposizione che impone l'obbligo di identificazione ai fini di pubblica sicurezza dei clienti delle strutture ricettive.

[39] Come previsione di semplificazione, infatti, il Decreto 16 agosto 2005 prevede all'art. 1, c. 4, che per gli esercizi o i circoli aventi non più di tre apparecchi terminali a disposizione del pubblico, i predetti dati possono essere registrati su di un apposito registro cartaceo con le pagine preventivamente numerate e vidimate dalla autorità locale di pubblica sicurezza ove viene registrato anche l'identificativo della apparecchiatura assegnata all'utente e l'orario di inizio e fine della fruizione dell'apparato.

[40] Inoltre, per le università e altri centri ricerca, il discorso di complica, in quanto vengono spesso messe a disposizione di studenti e ricercatori prese di linea dedicate in modo da accedere il più velocemente possibile tramite risorse dell'utente sia a banche dati su reti locali, sia al web in generale.

[41] Vedi nota 43.

[42] Per intenderci, sono aree di accesso non vigilate, per esempio, le postazioni degli aeroporti o delle stazione ferroviarie messe a disposizione dei viaggiatori da parte della struttura di accoglienza su accordo pregresso con un fornitore di servizi di telecomunicazione.

[43] Continua il comma stabilendo che in tal caso gli abbonamenti, forniti anche mediante credenziali di accesso prepagate o gratuite, non potranno avere validità superiore ai dodici mesi dall'ultima operazione di identificazione. È interessante notare come il comma 2 preveda, in questo senso,

cesso di utenti alle risorse telematiche attraverso postazioni fisse, usando sia collegamenti cablati che collegamenti *wireless*. In genere, presso queste postazioni non è prevista la presenza di personale per l'identificazione degli utenti e la registrazione delle postazioni utilizzate. L'accesso, infatti, è regolato attraverso abbonamento o carta prepagata, con l'individuazione dell'utente al momento del rilascio dell'user name e della password. Il controllo del traffico, quindi, viene effettuato a monte, associando i dati identificativi dell'utente, precedentemente acquisiti, con il periodo di utilizzo e consumo del servizio in relazione all'inserimento dell'user name e della password. Questo significa che, sebbene non si dovranno adottare le forme di monitoraggio diretto dell'attività, previste all'art. 2 del decreto, si dovranno comunque applicare le disposizioni sulle misure di sicurezza, sull'identificazione degli abbonati e sulla conservazione dei dati (secondo quanto previsto dall'art. 1, comma 3), da attuarsi, probabilmente — e in mancanza di altre indicazioni — mediante sistemi automatici di raccolta e memorizzazione.

— *Obblighi: licenza*.

Dal 17 agosto 2005[44] al 31 dicembre 2007[45] è necessaria la richiesta di una *licenza al questore* (licenza « di polizia ») per l'apertura di un pubblico esercizio o di un circolo privato di qualsiasi specie nel quale siano posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche. Tale licenza, come sopra osservato, non è richiesta nel solo caso di installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale. Chi aveva già avviato un'attività di questo genere, doveva richiedere la licenza al questore entro il 26 settembre 2005[46]. In entrambi i casi, la licenza si intende rilasciata trascorsi 60 sessanta giorni dall'inoltro della domanda (Art. 7, comma 3)[47].

Inoltre, la Circolare 557/2005 precisa che la licenza di cui trattasi non sostituisce ma si aggiunge alla dichiarazione di inizio attività di cui all'art. 25, Decreto Legislativo 259/2003 (che, anzi, viene considerata presupposto essenziale) ed inoltre a tale licenza si applicano, per espressa indicazione del suddetto art. 7, le disposizioni del Testo Unico delle leggi di Pubblica

deroghe temporali (fino a cinque anni) a favore di università, centri di ricerca e istituti di istruzione similari, per abbonamenti per l'accesso ad uso plurimo dei propri utenti.

[44] Ovvero 15 giorni dopo l'entrata in vigore della Legge 155/2005 (art. 7, c. 1, D.L. 144/2005, come modificato dalla Legge di conversione 155/2005).

[45] Prorogato al 31 dicembre 2008 dal Decreto « Milleproroghe » del 31 dicembre 2007.

[46] Ovvero entro 60 giorni dall'entrata in vigore del D.L. 144/2005.

[47] In quest'arco temporale, le Questure, come evidenziato dalla Circolare 557/2005 dovranno svolgere gli accertamenti di rito, con particolare attenzione ai profili di sicurezza, dandone comunicazione alla Direzione Centrale della Polizia di Prevenzione, anche ai fini di un eventuale approfondimento informativo nelle sedi più appropriate, e, se trattasi di stranieri, alla Direzione Centrale della Polizia Criminale, al fine di un eventuale approfondimento attraverso i canali di scambio informativo con gli organi di polizia esteri. Di converso, nel caso in cui la domanda sia presentata per il tramite di un Commissariato di pubblica sicurezza o di un Comando territoriale dei Carabinieri, i predetti Uffici, verificata la completezza della documentazione, provvederanno a trasmettere rapidamente il carteggio alla Questura, corredato delle informazioni di competenza e segnalando le eventuali controindicazioni ai fini della sicurezza. In caso di comunicazione di rigetto, è previsto il ricorso gerarchico al Prefetto, oltre al ricorso giurisdizionale.

Sicurezza concernenti: *a*) le autorizzazioni di polizia (Titolo I - Capo III), fra cui, particolarmente, quelle degli artt. 9 (prescrizioni), 10 e 11 (condizioni per il rilascio, la sospensione e la revoca); *b*) i controlli e le sanzioni (Titolo I - Capo IV), e, particolarmente, l'art. 16 (controlli) e l'art. 17 (sanzioni penali); *c*) la disciplina generale dei pubblici esercizi (Titolo III - Capo II), fra cui, particolarmente, quelle degli artt. 92 (ulteriori condizioni di rilascio), 93 (conduzione tramite rappresentanza) e 100 (sospensione della licenza per motivi di pubblica sicurezza); e quelle corrispondenti del regolamento di esecuzione (fra cui gli artt. 152 e 153)[48].

— *Obblighi: adempimenti per l'acquisizione e la conservazione dei dati.*

I titolari e i gestori di cui sopra, secondo quando emerge dal decreto 16 agosto 2005, sono tenuti a identificare le persone che accedono ai servizi telefonici o telematici offerti, tramite l'acquisizione dei dati anagrafici riportati sul documento di identità e tramite la riproduzione dello stesso, da effettuarsi in modalità elettronica (ovvero attraverso apparato scanner), secondo quanto stabilito dall'art. 1, comma 4, decreto 16 agosto 2005[49]. Gli stessi sono anche tenuti ad adottare le misure fisiche e tecnologiche al fine di impedire l'accesso ai predetti servizi in assenza della previa identificazione. Tale disposizione risulta ancora più importante se messa in relazione a quanto esaminato a riguardo delle postazioni non vigilate (art. 3, decreto 16 agosto 2005) e, soprattutto, a riguardo dell'accesso alle reti telematiche attraverso tecnologia senza fili (art. 4, decreto 16 agosto 2005). Infatti, mentre è semplice monitorare gli accessi all'interno dei locali di esercizio, più difficile è garantire l'identificazione, nonché l'univoca associazione tra utente e postazione, in caso di utilizzo di tecnologia senza fili. Questa tipologia di trasferimento dati, come si osserverà in seguito, sebbene logicamente funzioni come una postazione cablata (come conduttore, a posto del filo di rame c'è una particolare frequenza), è più debole nella protezione contro attacchi di terze persone o tentativi di accesso abusivo.

I titolari ed i gestori sono, inoltre, tenuti ad informare, anche in lingue straniere (non meglio specificate dal decreto), il pubblico delle condizioni d'uso dei terminali messi a disposizione, comprese le modalità di identificazione e di accesso di cui sopra.

---

[48] In conseguenza di quanto sopra, secondo quanto stabilito nella Circolare 557/2005, la domanda da inoltrare alla Questura, con le modalità indicate nella Circolare ministeriale 11001/114/1 Gab. del 16 agosto 2005, sarà corredata di copia della dichiarazione già inoltrata al Ministero delle Comunicazioni, secondo il modello prescritto dall'art. 25 del Decreto Legislativo 259/2003, e di copia della documentazione di trasmissione. Per installazioni che non dovessero rientrare nel campo di applicazione del predetto art. 25, la domanda sarà acquisita con riserva di verifica presso il Ministero competente.

