

## Dovere di protezione e rispetto dei diritti civili

di Marco Bufacchi, dottore in Giurisprudenza

La recente pubblicazione del decreto legge 30 dicembre 2008, n. 207<sup>1</sup> recante “*Proroga di termini previsti da disposizioni legislative e disposizioni finanziarie urgenti*” (c.d. “decreto milleproroghe” 2008), con il quale vengono prorogati alcuni termini previsti da disposizioni legislative<sup>2</sup>, ci spinge a due brevi riflessioni sul tema della *privacy* e della libera diffusione delle reti *wi-fi* in Italia, in quanto, con l’art. 11 del decreto citato, rubricato “*Contrasto al terrorismo internazionale*”, è stata inserita un’ulteriore dilatazione<sup>3</sup> dei tempi relativi agli obblighi derivanti dalla disciplina amministrativa degli esercizi pubblici di telefonia e *Internet*. Infatti, l’art. 7 del c.d. “decreto Pisanu”<sup>4</sup>, prescrive, per chi offra un servizio di accesso a *Internet* in un pubblico esercizio o in un circolo privato, di registrarsi presso la Questura, di tenere un registro dei dati dei propri clienti e/o soci che si connettano a *Internet* con l’obbligo di identificare in modo certo gli utenti della proprio *network*, nonché di conservare i dati sul traffico telematico che abbiano effettuato durante la navigazione *Internet* (cioè i cosiddetti “*file di log*” relativi ai dati esterni alle comunicazioni<sup>5</sup>). Prima di proseguire nel nostro approfondimento, cerchiamo, parimenti, di affrontare il quadro che ha interessato la mutevole materia della conservazione dei dati del traffico telefonico e telematico

---

<sup>1</sup> Pubblicato in *GU n. 304 del 31-12-2008* ed entrato in vigore lo stesso giorno della sua pubblicazione. In data 7 gennaio 2009, è stato presentato il relativo DDL di conversione con [atto Senato n. 1305](#) e assegnato alla 1ª Commissione permanente (Affari Costituzionali) in sede referente l’8 gennaio 2009.

<sup>2</sup> In materia di difesa, riforme per il federalismo, beni e attività culturali, lavoro, salute, università, infrastrutture e trasporti, pubbliche amministrazioni, agricoltura e pesca, sviluppo economico, affari esteri e interno.

<sup>3</sup> All’articolo 7, comma 1, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, le parole: «fino al 31 dicembre 2008» sono sostituite dalle seguenti: «**fino al 31 dicembre 2009**».

<sup>4</sup> Decreto legge 27 luglio 2005, n. 144 recante “*Misure urgenti per il contrasto del terrorismo internazionale*” (c.d. “decreto Pisanu”).

<sup>5</sup> E quindi non ai loro contenuti.

negli ultimi anni. In particolare, il combinato dell'art. 132 del Codice della *privacy*<sup>6</sup> e dell'art. 6 del “decreto Pisanu”, dispone l'obbligo di conservazione del traffico telefonico o telematico in capo agli *Internet Service Provider* (I.S.P.), ai fornitori di rete o di altri servizi di telecomunicazioni offerti al pubblico. Al riguardo, si evidenzia come già l'art. 34<sup>7</sup> del decreto legge 31 dicembre 2007, n. 248 (c.d. “decreto milleproroghe” 2007 convertito, con modificazioni, dalla legge n. 31/2008) aveva prorogato<sup>8</sup> gli obblighi di detta conservazione “*fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE<sup>9</sup> del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008*”<sup>10</sup>. A seguito del recepimento nell'ordinamento italiano<sup>11</sup> della richiamata direttiva europea 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, sono state, altresì, individuate le “categorie di dati da conservare”<sup>12</sup>. Il richiamato D.lgs., con l'art. 2, ha novellato l'art. 132 del Codice della *privacy*, modificando in tal modo i tempi di conservazione del traffico telefonico e telematico, rispettivamente in “ventiquattro mesi dalla data della comunicazione” e “dodici mesi dalla data della comunicazione”.

---

<sup>6</sup> D.gs. n. 196/2003 e successive modifiche e integrazioni.

<sup>7</sup> Recante “*Proroghe in materia di contrasto al terrorismo internazionale*”.

<sup>8</sup> In concomitanza con la scadenza del 31 dicembre 2007 prevista originariamente dalla normativa d'urgenza dettata con il citato decreto Pisanu.

<sup>9</sup> Meglio nota come “*direttiva Frattini*” relativa alla c.d. “*data retention*”.

<sup>10</sup> Pertanto sino a tale data, non potevano essere cancellati i richiamati dati relativi al traffico telematico.

<sup>11</sup> Con il D.lgs. 30 maggio 2008, n. 109, recante “*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*” (pubblicato in *G.U. n. 141 del 18 giugno 2008*).

<sup>12</sup> Art. 3, D.lgs. n. 109/2008.

