Innovazione a ostacoli: una questione di proroga

di Marco Bufacchi, dottore in Giurisprudenza

In una riflessione[1] nell'ambito della proroga di termini previsti da disposizioni legislative, erano state affrontate talune problematiche relative alla *privacy* nonché alla libera diffusione delle connessioni *wi-fi* in Italia. Al riguardo, si torna ad approfondire tali aspetti in ragione del recente Consiglio dei Ministri n. 76 del 17/12/2009[2], che ha approvato un provvedimento contenente, tra l'altro, una protrazione del termine per munirsi della licenza del Questore per l'apertura dei cosiddetti "*internet points*", *limitando gli adempimenti a carico dei gestori*. A seguito della deliberazione del citato Consiglio dei Ministri è stato emanato il decreto legge 30 dicembre 2009, n. 194[3] (c.d. "decreto mille proroghe" 2009), recante "*Proroga di termini previsti da disposizioni legislative*" convertito, con modificazioni, dalla legge 26 febbraio 2010, n. 25[4].

L'art. 3[5], comma 1, di detto decreto, prevede in particolare che "*al comma 1 dell'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, le parole: «fino al 31 dicembre 2009» sono sostituite dalle seguenti: «fino al 31 dicembre 2010»*". Un comma quest'ultimo[6] che, dopo la sua introduzione nel 2005, è stato novellato sistematicamente:

- dall'art. 34 del decreto legge 31 dicembre 2007, n. 248;
- dall'art. 11 del decreto legge 30 dicembre 2008, n. 207;
- da ultimo, dal comma 1 dell'art. 3 del richiamato decreto legge n. 194/2009.

Da una prima lettura della norma, preliminarmente si rileva come, se da un

[1] "***Dovere di protezione e rispetto dei diritti civili***", su: http://www.contabilita-pubblica.it/Archivio09/Dottrina/Articolo%20A&C.pdf, gennaio 2009.
[2] Su http://www.governo.it/Governo/ConsiglioMinistri/testo_int.asp?d=53740.
[3] Pubblicato nella *Gazzetta Ufficiale 30 dicembre 2009, n. 302*.
[4] Pubblicata nella *Gazzetta Ufficiale 27 febbraio 2010, n. 48 - Supplemento ordinario n. 39*.
[5] Rubricato "*Proroga di termini in materia di amministrazione dell'interno*".
[6] Comma 1, art. 7 del decreto legge n. 144/2005.

lato viene prorogato al 31 dicembre 2010 l'obbligo della richiesta di licenza al Questore per chi offra un servizio di accesso a *Internet* in un pubblico esercizio o in un circolo privato, dall'altro non sembrano rinvenirsi *ictu oculi* i dichiarati "adempimenti limitati a carico dei gestori" del servizio di connettività in esame[7].

Numerose sono state le osservazioni volte all'opportunità di rimuovere gli oneri previsti. Infatti, soprattutto gli oneri causati dall'obbligo di identificare i fruitori del servizio di accesso a *Internet*, si sono tramutati in un forte disincentivo a realizzare reti *wi-fi* aperte[8].

Ciò posto, le misure rappresentate dalla licenza del Questore, dall'identificazione a mezzo documento di identità nonché dall'attività di *logging*, non sempre hanno sortito, alla prova dei fatti, l'effetto sperato. Ne sono riprova le continue omissioni da parte degli esercenti in ordine sia all'identificazione, sia, in particolare, al *logging*[9].

La disposizione prorogata, che incide sulla regolamentazione dell'accesso alla connettività messa a disposizione da locali pubblici e circoli privati, non appare considerare la possibile attività di sfruttare impropriamente detta connettività e attribuire la responsabilità della condotta telematica a un qualsiasi soggetto che lasci inconsapevolmente "aperta"[10] (*rectius*: non protetta) la propria rete *wi-fi*. In tale prospettiva, la vera questione da affrontare sarebbe quella più generale dell'imputabilità ad un determinato soggetto di talune condotte telematiche di particolare rilievo giuridico. Si tratta, peraltro, di una

[7] Come riportato nel comunicato stampa del Consiglio dei Ministri n. 76 del 2009 citato.
[8] LA CARTA DEI CENTO PER IL LIBERO *WI-FI*, su: http://gilioli.blogautore.espresso.repubblica.it/2009/11/26/la-carta-dei-cento-per-il-libero-wi-fi.
[9] A titolo esemplificativo si veda: http://www.sienafree.it/index.php?option=com_content&view=article&id=6819:licenza-sospesa-per-15-giorni-ad-un-internet-point-di-siena&catid=142:siena&Itemid=198.
[10] Ossia mantenendo le impostazioni predefinite senza configurare le misure di protezione di cui tutti i dispositivi *wi-fi* sono dotati. In ipotesi di accesso e sfruttamento della rete *wi-fi*, la responsabilità penale rileva, seppur in diverso modo, a seconda dell'attività posta in essere dal soggetto. Se la rete è aperta (non protetta) il soggetto agente potrà andare incontro alle sanzioni previste dal codice penale. In questo caso, considerata la libertà di accesso alla rete, non si potrà configurare il reato di accesso abusivo a sistema informatico o telematico in quanto la stessa rete non prevede misure di sicurezza attive (art. 615 *ter* c.p.), mentre a seconda dell'ulteriore attività posta in essere una volta entrato nella rete le ipotesi di reato configurabili possono essere molteplici. Ma il problema principale, in tali casi, risiede evidentemente nella concreta possibilità di individuare il reale soggetto a cui ricondurre la condotta illecita (Cassazione penale, Sez. V, Sent. n. 37322 del 08-07-2008, ud. del 08-07-2008, S.R. c/ B.P.).

raccomandazione emersa in seno allo stesso Consiglio dell'Unione europea[11], che ha evidenziato l'esigenza di definire il problema della natura anonima dei servizi di telecomunicazione prepagati.