[49] Il comma in questione prevede anche l'acquisizione del « tipo » e del « numero » di documento di identità, sebbene il concetto di « riproduzione elettronica » ricomprenda in esso tali informazioni (come un fotografia o una fotocopia, la copia a mezzo scanner riproduce perfettamente il documento, dal quale, ovviamente, emergono sia tipologia che numerazione). Considerato quanto disposto, è pertanto da intendersi necessario provvedere alla registrazione dei dati anagrafici comprensivi del tipo e del numero di documento su un file di testo (anche per facilitarne archiviazione e conservazione), mentre su un file di immagine (tipo jpeg o bitmap) sarà riprodotta elettronicamente, archiviata e conservata la copia fotografica del documento cartaceo.

I titolari ed i gestori sono tenuti poi, secondo la normativa, a monitorare l'attività, ovvero ad adottare le misure necessarie per memorizzare e mantenere i dati acquisiti, in modo da renderli disponibili a richiesta, anche per via telematica, al Servizio di Polizia postale e delle comunicazioni, nonché all'autorità giudiziaria e alla polizia giudiziaria. Con riferimento a quanto stabilito nelle normative esaminate, i *dati* che dovranno essere di volta in volta registrati come monitoraggio dell'attività, risulterebbero essere (ricordando che rimangono comunque esclusi i contenuti delle comunicazioni):

- i Dati identificativi di cui sopra (anagrafici, documento di identità, ecc.);
- l'associazione dell'indirizzo IP della postazione con i dati identificativi dell'utente;
- i *Log* forniti dal service provider e le relative *sessioni attivate* (da associare all'indirizzo IP della singola postazione);
- data e ora, nonché la tipologia del servizio utilizzato[50].

Il decreto 16 agosto 2005 prevede, inoltre, che gestori e titolari assicurino il corretto trattamento dei dati acquisiti, nonché il mantenimento con modalità che ne garantiscano l'inalterabilità e la non accessibilità da parte di persone non autorizzate sino al 31 dicembre 2007[51]. Come sopra evidenziato, i dati sono raccolti e conservati con modalità informatiche[52]. In sostanza, si prevedono in capo ai soggetti di cui sopra gli obblighi in materia di trattamento di dati personali di cui al Codice Privacy (informativa, richiesta di consenso, incarichi a responsabile, misure di sicurezza), essendo questi a tutti gli effetti titolari di trattamento. Inoltre, mancando norme specifiche a riguardo, per garantire l'inalterabilità e la non accessibilità, gli stessi soggetti dovranno riversare quanto prima i dati acquisiti, secondo le modalità elencate, in supporti inalterabili quali CD o DVD. Il fatto che tali dati siano facilmente modificabili (i file di log non sono altro che semplici file di testo in cui sono memorizzate delle informazioni), presupporrebbe l'immediato riversamento non appena creati. Vista l'oggettiva impossibilità di tale operazione, risulterebbe quantomeno opportuno apporre la propria firma digitale al momento della creazione del file sul supporto rigido, in modo di garantirne la non modificabilità e permettere l'accumulo di più dati prima del riversamento su supporto rimovibile.

— *Accesso*.

L'accesso ai dati conservati, da parte dell'autorità giudiziaria e degli altri soggetti di cui all'art. 1, comma 1, lett. *e*)[53], è disciplinato, in conformità al Codice di Procedura Penale ed al Codice privacy[54].

---

[50] Vedere di seguito gli approfondimenti tecnici per una descrizione dettagliata della tipologia dei dati interessati.

[51] Termine prorogato al 31 dicembre 2008 dal Decreto « Milleproroghe » (si veda l'art. 2 del decreto 16 agosto 2005).

[52] È prevista una forma di semplificazione per realtà di piccole dimensioni (vedi nota 39).

[53] Ovvero il Servizio di polizia postale e delle comunicazioni, quale Organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni.

[54] Quindi si presume in base al comma 3 del nuovo testo dell'art. 132, poiché i commi 4 e 4-*bis* sono stati abrogati dal D. Lgs. 109/2008 (si veda paragrafo 8) del nuovo testo dell'art. 132.

Il decreto 16 agosto 2005 precisa che l'accesso da parte della Polizia postale, può comprendere i dati del traffico telematico, solo se effettuato tramite autorizzazione dell'autorità giudiziaria, in conformità alla legge in vigore.

— *Profili tecnici.*

Il decreto « Pisanu » parla più volte di apparecchio terminale. In linea generica, un terminale è un'interfaccia per la comunicazione. L'accezione del termine usato dal legislatore risulta essere corretto in associazione alla specifica di « apparecchio terminale utilizzabile per le comunicazioni », ovvero tutti quei sistemi di input e output che permettono la comunicazione tra la macchina messa a disposizione dell'utente e le risorse collegate in rete, siano esse reti locali, intranet o reti esterne[55]. Pertanto, a prescindere dalle modalità di accesso e di utilizzo[56], per apparecchio terminale è da intendersi una postazione computerizzata, che permette l'interscambio di dati con una qualsiasi altra postazione.

Accontentandoci di definire « rete telematica », quell'insieme di reti interconnesse tra più postazioni computerizzate, che adottano una codifica comune per l'interscambio di dati[57], è necessario definire il concetto di rete senza fili, o wireless. Il termine è riferito ad un apparato di rete (tipicamente computer, palmare, cellulare), in cui la trasmissione dati tra i componenti terminali della comunicazione avviene tramite onde radio, senza alcun tipo di cablaggio. Diversamente, i modem e gli hub[58] (a seconda delle porte usate su quest'ultimo) sono dispositivi di Data Communication Equipment, ossia un tramite necessario per la comunicazione. Pertanto, appare in parte errato il concetto di « accesso alle reti telematiche attraverso tecnologia senza fili », mentre risulta più corretta la formulazione di « utilizzo della tecnologia (di trasferimento dati) senza fili per l'accesso alle postazioni fisse cablate che permettono l'interscambio di dati su una rete ». La differenza è notevole, in quanto, prestando fede all'accezione utilizzata dal legislatore, l'accesso alla rete risulta essere a monte, ovvero tramite il dispositivo senza fili, mentre in realtà esso è a valle, ovvero tramite il modem o l'hub della postazione fissa, che gestisce l'interazione con le altre postazioni wireless. Pertanto, le misure da adottare per il controllo dell'accesso alle reti telematiche, attraverso tecnologia senza fili, di cui all'art. 4, decreto 16 agosto 2005, devono essere logicamente effettuate come se si trattasse di postazione fissa: si identifica la postazione collegata, anche senza fili, e la si correla all'utente che la utilizza in quel determinato momento. L'accesso alla rete telematica, come per le postazioni fisse, rimane gestito dal server centrale che utilizza il modem o l'hub specifico per il tipo di connessione prescelta.

---

[55] Sono da escludersi, secondo quanto previsto dall'art. 1, c. 1, Decreto 16 agosto 2005, i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale.

[56] Normale computer con tastiera o mouse e modem dedicato, piuttosto che touch-screen in una intranet locale o postazioni di video conferenza con telecamera e microfono, ecc.

[57] Esistono svariati protocolli di comunicazione, più o meno sicuri a seconda dei sistemi utilizzati (il TCP/IP è il più comune, ma certamente uno dei meno sicuri), e numerose modalità di cablaggio che si diversificano per la gestione del flusso dei dati e per la collocazione dei nodi di scambio (token ring, ehternet, ecc.).

[58] Rispettivamente, il dispositivo per la trasmissione e la ricezione seriale dei dati in forma analogica o digitale e il dispositivo per mettere in comunicazione più postazioni computerizzate, al fine di creare una rete.