Il citato D.lgs. n. 109/2008 di recepimento, è stato a sua volta recentemente modificato dal decreto legge 2 ottobre 2008, n. 151<sup>13</sup>, che, con l'art. 1 rubricato "*Modifiche al decreto legislativo 30 maggio 2008, n. 109*", ha prorogato gli obblighi di conservazione, in capo ai fornitori di servizi di telecomunicazione, dei dati del traffico telematico di cui al "decreto Pisanu", fino al 31 marzo 2009 "compresi quelli non cancellati".

Al quadro delineato, per completezza, devono ricordarsi le modifiche introdotte con la recente legge di ratifica<sup>14</sup> alla "*Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001*". Infatti, l'art. 10 di tale ratifica, ha inserito i commi 4 *ter*, 4 *quater* e 4 *quinqüies* all'articolo 132 del Codice della *privacy*. Con tali commi, vengono apportate rilevanti modifiche inerenti tra l'altro:

- l'attribuzione al Ministro dell'Interno<sup>15</sup> del potere di disporre la conservazione<sup>16</sup> d'urgenza dei dati relativi al traffico telematico, subordinando l'efficacia del provvedimento alla convalida entro 48 ore da parte del pubblico ministero;
- le misure di sicurezza ai fini della protezione dei dati da conservare da parte dei fornitori e degli operatori di servizi informatici o telematici, secondo le modalità indicate.

I passaggi sin qui ripercorsi, mostrano una situazione *in fieri* che impone delle riflessioni su come in Italia, la possibilità di promuovere

---

<sup>13</sup> Recante "*Misure urgenti in materia di prevenzione e accertamento dei reati*" (pubblicato in *G.U. n. 231 del 2 ottobre 2008*) convertito, con modificazioni, dalla legge 28 novembre 2008, n. 186 (pubblicata in *G.U. n. 281 del 1° dicembre 2008*).

<sup>14</sup> Legge 18 marzo 2008, n. 48 recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" (pubblicata in *G.U. 4 aprile 2008, n. 80, Supplemento ordinario n. 79*).

<sup>15</sup> 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.

<sup>16</sup> Secondo la dizione della norma, non si tratterebbe di una misura che stabilisce un potere di "acquisizione" al di fuori di quanto previsto dal primo comma dell'art 132 citato, bensì un potere meramente di "conservazione e protezione del dato" e tra l'altro con scadenza variabile dai 90 giorni fino ad un massimo di 6 mesi. Inoltre, tale potere di ordinare la "conservazione e protezione" agli operatori di servizi informatici e telematici, sarebbe esperibile da parte dei soggetti appositamente individuati (comma 4 *ter*, art. 132 Codice *privacy*), anche a seguito di richiesta avanzata da parte di autorità investigative straniere.

iniziative costituite dalla realizzazione di accessi *Internet* pubblici gratuiti, sia subordinato all'iniziativa delle Pubbliche Amministrazioni<sup>17</sup>, supportando gli onerosi costi di identificazione degli utenti tramite un *server* centralizzato.

La dicotomia intercorrente tra il dovere di protezione da parte dello Stato e il diritto dei cittadini a vedersi garantite le proprie libertà personali, andrebbe affrontata considerando il ruolo di strumento attraverso il quale disegnare idealmente un confine tra se stesso e gli altri, che racchiuda quell'esigenza naturale degli individui ad avere un personalissimo spazio fisico di solitudine.

La crescente attività di produzione degli organismi posti dagli ordinamenti a tutela della sfera personale degli individui, ha fatto sì che la *privacy* si affermasse come diritto fondamentale oggi riconosciuto e tutelato nei Paesi dell'Unione Europea nonché nella maggior parte delle società in cui vigano sistemi democratici. Il suo riconoscimento come posizione giuridica rilevante è, invero, frutto di una stratificazione concettuale avvenuta nel tempo e dettata dalla necessità di valicare il semplice diritto di proprietà e la sua più intuitiva e primitiva proiezione mentale, ovvero il diritto a non vedere "invasa"<sup>18</sup> la propria sfera personale da soggetti estranei. Nel corso di più di un secolo, essa ha mostrato una natura multiforme, poliedrica, capace di modellarsi in relazione all'evoluzione dei costumi ed al frenetico progresso tecnologico.

E la strada da percorrere, come direbbe Dante, ... sembra ancora "irta di ostacoli e ardua da attraversare" !

---

<sup>17</sup> Si veda ad esempio il progetto *wi-fi* della Provincia di Roma, che, il mese ultimo scorso, ha avviato un'iniziativa finalizzata alla diffusione di connessioni gratuite ad *Internet* presenti su Roma e sui comuni della provincia.

<sup>18</sup> Il c.d. "*right to be let alone*", così come definito dal giudice americano Cooley, grazie anche alla originale giurisprudenza nord-americana, è divenuto "*one theme that pervades the entire constitutional structure*".