Per quanto concerne, poi, la problematica sulla conservazione dei dati[12] (i c.d. *file* di *log*) del traffico telefonico[13] e telematico[14] da parte dei fornitori di servizi di telecomunicazione, si rileva che l'ultimo intervento normativo in materia[15] è stato rappresentato dall'art. 2 del decreto legge 2 ottobre 2008, n. 151[16] (c.d. "decreto mille proroghe" 2008) recante "*Misure urgenti in materia di prevenzione e accertamento dei reati*" convertito, con modificazioni, dalla legge 28 novembre 2008, n. 186[17].

Pertanto, allo stato, i dati di traffico telefonico e telematico non sono soggetti a conservazione oltre i termini previsti dal vigente art. 132 del Codice della *privacy*, neanche nel caso in cui ricorrano i presupposti di sicurezza di cui al "decreto Pisanu".

La stessa Autorità garante per la protezione dei dati personali, nella *newsletter* n. 335 del 1° marzo u.s.[18], ha comunicato il divieto in capo a tre società che operano nel settore della telefonia e *Internet* dell'uso di dati trattati in modo illecito ordinandone la cancellazione. In particolare, il Garante ha

[11] Su http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2297.

[12] Attualmente disciplinata unicamente dall'art. 132 (rubricato "*Conservazione di dati di traffico per altre finalità*") del Codice in materia di protezione dei dati personali in quanto l'art. 6 del c.d. "decreto Pisanu" – che disponeva lo straordinario 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 – non esplica più i suoi effetti a partire dal 01/04/2009.

[13] Ai sensi dell'art. 132 del Codice in materia di protezione dei dati personali, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, esclusi comunque i contenuti delle comunicazioni.

[14] Ai sensi dell'art. 132 del Codice in materia di protezione dei dati personali, i dati relativi al traffico telematico sono conservati dal fornitore per dodici mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, esclusi comunque i contenuti delle comunicazioni.

[15] Se si esclude il differimento (comunque non oltre il 31/12/2010) - relativo all'obbligo di rendere disponibili i dati delle "chiamate senza risposta" generate dai clienti collegati alle reti fisse di nuova generazione in tecnologia IP (VoIP) - disposto dall'art. 12 *ter* (rubricato "*Categorie di dati da conservare di cui all'articolo 3 del decreto legislativo 30 maggio 2009, n. 108*") del decreto legge 23 febbraio 2009, n. 11, come inserito dalla legge di conversione 23 aprile 2009, n. 38 concernente "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*". Il comma 2 del medesimo articolo ha previsto l'obbligo per gli operatori di rete mobile di rendere disponibili detti dati a decorrere dal 31 dicembre 2009.

[16] Pubblicato nella *Gazzetta Ufficiale 2 ottobre 2008, n. 231*.

[17] Pubblicata nella *Gazzetta Ufficiale 1° dicembre 2008, n. 281*.

[18] http://www.garanteprivacy.it/garante/doc.jsp?ID=1695856.

evidenziato le gravi violazioni emerse nel corso degli accertamenti ispettivi effettuati, consistenti nei tempi di conservazione dei dati di traffico telefonico e telematico oltre i limiti consentiti nonché nella conservazione di informazioni sui siti *web* visitati dagli utenti.

I continui contrasti relativi alla mutevole materia della *data retention*, non risultano investire il solo territorio nazionale. Le Corti costituzionali degli Stati democratici, e la stessa Corte di giustizia dell'Unione europea, sono chiamate sempre più spesso a stabilire, nei casi specifici a loro sottoposti, la linea di confine tra limitazioni dei principi e dei diritti fondamentali costituzionalmente protetti che appaiono accettabili alla luce delle esigenze di tutela della sicurezza esterna ed interna degli Stati medesimi, nonché vere e proprie violazioni di tali principi e diritti. In questo contesto si inserisce la recente[19] decisone della Corte costituzionale federale tedesca[20], con cui è stata dichiarata incostituzionale la normativa che ha recepito, in Germania, la Direttiva europea 2006/24/CE[21] (c.d. "Direttiva Frattini"). L'Alto consesso tedesco, non ha inteso porre in discussione *tout court* il recepimento della stessa Direttiva europea, bensì le modalità con cui essa è stata introdotta nell'ordinamento interno della Germania[22].

Tale decisione, invero, potrebbe essere gravida di conseguenze anche in ambito comunitario. Il problema dell'articolato bilanciamento tra interessi individuali e collettivi potenzialmente in conflitto - ma che, ad un esame più approfondito, si presentano necessariamente come complementari - rimane aperto, aspettando la prossima proroga!

---

[19] Comunicato stampa in data 2 marzo 2010 su : http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-008.html.

[20] Su http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html; al riguardo si veda un'ulteriore innovativa decisione della stessa Corte, su : http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=601.

[21] 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. Ai sensi dell'art. 6 della citata Direttiva europea, la Germania aveva provveduto alla conservazione dei dati relativi al traffico telefonico e telematico per sei mesi dalla data della comunicazione e a renderli disponibili in caso di richiesta dell'Autorità giudiziaria.

[22] La richiamata Corte tedesca ha stabilito che la conservazione indiscriminata dei dati di traffico dei cittadini si pone in contrasto con la costituzione tedesca, stabilendone l'immediata cancellazione. Quello della riservatezza delle comunicazioni rappresenta, secondo quanto affermato, un diritto costituzionalmente garantito, e la *data retention* così dispiegata non sembra potersi conciliare con lo stesso.