Il fatto che le previsioni del decreto 16 agosto 2005 non vengano applicate, secondo quanto previsto dall'art. 1, comma 1, ai telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, dovrebbe lasciar intendere che le stesse si applichino ad ogni altri servizio di comunicazione[59]. Inoltre, l'art. 5 del Decreto, prevede espressamente al comma 1, lett. *b*), che le disposizioni si applichino in caso di « utilizzo di tecnologie a commutazione di pacchetto », e del sistema « voip », che, inserito tra parentesi nella formulazione del comma, dovrebbe essere una specificazione del primo concetto. La commutazione a pacchetto è definita come metodo di comunicazione che suddivide un messaggio in parti più piccole (pacchetti[60]) prima di inoltrarle in rete al destinatario. Ogni pacchetto inviato da una stazione (nodo[61]) segue un proprio percorso di rete per raggiungere la stazione finale, la quale provvederà a riordinare i pacchetti e riassemblare il messaggio di partenza. Il Voip (Voice over Internet Protocol) è il protocollo utilizzato per implementare su reti Internet la telefonia vocale, che pertanto utilizza il sistema di commutazione a pacchetto[62], ma non è nient'altro che un insieme di regole standard che permettono il trasferimento dei dati tra macchine (esattamente come il protocollo TCP/IP). Pertanto l'associazione effettuata dal legislatore tra commutazione a pacchetto e Voip, risulta poco comprensibile (come anche il concetto di fax attraverso il protocollo Voip, che, avendo una banda di frequenza limitata, può solamente inviare segnali vocali tramutati in digitale). Secondo il legislatore, bisognerebbe applicare le disposizioni in materia, a qualsiasi comunicazione di dati effettuata tramite la commutazione a pacchetto o, *rectius*, a qualsiasi comunicazione effettuata tramite connessione ad una rete telematica che non utilizzi la commutazione a circuito tradizionale (non esistendo altre forme di commutazione dati). Inoltre, alla luce di quanto osservato, emerge chiaramente come, essendo *ex* art. 5, comma 1, decreto 16 agosto 2005, espressamente esclusa dall'applicazione delle disposizioni l'offerta del servizio fax tradizionale, faccia poca differenza accertare l'esistenza o meno della possibilità di inviare fax tramite una determinata tecnologia (voip), dal momento che sarebbe sufficiente approfittare dell'altra tecnologia (fax tradizionale tramite commutazione circuitale) per non lasciare tracce particolari di riconoscimento dietro di sé.

Inoltre dal momento che il decreto obbliga, come precedentemente osservato, i titolari ed i gestori al monitoraggio di ogni attività di telecomunicazione effettuata nei propri locali, è sostanzialmente prevista la tracciabilità di ogni dato trasmesso attraverso la procedure di commutazione di pacchetto. Ovvero ogni dato in entrata e in uscita da un determinata postazione di comunicazione deve essere tracciato e registrato limitatamente a quelli che sono definiti dati di traffico (data e ora della comunicazione, soggetti della comunicazione, modalità di comunicazione)[63], a prescindere dalle tipologie di protocollo e trasmissione dati utilizzata. Se tale disposi-

[59] Così come evidenziato dalla Circolare 557/2005.

[60] Unità di informazione trasmessa e riconosciuta in rete dall'entità mittente e destinataria.

[61] Computer o risorsa di rete, univocamente identificabile da un indirizzo di rete e capace di ricevere e riconoscere i dati trasmessi.

[62] Invece della commutazione a circuito della telefonia tradizionale.

[63] Si ricorda che ai sensi dell'art. 6, c. 1, D.L. 27 luglio 2005, n. 144, come modificato dalla Legge di conversione 155/2005,

zione può funzionare per il protocollo TCP/IP che, sebbene possa aprire contemporaneamente più canali di comunicazione (sia di basso che di alto livello) permette in pratica la conservazione delle sessioni IP effettuate sulla rete, altrettanto non vale nel caso, per esempio, della comunicazione di posta elettronica. La gestione delle e-mail, infatti, può utilizzare protocolli particolari (quali SMTP o IMAP) in caso di programmi particolari (Outlook, Eudora), che ne facilitano la tracciabilità grazie a file log[64] predefiniti. Ma la maggior parte delle volte, la gestione delle e-mail viene effettuata direttamente sul server (vedi Hotmail, Google Mail, ecc.) tramite una interfaccia di una pagina Web e non rimane traccia del tipo di operazioni effettuate (invio, ricezione, ecc.) sul server locale. Pertanto esse appariranno come una normale pagina web visitata dal tal soggetto al tal orario, ma non si avranno tracce né dell'avvenuta spedizione o ricezione di mail, né del soggetto al quale il messaggio è stato spedito.

Alcuni server particolari, poi, permettono un servizio di gestione della posta elettronica che garantisce una forma di corrispondenza anonima, definito Anonymous Remailer. Tali server, in sostanza ricevono una mail e la reinstradano ad un destinatario, impedendo di risalire, almeno non direttamente, al mittente originario. La normativa a riguardo è chiara, come emerso in precedenza: è obbligatorio assicurare il corretto trattamento dei dati di traffico acquisiti (necessari all'individuazione dei soggetti, delle tempistiche e delle metodologie di comunicazione) e la loro conservazione[65]. Pertanto, non sarebbe possibile l'utilizzo di un server che nasconda tali dati non permettendone la individuabilità, ovvero garantendo l'anonimato dell'utente.

Per ultimo, si accenna all'eventualità dell'utilizzo di particolari server che, attraverso programmi di gestione e mappatura dati, rendono invisibili le operazioni effettuate, dissociandosi dal numero IP di identificazione assegnato normalmente, al momento della connessione. In teoria l'utilizzo di tali tecnologie[66] sarebbe vietato come nel caso delle precedenti, e varrebbero le stesse considerazioni di cui sopra, ma l'eventualità che essi siano stabiliti in paesi stranieri renderebbe ancora più difficoltoso tracciare le comunicazioni di dati che transitano su tali server.

4. La Direttiva 2006/24/CE.

Nell'ambito della lotta al terrorismo, anche il Consiglio dell'Unione Europea aveva avviato, dal 2004, lo studio di misure comuni in materia di conservazione dei dati relativi alle telecomunicazioni[67].

sono esclusi comunque i contenuti delle comunicazioni.

64 Ovvero file in cui si tengono registrate le attività compiute da un'applicazione, da un server, o da un programma interprete di comandi.

65 Art. 1, c. 1, lett. *b*) e *f*), art. 2, c. 1 e c. 2, Decreto 16 agosto 2005.

66 Rientrano tra esse vari programmi dinamici di condivisione file, quali IDC++ o Emule, che, di fatto, creano sessioni di IP fasulle per rendere non tracciabile la trasmissione dei dati. (*L'obbligo, a carico dei Provider, di fornire soltanto indirizzi di protocollo internet che assicurino l'effettiva univocità, è stato introdotto dal D. Lgs. 109/2008 ed entrerà in vigore, a seguito della proroga contenuta nel D.L. 151/2008, del 31 dicembre 2008*).

67 Dichiarazione del Consiglio europeo del 25 marzo 2004, ribadita il 13 luglio 2005, sottolineandone l'urgenza a seguito degli attentati di Londra.

Il 15 marzo 2006 era stata approvata la Direttiva 2006/24/CE[68] (cosiddetta Direttiva « Frattini »), con l'obiettivo di armonizzare le disposizioni degli Stati membri, relative agli obblighi di conservazione dei dati di traffico, …« allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale » (art. 1, comma 1).

Nei *considerandа* il legislatore comunitario ha disegnato molto chiaramente il quadro di riferimento che ha portato a fissare il « punto di equilibrio », tra gli opposti interessi in gioco, quale emerge dall'articolato vero e proprio.

Partendo dalla conferma dell'obbligo degli Stati membri di « ..tutelare i diritti e le libertà delle persone fisiche relativamente al trattamento dei dati personali e, in particolare il diritto alla vita privata, per assicurare la libera circolazione dei dati personali nella Comunità » (considerando 1)[69], la Direttiva rileva che diversi Stati membri hanno adottato normative sulla conservazione dei dati, ai sensi dell'art. 15, paragrafo 1, Dir. 2002/58/CE[70] e che queste differiscono considerevolmente tra di loro (considerando 5).

Dopo aver ribadito che « ogni restrizione di questo tipo deve essere necessaria, opportuna e proporzionata, all'interno di una società democratica, per specifici fini di ordine pubblico, … »[71]. (considerando 4), la Direttiva rileva che le differenze giuridiche e tecniche tra tali normative, « …costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche, giacché i fornitori di 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 » (considerando 6).

D'altra parte, poiché è indubbia l'importanza e la validità della conservazione dei dati di traffico delle comunicazioni elettroniche, quale strumento per la prevenzione, indagine, accertamento e perseguimento dei reati (considerando 7), è necessario garantire, a livello europeo, la conservazione di tali dati per un certo periodo di tempo (considerando 11), in conformità ai requisiti dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) (considerando 9)[72], ferma restando la piena applicabilità, ai dati conservati, delle Direttive 95/46/CE e 2002/58/CE (considerando 15).

---

[68] (GUCE n. L 105 del 13 aprile 2006), « riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE ». Quest'ultima « relativa al trattamento dei dati personali e della vita privata nel settore delle comunicazioni elettroniche » (GUCE n. L 201 del 31 luglio 2002).

[69] Conformemente alla Direttiva 95/46/CE del 24 ottobre 1995 « relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati » (GUCE n. L. 281 del 23 novembre 1995) ed alla Direttiva 2002/58/CE.

[70] L'articolo consente agli Stati membri di adottare misure legislative che prevedano la conservazione di certi tipi di dati, per un periodo di tempo limitato, « …per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica… »

[71] replica il contenuto dell'art. 15 Dir. 2002/58/CE, riportato alla nota precedente.

[72] « …Non può esservi ingerenza della

Entrando nel merito dell'articolato, la Direttiva definisce i destinatari degli obblighi di conservazione, individua le categorie di dati oggetto dell'obbligo e la durata del medesimo, fornendo agli Stati membri le indicazioni per definire i soggetti che potranno accedere ai dati, individuare le misure di sicurezza[73] e le autorità pubbliche, cui dovrà essere demandata la responsabilità del controllo.

Innanzitutto vi è la conferma che l'obbligo di conservazione riguarda soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, nell'ambito della giurisdizione dello Stato membro, qualora i dati …« siano generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati… » (art. 3). Nella misura in cui tali dati non siano generati o trattati da detti fornitori, non sussiste alcun obbligo di conservarli (considerando 23).

In secondo luogo si chiarisce che l'obbligo di conservazione non riguarda « …il contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche » (art. 1, comma 2)[74]. Riguarda viceversa anche i dati relativi ai tentativi di chiamata non riusciti (sia telefonici che telematici), escluse le chiamate non collegate (art. 3, comma 2).

Le categorie di dati da conservare sono specificamente individuate, distinte per telefonia fissa e mobile, o per accesso Internet, posta elettronica e telefonia via Internet, secondo i seguenti criteri:

a) dati necessari per identificare la fonte di una comunicazione,

b) dati necessari per rintracciare e identificare la destinazione di una comunicazione,

c) dati necessari per determinare la data, l'ora e la durata di una comunicazione,

d) dati necessari per determinare il tipo di comunicazione,

e) dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature,

f) dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile.

In terzo luogo si stabilisce che la durata dei periodi di conservazione dovrà essere stabilita, dagli Stati membri, tra un minimo di sei mesi ed un massimo di due anni, dalla data della comunicazione (art. 6)[75].

Inoltre si demanda agli Stati membri la responsabilità di adottare misure per garantire che i dati conservati siano trasmessi solo alle autorità nazionali competenti, in casi specifici e conformemente alle normative na-

---

pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria tra l'altro per la sicurezza nazionale, l'ordine pubblico, la prevenzione di disordini o reati, la protezione dei diritti e delle libertà fondamentali altrui… » (considerando 9).

[73] Facendo salve comunque quelle adottate in conformità alle Direttive 95/46/CE e 2002/58/CE.

[74] A questo proposito si rimanda al prossimo paragrafo 6 per l'interpretazione fornita dall'Autorità Garante italiana, nell'ambito del provvedimento ivi commentato. Il divieto di conservazione di alcun dato relativo al contenuto della comunicazione è ribadito anche all'art. 5, comma 2.

[75] È data facoltà allo Stato membro, che si trovi ad affrontare circostanze particolari, tali da giustificare una proroga, di estendere il periodo massimo di conservazione, per un periodo limitato, previa procedura di notifica alla Commissione (art. 12).

zionali, secondo procedure di accesso conformi a criteri di necessità e proporzionalità, da definirsi con legislazione nazionale (art. 4)[76].

Per quanto concerne infine le misure di sicurezza, la Direttiva fissa alcuni principi minimi di carattere generale, facendo salve le disposizioni adottate in conformità alle Direttive 95/46/CE e 2002/58/CE e prevedendo l'obbligo di distruzione dei dati alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati (art. 7). È riservato agli Stati membri il compito di provvedere a stabilire e far rispettare regole di immagazzinamento conformi, tali per cui i dati conservati possano essere trasmessi immediatamente alle autorità competenti, su loro richiesta (art. 8).

La Direttiva doveva essere recepita dagli Stati membri, entro il 15 settembre 2007.

5. La proroga del Decreto « Milleproroghe ».

Poiché l'Italia non si era avvalsa, a differenza di molti altri Stati, della facoltà di differimento, fino al 15 marzo 2009, dell'applicazione della Direttiva 2006/24/CE, previa dichiarazione all'atto dell'adozione, il termine di recepimento era rimasto quello originario, ormai scaduto.

Nel frattempo, si stava avvicinando la scadenza del termine di « sospensione » dell'obbligo o facoltà di cancellazione dei dati conservati, introdotto dal decreto « Pisanu »[77], senza che fosse stato reso operativo il testo dell'art. 132, stabilito da detto decreto, in particolare con riguardo alla tipologia di dati ed alla tempistica di conservazione. Alla scadenza di tale termine, non essendo stato emanato né il Regolamento attuativo, né il Provvedimento sulle misure di sicurezza da parte del Garante, sarebbe scattato l'obbligo di cancellazione per i dati conservati, telematici e telefonici, con il ritorno alla disciplina dell'art. 132, nella versione stabilita dalla L. 45/2004, che prevedeva la conservazione dei soli dati telefonici, per 24 mesi più 24, fatta salva la disciplina transitoria del termine quinquennale facoltativo.

Con il Decreto « Milleproroghe » del 31 dicembre 2007[78] è stato posticipato, al 31 dicembre 2008, tale termine di « sospensione », prorogando di un altro anno la conservazione indiscriminata dei dati telefonici e telematici.

A seguito di un intervento del Garante[79], teso a denunciare l'anomalia italiana, che avrebbe portato i tempi di conservazione a superare di 4 volte il limite fissato a livello comunitario, con la legge di conversione è stato modificato il precedente testo, prorogando il termine di « sospensione » fino « ...all'entrata in vigore del provvedimento di attuazione della Direttiva 2006/24/CE ...e comunque non oltre il 31 dicembre 2008 ».

---

[76] Nel rispetto della normativa comunitaria ed in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo.

[77] 31 dicembre 2007 si veda paragrafo 3.1.

[78] D.L. 31 dicembre 2007 n. 248-Art. 34.

[79] Lettera al Parlamento e al Governo del 15 gennaio 2008, in cui il Garante ha rilevato che, con tale proroga, i tempi di conservazione dei dati telefonici sarebbero arrivati a 8 anni e quelli telematici a quasi 4 anni.

6. Il Provvedimento del Garante del 17 gennaio 2008.

Contemporaneamente alla lettera di denuncia, il Garante ha emesso l'atteso provvedimento prescrittivo delle misure di sicurezza da adottare, per la conservazione dei dati di traffico, ai sensi dell'art. 132, V comma[80] e dell'art. 17 Codice[81], dando così attuazione, per quanto di competenza dell'Autorità e ferma restando la prorogata « sospensione » di cui al decreto « Pisanu », alla normativa generale contenuta nell'attuale testo dell'art. 132 e, di conseguenza, eliminando la disciplina transitoria del termine quinquennale facoltativo[82].

Il Provvedimento contiene, oltre ad una sintesi puntuale del quadro normativo di riferimento comunitario e nazionale, alcune premesse interpretative di rilievo, in ordine ai soggetti/fornitori destinatari dell'obbligo di conservazione, ai tipi di dati che devono essere conservati, alle finalità perseguibili ed alle modalità di acquisizione dei dati medesimi.

Innanzitutto viene chiarito che i fornitori/destinatari dell'obbligo sono « ...i soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete e che offrono servizi a utenti finali secondo il principio di non discriminazione... ».

L'obbligo di conservazione riguarda in sostanza i fornitori diretti di connessione, telefonica o telematica, e pertanto non sono ritenuti destinatari del provvedimento:

— i soggetti pubblici o privati, che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (es. Intranet aziendale per dipendenti o collaboratori);

— i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i dati relativi al traffico (es. rivenditori di connessione);

— i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, ovvero punti di accesso a Internet utilizzando tecnologia senza fili...[83].

— i gestori di siti Internet che diffondono contenuti sulla rete (c.d. « *content provider* »)

---

[80] Comma 5. « Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a:

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B);

b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;

c) individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;

d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2. ». Comma modificato successivamente dal D.Lgs. 109/2008.

[81] Provvedimento a carattere generale del 17 gennaio 2008 (G.U. n. 30 del 5 febbraio 2008).

[82] La piena operatività dell'art 132 risultava tuttavia ancora subordinata all'emanazione del regolamento attuativo, previsto dall'art. 6, comma 4, del decreto Pisanu. (Successivamente abrogato dal D.Lgs. 109/2008).

[83] In sostanza i destinatari degli obblighi di cui all'art. 7 del Decreto Pisanu, si veda paragrafo 3.2.

— i gestori di motori di ricerca, in quanto i dati che essi trattano, consentendo di tracciare agevolmente le operazioni compiute dall'utente in rete, sono, comunque, parimenti qualificabili alla stregua di « contenuti »[84].

I dati da conservare devono essere soltanto quelli « …sottoposti a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione »[85], quindi soltanto quelli « …che risultino nella disponibilità dei fornitori, in quanto derivanti da attività tecniche strumentali alla resa dei servizi offerti dai medesimi, nonché dalla loro fatturazione. Ciò in ossequio anche ai principi di pertinenza e non eccedenza stabiliti dagli artt. 3 e 11 del Codice »[86].

Per quanto riguarda le comunicazioni telematiche, in particolare, il Garante ha rilevato nelle Premesse, specifiche criticità ulteriori, rispetto a quelle telefoniche, in quanto dati apparentemente esterni (es. una pagina web visitata o un indirizzo IP di destinazione) sono in grado di rilevare o identificare sostanzialmente anche il contenuto della comunicazione e quindi permettere di ricostruire relazioni personali e sociali, desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Il Provvedimento si riferisce in sostanza ai dati relativi alla navigazione in Internet e all'uso dei motori di ricerca, generalmente conservati dai gestori, anche a causa dell'utilizzo di sistemi informatici (es. proxy server) che, interponendosi tra l'utente e i siti, consentono una ingente raccolta di dati relativi alle connessioni effettuate durante la navigazione[87].

A questo proposito, con comunicato stampa del 24 gennaio 2008, il Garante ha reso nota l'emanazione di una serie di provvedimenti con cui ha vietato, ai maggiori gestori (Telecom, Vodafone e H3G), la conservazione di tali dati ai fini di giustizia, disponendone la cancellazione, in quanto illegittimi perché non necessari, né per l'instradamento della comunicazione né per la fatturazione.

Il Provvedimento individua specificamente, in ogni caso, i diversi « servizi » telefonici e telematici, oggetto dell'obbligo di conservazione dei dati di traffico.

Nei primi sono ricompresi:

— le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax;

— i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;

— la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms.

Nei secondi sono ricompresi:

— l'accesso alla rete Internet;

— la posta elettronica;

— i fax (nonché i messaggi sms e mms) via Internet;

---

[84] Provvedimento 17 gennaio 2008 par. 3.

[85] Art. 4, comma II, lett. *h* del Codice.

[86] Provvedimento 17 gennaio 2008 par. 4

[87] Questa interpretazione del Garante ha suscitato forti preoccupazioni, da parte di esponenti dell'Autorità giudiziaria preposti alla funzione inquirente, in quanto l'impossibilità di utilizzo di tali dati renderebbe oltremodo difficili le indagini in materia di reati di pedopornografia, che notoriamente trovano nella rete un mezzo di propagazione collaudatissimo.

— la telefonia via Internet (cd. Voice over Internet Protocol-VoIP).

Poiché i dati sono conservati obbligatoriamente soltanto per le finalità di accertamento e repressione di reati, indicate ai commi 1 e 2 dell'art. 132 del Codice, il Provvedimento specifica anche le conseguenti limitazioni che ne derivano, per i fornitori, nel caso in cui ricevessero richieste volte a perseguire scopi diversi.

Questi non sono autorizzati a corrispondere a richieste riguardanti tali dati, nell'ambito di controversie civili, amministrative e contabili e devono essere consapevoli del fatto che tale vincolo di finalità deve essere rispettato anche dall'interessato (che può esercitare il proprio diritto di accesso *ex* art. 7 del Codice unicamente in riferimento alle predette finalità penali), come pure, nell'ambito del procedimento penale, dal difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle parti private[88].

La responsabilità che viene a gravare sui gestori non è di poco conto, se si considera che l'art. 132, 3º comma, consente al difensore dell'imputato e della persona sottoposta alle indagini, di rivolgersi direttamente ad essi per richiedere i dati di traffico, relativi alle utenze del proprio assistito, « …con le modalità indicate dall'art. 391-*quater* c.p.p., ferme restando le condizioni di cui all'art. 8, comma 2, lett. *f*, per il traffico entrante »[89].

Ciò comporta anche per i gestori, sottolinea il Provvedimento, « …la necessaria valutazione preliminare della circostanza che dalla mancata conoscenza dei dati richiesti possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 »[90]. Essi sono quindi chiamati ad effettuare una valutazione di merito, circa il rispetto delle finalità, nell'ambito delle richieste avanzate dagli interessati e dai difensori.

Nel merito delle misure di sicurezza, su cui non appare opportuno soffermarsi in questa sede, queste sono state individuate con notevole accuratezza e specificità e riguardano: i sistemi di autenticazione e di autorizzazione, la conservazione separata, gli incarichi al trattamento, la cancellazione dei dati, i sistemi di *audit log* , quelli di *audit* interno, la documentazione dei sistemi, la cifratura dei dati. Tali misure avrebbero dovuto (si veda paragrafo 9) essere adottate dai gestori al più presto e, comunque, entro e non oltre il 31 ottobre 2008.

7. Le modifiche introdotte dalla Legge n. 48/2008 di ratifica della Convenzione di Budapest.

Con la legge 18 marzo 2008 n. 48[91], di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest

[88] Provvedimento 17 gennaio 2008 par. 5

[89] L'art. 8, comma 2, lett. *f*, vieta all'interessato di esercitare i diritti *ex* art. 7, nel caso in cui il trattamento sia effettuato da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397.

[90] A questo proposito il Provvedimento rimanda ad un precedente provvedimento del Garante del 3 novembre 2005.

[91] Entrata in vigore il 5 aprile 2008 (G.U. n. 80 del 4 aprile 2008, Suppl. Ord. n. 79).

il 23 novembre 2001, sono state introdotte nuove fattispecie di reato in materia di sistemi informatici[92] e trattamento dati, potenziati i mezzi di contrasto con modifiche al codice di procedura penale e ampliato notevolmente l'ambito applicativo dell'art. 132 del Codice, in materia di conservazione di dati di traffico[93].

La modifica di tale norma consiste nell'introduzione di tre nuovi commi[94], con i quali si è conferito, ad organi facenti capo al Ministero dell'interno[95], il potere di ordinare ai gestori la conservazione e protezione di dati di traffico telematico, esclusi i contenuti, a fini diversi e con tempistiche particolari, rispetto a quelli stabiliti, ai primi due commi, per la generalità dei dati.

Le nuove finalità sono: lo svolgimento delle investigazioni preventive, previste dall'art. 226 delle norme di attuazione, coordinamento e transitorie del codice di procedura penale[96], nonché l'accertamento e la repressione di specifici reati (che dovranno evidentemente essere indicati nel singolo provvedimento con cui si dispone l'ordine), anche in relazione alle eventuali richieste avanzate da autorità investigative straniere (comma 4-*ter*).

L'ordine di conservazione può essere disposto per un periodo non superiore a 90 giorni, prorogabile per motivate esigenze, per una durata complessiva non superiore a sei mesi. I gestori, destinatari di tali ordini, dovranno ottemperarvi senza ritardo, fornendo all'autorità richiedente l'immediata assicurazione dell'adempimento e mantenendo il segreto, in relazione all'ordine ed alle attività svolte, per tutto il periodo indicato dall'autorità.[97]

L'autorità giudiziaria è chiamata ad intervenire solo in sede di convalida, da parte del pubblico ministero[98], cui il provvedimento dovrà essere comunicato, per iscritto, entro le 48 ore.

Limitandoci, in questa sede, alle considerazioni inerenti esclusivamente gli aspetti relativi alla tutela dei dati personali, nell'ottica dell'attuale assetto della normativa, comunitaria e nazionale, in materia di *data retention*, si deve rilevare come la nuova formulazione dell'art. 132 introduca una disciplina autonoma e sostanzialmente sovversiva del sistema esistente: sia sotto il profilo dei soggetti destinatari dell'obbligo di conservazione, che sotto quello delle misure di sicurezza da applicare.

Nei paragrafi precedenti si è evidenziato come, sia la Direttiva 2006/24/CE che il D.Lgs. 196/2003, individuino come unici destinatari dell'obbligo

---

92 Che sarebbero quindi andate ad aggiungersi alle finalità di accertamento e repressione dei delitti in danno di sistemi informatici e telematici di cui al II comma dell'art. 132.

93 Art. 10 L. 48/2008.

94 4-*ter*, 4-*quater* e 4-*quinquies*.

95 Il Ministro dell'interno o su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza, nonché gli altri soggetti indicati nel comma 1 dell'art. 226 dellenorme di attuazione, coordinamento e transitorie del c.p.p.

96 D.Lgs. 28 luglio 1989 n. 271 e ss. modifiche: « ...per l'acquisizione di notizie concernenti la prevenzione di delitti di cui all'art. 407, comma 2, lettera *a*) n. 4 e 51, comma 3-*bis* del codice ».

97 In caso di violazione si applica l'art. 326 codice penale (« Rivelazione e utilizzo di segreto d'ufficio »).

98 In mancanza di convalida, il provvedimento perde efficacia. Trattandosi di investigazioni preventive si deve presumere che non vi sia un procedimento penale in corso e quindi neanche un P.M. competente, in quanto assegnatario di un'indagine.

di conservazione dei dati di traffico, i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione[99]. I nuovi commi 4-*ter* e 4-*quater* dell'art. 132, indicando, come destinatari dell'ordine di conservazione, genericamente: « ...fornitori e operatori di servizi informatici o telematici », escono dallo schema comunitario, individuando una platea enormemente più ampia, che può ricomprendere qualsiasi soggetto che fornisca servizi tecnologici, ivi incluse le categorie di soggetti espressamente richiamate nel Provvedimento del Garante del 17 gennaio 2008, in quanto escluse dall'obbligo di conservazione e dalle misure di sicurezza.

Inoltre la conservazione dei dati di traffico telematico, disposta dai provvedimenti di cui ai nuovi commi, rischia di sfuggire all'obbligo di applicazione delle specifiche misure di sicurezza, previste dal 5º comma dell'art. 132 e stabilite dal Garante, ai sensi dell'art. 17 del Codice, nel suddetto Provvedimento.

In primo luogo perché nel 5º comma sono contemplate, ai fini delle misure di sicurezza da individuare ed applicare, soltanto le finalità di trattamento indicate ai commi 1 e 2, del medesimo articolo, restando così escluse le nuove finalità indicate dal comma 4-*ter*.

In secondo luogo perché i destinatari dell'obbligo di conservazione sono, come già rilevato, diversi, essendo immensamente più ampia la definizione di fornitori contenuta nel comma 4-*ter*, potenziali destinatari dei futuri « ordini » di conservazione.

In terzo luogo perché, essendo il Provvedimento sulle misure di sicurezza del 17 gennaio 2008, coerente con le premesse, esso prevede esplicitamente, come propri destinatari, soltanto i fornitori che mettono a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione, escludendo espressamente tutti gli altri, come già indicato in precedenza e per le esclusive finalità di cui ai commi 1 e 2 dell'art. 132.

Tutto ciò appare altresì confermato dal fatto che è lo stesso nuovo comma 4-*ter* a prevedere che, nell'ordine di conservazione, possano essere indicate particolari modalità di custodia dei dati e l'eventuale indisponibilità degli stessi da parte dei fornitori medesimi ovvero di terzi.

In sintesi non si può non rilevare come le modifiche introdotte dalla L. 48/2008, in materia di *data retention*, abbiano avuto l'effetto di rompere il difficile equilibrio, faticosamente raggiunto, a livello comunitario, tra esigenze di lotta alla criminalità e quelle di tutela della riservatezza dei cittadini, scardinando l'assetto normativo vigente.

Come ciò sia potuto avvenire, nonostante l'attenta opera di vigilanza e sensibilizzazione portata avanti dall'Autorità Garante, il quasi contemporaneo Provvedimento del 17 gennaio 2008, il divieto di conservazione dei dati relativi alla navigazione in Internet ed all'uso dei motori di ricerca ed infine la sollecitazione all'attuazione urgente della Direttiva 2006/24/CE, che vanno in senso diametralmente opposto, risulta di difficile comprensione.

---

[99] Art. 1 Direttiva e Titolo X, Capo I del Codice, di cui fa parte l'art. 132. Confermato anche dall'art. 6 del decreto « Pisanu ».

8. Il D.Lgs. n. 109/2008 di recepimento della Dir. 2006/24/CE.

A distanza di due mesi è stata comunque recepita, con D.Lgs. n. 109 del 30 maggio 2008[100], anche la Direttiva 2006/24/CE.

Il Decreto ha operato un intervento di secca « chirurgia » normativa, senza nulla concedere e/o recepire né delle indicazioni di politica legislativa, né delle specificazioni interpretative contenute, sia nella Direttiva che nel Provvedimento del Garante del 17 gennaio 2008. Si è già rilevato che entrambi si sono soffermati in particolare sull'individuazione della tipologia di soggetti tenuti all'obbligo di conservazione e sulla conseguente esclusione di tutti gli altri soggetti[101], come pure sull'interpretazione del divieto di conservare il contenuto delle comunicazioni[102], nonché sull'esclusione dell'obbligo di conservare i dati relativi alle chiamate non collegate[103].

Il Decreto tace su tutto ciò, limitandosi a implementare e/o recepire alcune definizioni (fra cui quella di « chiamata senza risposta »), a modificare gli artt. 132 e 154 del Codice ed aggiungere l'art. 162-*bis*, a prevedere un ulteriore illecito, la cui sanzione è applicabile dal Ministero dello sviluppo economico, ad abrogare l'art. 6, comma 4, del decreto « Pisanu ».

In ogni caso cerchiamo di procedere con una qualche sistematicità e cominciamo dalle modifiche effettuate.

Per quanto concerne le definizioni[104], sono state modificate alcune fra quelle già esistenti nel Codice, per renderle conformi a quelle contenute nella Direttiva: come la definizione di « utente » che adesso ricomprende anche le persone giuridiche, quella di « dati relativi al traffico » che adesso ricomprende anche « ...i dati necessari per identificare l'abbonato o l'utente » e quella dei « dati relativi all'ubicazione », che adesso ricomprende anche quelli relativi « ...alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude ». Facendo salve tutte le ulteriori definizioni già elencate nel Codice[105], sono state altresì inserite le nuove definizioni di: « traffico telefonico »[106], « chiamata senza risposta »[107], « identificativo dell'utente »[108], « indirizzo di protocollo Internet (IP) univocamente assegnato »[109].

L'art. 132 è stato modificato, in maniera consistente, per adeguare i termini di conservazione ai limiti comunitari[110]:

---

[100] « Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE » (G.U. n. 141 del 18 giugno 2008).

[101] Artt. 1 e 3, comma 1 e considerando 11 e 23 Direttiva, paragrafi 3 e 4 Provvedimento del Garante.

[102] Artt. 1, comma 2 e 5, comma 2, considerando 13 Direttiva, Premesse e paragrafo 4 Provvedimento del Garante.

[103] Artt. 2, comma 2 lett. *f*) e 3, comma 2 e considerando 12 Direttiva, paragrafo 4 Provvedimento del Garante.

[104] Art. 1 del D.Lgs. n. 109/2008.

[105] All'art. 4, comma 1.

[106] Recependo il contenuto della definizione di « servizio telefonico » della Direttiva.

[107] Recependo il contenuto della definizione di « tentativo di chiamata non riuscito » della Direttiva.

[108] Conforme alla Direttiva.

[109] Ampliando il contenuto della definizione di « identificativo dell'utente » della Direttiva.

[110] Art. 2 del D.Lgs. 109/2008 (que-

— è stata eliminata la distinzione tra reati più e meno gravi, unificando i termini di conservazione a ventiquattro mesi, dalla data della comunicazione, per i dati di traffico telefonico e dodici mesi per quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, per finalità di accertamento e repressione dei reati (modifiche al comma 1, abrogazione del comma 2 e conseguentemente dei commi 4 e 4-*bis*);

— è stato previsto un termine brevissimo per i dati relativi alle chiamate senza risposta che, trattati temporaneamente dagli operatori, devono essere conservati per trenta giorni (creazione del comma 1-*bis*)[111];

— sono rimasti invariati i commi 4-*ter*, 4-*quater* e 4-*quinquies*, aggiunti dalla legge n. 48/2008, su cui permangono le osservazioni svolte al paragrafo precedente[112];

— è stato modificato il comma 5: con l'eliminazione del riferimento alle finalità di cui al comma 2 (abrogato), con la soppressione dei punti *b*) e *c*), in quanto riferiti anch'essi alle misure di sicurezza ulteriori, per la conservazione separata dei dati, per la finalità indicata al comma 2 e con l'eliminazione del riferimento ai termini di cui al comma 2, dal punto *d*).

Le categorie di dati da conservare, da parte degli « operatori di telefonia e di comunicazione elettronica »[113], sono stati specificati più dettagliatamente di quanto non avesse fatto la Direttiva, in quanto sono stati indicati distintamente, per ogni categoria di dati, quelli necessari per la telefonia di rete fissa e mobile, quelli necessari per l'accesso Internet, quelli per la posta elettronica e quelli per la telefonia-invio di fax-sms-mms — via Internet.

Con riguardo all'accesso ad Internet, è stato stabilito l'obbligo di assicurare la disponibilità e l'effettiva univocità degli indirizzi di protocollo Internet, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico che offrono servizi di accesso a Internet (Internet Access Provider) e che devono provvedervi entro 90 giorni dalla data di entrata in vigore del Decreto[114].

È stata altresì prevista la possibilità, nel caso si renda necessario anche al fine dell'adeguamento all'evoluzione tecnologica, di specificare ulteriormente i dati da conservare (sempre nell'ambito delle categorie date), con apposito decreto[115].

---

sta è la VI volta che viene modificato l'art. 132).

[111] Quest'obbligo acquista efficacia « ...decorsi tre mesi dalla data di entrata in vigore del presente decreto » (art. 6, comma 3, D.Lgs. n. 109/2008). La Direttiva sembrerebbe disporre diversamente in quanto, ferma restando l'esclusione delle chiamate non collegate, fa rientrare le chiamate senza risposta tra i dati da conservare per periodi non inferiori a sei mesi e non superiori a due anni (artt. 3, comma 2 e 6).

[112] A giudicare dalla numerazione dei commi, sembrerebbe quindi che l'iter di approvazione del Decreto non abbia tenuto conto delle modifiche intervenute, due mesi prima, con la L. 48/2008.

[113] Questa espressione, contenuta nel titolo dell'art. 3 del D.Lgs. 109/2008, è approssimativa e non contribuisce alla chiarezza necessaria ed auspicata, in considerazione dei rilievi espressi sia in questo paragrafo che in quello precedente, relativo ai destinatari dell'obbligo di cui al comma 4-*ter*.

[114] Art. 6, comma 5 del D.Lgs. n. 109/2008.

[115] Da emanarsi da parte del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri per le politiche europee, dello sviluppo economico, dell'interno, della giustizia, dell'economia e delle finanze e della difesa, sentito il Garante

L'attività di controllo sul rispetto della normativa vigente, « ..con riferimento alla conservazione dei dati di traffico », è stata attribuita al Garante per la protezione dei dati personali, aggiungendola ai compiti elencati dall'art. 154, comma 1, lett. *a*) del Codice[116].

La violazione delle disposizioni di cui all'art. 132, commi 1 e 1-*bis*, è stata inserita tra gli illeciti amministrativi, con l'aggiunta dell'art. 162-*bis* al Codice, che stabilisce l'applicazione, salvo che il fatto costituisca reato, della sanzione amministrativa pecuniaria da 10.000,00 euro a 50.000,00 euro, aumentabile sino al triplo in ragione delle condizioni economiche dei responsabili della violazione[117].

La norma fa salvo anche quanto previsto dal comma successivo, del medesimo art. 5 del D.Lgs. 109/2008, che configura una ulteriore ipotesi di illecito amministrativo, non inserita nel Codice, inerente l'omessa o incompleta conservazione dei dati, ai sensi dell'art. 132, commi 1 e 1-*bis* del Codice, cui si deve applicare la medesima sanzione amministrativa indicata sopra, da parte viceversa del Ministero dello sviluppo economico.

In altri termini, sembra di poter dedurre che mentre all'Autorità Garante è stato lasciato il compito di verificare e sanzionare, dal punto di vista della « privacy », il mancato rispetto dei termini massimi di conservazione dei dati, la verifica e relativa sanzione della violazione dell'obbligo di conservare i medesimi dati, è stata demandata al Ministero dello sviluppo economico. La prima deve sanzionare l'eccessiva conservazione, mentre il secondo deve sanzionare la incompleta o mancata conservazione, ai sensi dei commi 1 e 1-*bis* dell'art. 132.

Al medesimo Ministero è stato altresì affidato il compito di applicare la sanzione amministrativa, da 5.000,00 euro a 50.000,00 euro anch'essa, come le altre, aumentabile fino al triplo in ragione delle condizioni economiche dei responsabili della violazione, nel caso di assegnazione di indirizzo IP che non consenta l'identificazione univoca dell'utente o abbonato[118].

I destinatari dell'obbligo di conservazione, di cui all'art. 132, sono anche tenuti ad inviare al Ministero della Giustizia, entro il 30 giugno di ogni anno, le informazioni statistiche relative:

— al numero complessivo dei casi in cui sono stati forniti dati, relativi al traffico telefonico o telematico, alle autorità competenti, conformemente alla legislazione nazionale applicabile;

— al periodo di tempo trascorso tra la data della memorizzazione dei dati di traffico e quella della richiesta, da parte delle autorità competenti;

— ai casi in cui non è stato possibile soddisfare le richieste di accesso ai dati.

Tali informazioni saranno successivamente inoltrate alla Commissione europea, ai sensi dell'art. 10 della Direttiva.

Il Decreto abroga infine l'art. 6, comma 4 del decreto « Pisanu », ovvero la norma che rimandava ad un emanando regolamento del Presidente

per la protezione dei dati personali (art. 3, comma 2).

[116] Art 4, comma 1 del D.Lgs. 109/2008.

[117] Art. 5, comma 1 del D.Lgs. n. 109/2008.

[118] Art. 5, comma 2 del D.Lgs. n. 109/2008.

del Consiglio dei Ministri, la disciplina delle modalità e dei tempi di attuazione dell'art. 132[119].

Dal quadro normativo nazionale vigente emerge, a questo punto, la seguente situazione.

Il legislatore nazionale non si è avvalso, nel recepire la Direttiva, della facoltà di proroga del periodo massimo di conservazione, prevista dall'art. 12, nel caso in cui « uno Stato membro si trovi ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato... »[120].

Dal combinato disposto del testo dell'art. 34 del Decreto « Milleproroghe » e del Decreto di attuazione della Direttiva 2006/24/CE, sembrerebbe quindi di poter concludere, essendo stato emanato, da parte dell'Autorità Garante, il Provvedimento del 17 gennaio 2008, ai sensi del comma 5 dell'art. 132, che nulla osti ormai alla piena operatività dell'art. 132 medesimo, nell'attuale ultima versione, così come emerge dalle modifiche introdotte dal D.Lgs. n. 109/2008 (in vigore dal 3 luglio).

Ne deriva che, se come sopra descritto, l'art. 132 è diventato operativo ed è pertanto decaduta l'efficacia della proroga di cui all'art. 34 del decreto « Milleproroghe »[121], dovrebbe essere necessariamente scattato l'obbligo di cancellazione, da parte degli operatori, di tutti i dati sottoposti a conservazione per un periodo più lungo di quello stabilito rispettivamente per il traffico telefonico (ventiquattro mesi) e per quello telematico (dodici mesi).

In mancanza di tale cancellazione, il cui controllo e verifica è demandato al Garante, dovrebbe applicarsi la sanzione stabilita dal nuovo art. 162-*bis* del Codice.

Tuttavia, trattandosi dell'art. 132, l'uso del condizionale ormai è d'obbligo e la cautela appare fondata ricordando innanzitutto che il Provvedimento del 17 gennaio 2008, ha concesso termine fino al 31 ottobre 2008, agli operatori per effettuare tutti gli adempimenti indicati nella lettera *a*), fra cui figura il punto 5, riguardante le operazioni di cancellazione o anonimizzazione dei dati.

9. Il Provvedimento del Garante, del 24 luglio 2008: « recepimento normativo in tema di dati di traffico telefonico e telematico ».

A seguito delle modifiche introdotte con la L. 48/2008 e con il D.Lgs. 109/2008, il Garante ha emesso un Provvedimento « correttivo » di quello del 17 gennaio 2008[122], con cui:

— ha dato atto delle avvenute modifiche alla normativa vigente in materia;

— ha apportato le correzioni necessarie per coordinare le prescrizioni ivi contenute con il nuovo assetto dell'art 132, eliminando la doppia fina-

[119] Art. 6, comma 4 del D.Lgs. n. 109/2008.

[120] D'altra parte sarebbe stato difficile qualificare come « circostanza particolare » la abnorme ma perenne lunghezza dei tempi della giustizia italiana.

[121] Quindi ha perso efficacia il termine di sospensione stabilito dall'art. 6, comma 1, del decreto « Pisanu » e tutte le conseguenze in esso disciplinate.

[122] Provvedimento 24 luglio 2008 in *G.U.* n. 189 del 13 agosto 2008.

lità di conservazione ed il doppio binario di tempistica, con le relative diverse misure di sicurezza;

— ha consentito che le procedure di *strong authentication*[123] siano realizzate sia con procedure integrate nelle applicazioni informatiche con cui vengono trattati i dati di traffico, sia con procedure per la protezione delle singole postazioni di lavoro, che si integrino alle funzioni di autenticazione proprie dei sistemi operativi utilizzati, a certe condizioni;

— ha opportunamente puntualizzato[124] che le misure di sicurezza, stabilite dal Provvedimento, devono essere adottate anche nei casi di conservazione temporanea dei dati relativi al traffico telematico, disciplinati dal nuovo comma 4-*ter*, dell'art. 132, introdotto dalla L. 48/2008;

— in accoglimento delle richieste avanzate dagli operatori, ha prorogato al 30 aprile 2009, i termini per l'attuazione di tutti gli adempimenti stabiliti dal Provvedimento (quindi anche quelli di cui al punto *a*) indicati al paragrafo precedente), ad eccezione delle procedure di strong authentication per gli incaricati che accedono ai dati nell'ambito dell'attività di call center, che è stata prorogata al 30 giugno 2009.

Quest'ultima proroga, concessa dal Garante, ha reso palese il fatto che gli operatori, destinatari dell'obbligo di conservazione, non erano evidentemente ancora pronti ed in grado di implementare le proprie infrastrutture, dal punto di vista tecnico ed organizzativo, in modo conforme alle misure di sicurezza prescritte, ivi incluse probabilmente le operazioni di cancellazione ed anonimizzazione dei dati di traffico.

10. La proroga del D.L. n. 151/2008.

A « risolvere » temporaneamente la questione, che rischiava di diventare abbastanza « imbarazzante » anche per l'Autorità (preposta al controllo), è intervenuto il legislatore, con l'ennesima proroga, entrata in vigore il giorno in cui (2 ottobre) sarebbero divenuti efficaci, per gli operatori, anche gli obblighi di fornire indirizzi di protocollo Internet univoci e di cancellare i dati relativi alle chiamate senza risposta entro 30 giorni. Il D.L. 2 ottobre 2008 n. 151[125] tuttavia, va ben oltre e reca modifiche sostanziali all'art. 6 del D.Lgs. 109/2008, nei seguenti termini:

— l'entrata in vigore dell'obbligo di cancellazione delle chiamate senza risposta, entro 30 giorni, viene posticipata al 31 dicembre 2008 (comma 3);

— l'entrata in vigore dell'obbligo di assicurare la disponibilità ed effettiva univocità degli indirizzi di protocollo Internet, viene posticipata al 31 dicembre 2008 (comma 5);

---

[123] Le procedure di *strong authentication* sono sistemi di autenticazione informatica, « ..consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, qualunque sia la modalità locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa avere luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti ». Provv. Garante punto 7.1.

[124] In conformità con le osservazioni critiche, e qui esposte al paragrafo 7.

[125] « Misure urgenti in materia di prevenzione e accertamento dei reati, di contrasto alla criminalità organizzata e all'immigrazione clandestina », in *G.U.* n. 231 del 2 ottobre 2008.

— si autorizzano gli operatori a conservare, fino al 31 dicembre 2008, i dati del traffico telematico indicati all'art. 6, comma 1, del Decreto « Pisanu », compresi quelli non ancora cancellati.

Quest'ultima disposizione risulta piuttosto « surreale », dal momento che, non solo prevede che si proceda « in deroga a quanto previsto dal medesimo comma 1 », ma riferendosi ai dati indicati nel Decreto « Pisanu », sospende di fatto, per tre mesi, l'operatività, su quel punto, del D.Lgs. n. 109/2008, consentendo la violazione delle relative disposizioni della Direttiva « Frattini », da questo recepite.

Con tale meccanismo si viene a vanificare la dettagliata individuazione delle tipologie di dati conservabili, ivi stabilita, consentendo la non cancellazione ed anzi l'ulteriore acquisizione, per altri tre mesi, di una massa di dati molto più ampia. Tutto ciò senza che l'Italia abbia inviato alcuna preventiva notifica a Bruxelles, in merito all'allungamento dei tempi di conservazione oltre i limiti comunitari.

11. Conclusioni.

Alla data di chiusura del presente lavoro quindi si può concludere paradossalmente che sia finalmente entrato in vigore l'art. 132, nell'attuale ultima versione (ad eccezione del comma 1-*bis*, che entrerà in vigore al 31 dicembre 2008), ma che la sua applicazione, per quanto concerne la conservazione dei dati di traffico telematico, risulta di fatto facoltativa, fino al 31 dicembre 2008, alla luce di quanto stabilito dal D.Lgs. 151/2008. L'unico dato certo sembra essere che la confusione giuridica continui a regnare sovrana e le circostanze fanno ritenere che non sia ovviamente ancora finita la fase di produzione normativa « a pioggia ».

Si rileva altresì che, con il recepimento della Direttiva, non si è colta l'occasione per riesaminare e correggere la disciplina introdotta dall'art. 7 del decreto « Pisanu » e dall'art. 10 della L. 48/2008 (i commi 4-*ter*, 4-*quater* e 4-*quinquies* dell'art. 132), allo scopo di riequilibrare il sistema della *data retention* e renderlo compatibile con i principi comunitari. Per quanto concerne il primo, si deve sottolineare che l'obbligo di conservazione dei dati relativi al monitoraggio delle attività dei gestori degli esercizi pubblici di telefonia e Internet (e di tutti gli altri soggetti indicati al paragrafo 3.2), sfugge completamente ai limiti stabiliti dalla Direttiva, per quanto riguarda i possibili destinatari di un obbligo di conservazione di dati, nonché all'applicazione delle misure di sicurezza stabilite dal Garante, per espressa esclusione effettuata nel Provvedimento del 17 gennaio 2008, coerentemente con tale premessa. Esso è inoltre ancora sottoposto al termine di scadenza del 31 dicembre 2008[126].

Per quanto riguarda il secondo, anche se sotto il profilo delle misure di sicurezza da applicare si è provveduto alla correzione descritta al precedente paragrafo 9, permangono interamente le osservazioni critiche svolte al paragrafo 7, sotto il profilo dei soggetti destinatari dell'obbligo.

---

[126] Come stabilito dall'art. 34 del decreto « Milleproroghe », non modificato dall'intervento del Garante (si veda nota 79). Il periodo di conservazione travalica quindi completamente i termini di 12 e 24 mesi, comunque stabiliti dalla Direttiva, ancorché per destinatari diversi.

Infine, come accennato al paragrafo 9, non si è colta l'occasione per recepire e fare chiarezza, con un provvedimento legislativo generale, in merito all'individuazione della tipologia di soggetti tenuti all'obbligo di conservazione ed alla conseguente esclusione di tutti gli altri soggetti, come pure in merito all'interpretazione del divieto di conservare il contenuto delle comunicazioni (es. dati di navigazione ecc.).

Tutte considerazioni che rendono impossibile ritenere conclusa, data la delicatezza degli interessi in gioco, l'attività di intervento del legislatore nazionale nella disciplina normativa della *data retention*, ma inducono ad auspicare vivamente l'avvio di una fase matura, progettuale e consapevolmente lungimirante, dell'attività di normazione, in materia di uso delle tecnologie in generale e di *data retention* in particolare.