Quel pasticcio brutto sulla data retention

Date : 7 settembre 2017

Lo scorso fine luglio è stata sollevata - invero esclusivamente da esperti del settore - un po' di bagarre dopo che la Camera dei Deputati, all'interno del disegno sulla legge europea 2017 (C. 4505-A) ed in calce ad una disposizione relativa alla sicurezza degli ascensori, ha approvato un emendamento (art.12 *ter*), proposto alla spicciolata dall'on. Verini, che estende a 6 anni la durata della conservazione dei dati del traffico telefonico e telematico per finalità di contrasto al terrorismo.

Il provvedimento è in attesa di essere, alla ripresa dei lavori parlamentari dopo la pausa estiva, esaminato in Senato.

Per meglio comprendere le ragioni per cui tale emendamento non può che essere additato come un pessimo intervento normativo, pare opportuno (ri)mettere alcuni paletti alla materia del contendere, ovverosia a quella che viene sinteticamente definita data retention.

Quali sono i dati soggetti a retention?

Con data retention si intende l'obbligo di conservazione imposto per legge ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione dei dati (*rectius*, dei metadati) di traffico telefonico e telematico dei loro utenti e/o abbonati.

Il primo nodo da sciogliere riguarda non tanto la definizione di dato di traffico quanto le categorie di dati di cui la legge impone ai gestori di servizi di telecomunicazione la conservazione.

È un passaggio importante perché, se è vero che i tempi di conservazione sono un argomento delicato in termini di potenziale lesione di diritti fondamentali, altrettanto può dirsi anche con riferimento all'individuazione dei dati che debbono essere sottoposti a retention.

L'art.4, 2° co., lett. h), del codice privacy stabilisce che è dato relativo al traffico " *qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente*".

Il D. Lgs. 109/2008, in attuazione della direttiva 2006/24/CE (c.d. Direttiva Frattini, di cui si parlerà nel proseguo), specifica che con la locuzione “traffico telefonico” si debbano intendere le chiamate telefoniche (incluse le chiamate vocali, di messaggeria vocale, in conferenza e quelle basate sulla trasmissione dati, purché fornite da un gestore di telefonia), i servizi supplementari (inclusi l'inoltro e il trasferimento di chiamata), la messaggeria e i servizi multimediali (inclusi i servizi di messaggeria breve, servizi mediali avanzati e servizi multimediali), mentre non prevede cosa si intenda per “traffico telematico”.

Sono considerati dati di traffico anche le chiamate senza risposta.

Non sono dati di traffico, ma rientrano comunque negli obblighi di conservazione, i dati di ubicazione con cui si intende (art.4, lett. i, codice privacy) “*ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude*”.

Il decreto 109/08 specifica in modo puntuale le categorie di dati da conservare, che sono:

- i dati necessari per rintracciare e identificare la fonte di una comunicazione (tra cui numero telefonico, nome dell’utente o dell’abbonato chiamante, indirizzo IP per accesso ad internet, indirizzo di posta elettronica, indirizzo IP e nome a dominio del mail exchenger host, etc.);
- i dati necessari per rintracciare e identificare la destinazione di una comunicazione (come sopra, ma riferito all’utente chiamato);
- i dati necessari per determinare la data, l'ora e la durata della comunicazione;
- i dati necessari per determinare il tipo di comunicazione (servizio telefonico e protocolli dei servizi internet utilizzati);
- i dati necessari per determinare le attrezzature di comunicazione degli utenti chiamanti e chiamati (IMSI - International Mobile Subscriber Identity e IMEI - International Mobile Equipment Identity);
- i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile (cell ID e ubicazione geografica della cell ID).

Dunque, non solo vengono conservati i metadati di traffico telefonico e telematico in senso stretto, ma anche i dati relativi all’identificazione dell’utente, i dati di localizzazione, nonché i dati identificativi dei device (IMEI) e delle SIM card (IMSI) utilizzati: una ingente mole di informazioni che può riguardare un soggetto in particolare, nell’ipotesi in cui l’autorità giudiziaria chieda i dati relativi ad uno specifico indagato, oppure un numero indeterminato di persone, allorquando, ad esempio, all’operatore telefonico vengono chiesti tutti i dati, compresi IMSI ed IMEI, dei cellulari agganciati ad una determinata cella telefonica (*rectius* una stazione radio base -BTS), in un determinato giorno ed orario.

La normativa di riferimento

Agli inizi del nuovo millennio, in concomitanza con la diffusione dei contratti telefonici *flat* che comportarono una radicale diminuzione, se non l’assoluta irrilevanza, della conservazione dei

dati di traffico a fini di fatturazione, in attuazione della direttiva 2002/58/CE (c.d. direttiva e-privacy), veniva introdotto l'art. 132 del codice privacy che, nella sua versione originale, imponeva *ex lege* alle TELCO la retention per finalità di accertamento e repressione di reati solamente dei dati di traffico telefonico. Il tempo massimo di conservazione, inizialmente indicato in trenta mesi, nel dicembre 2003 veniva ridotto a ventiquattro mesi, prorogabili di ulteriori ventiquattro per le indagini volte all'accertamento ed alla repressione dei delitti di cui all'art. 407, 2° co., lett. a), c.p.p.

Il D.L. 27 luglio 2005, n.144, convertito con modificazioni nella L. 31 luglio 2005, n.155 (c.d. decreto Pisanu), sotto l'egida della lotta al terrorismo, sottoponeva all'obbligo di retention anche i dati di traffico telematico e le chiamate senza risposta (in ragione del fatto che la bomba dell'attentato di Madrid era stata innescata proprio con una chiamata senza risposta), prevedendo due diversi regimi temporali di conservazione: ventiquattro mesi, prorogabili di ulteriori ventiquattro, per i dati di traffico telefonico e sei mesi, prorogabili di altri sei, per dati di traffico telematico. Il decreto stabiliva inoltre, contrariamente a quanto originariamente previsto, che l'acquisizione dei dati potesse essere disposta con semplice decreto motivato del pubblico ministero anziché del giudice per le indagini preliminari.

Lo stesso decreto, infine, contestualmente alla previsione di tali termini, disponeva la sospensione dell'obbligo di cancellazione dei dati alla naturale scadenza per ragioni emergenziali cosicché, in Italia, come denunciato dal Garante privacy (in allora nella persona del prof. Rodotà), si giunse a conservare i dati per ben otto anni.

Nel 2006, a livello europeo, veniva emanata la direttiva 2006/26/CE (c.d. direttiva Frattini) volta a disciplinare specificamente la materia e che vincolava gli Stati membri a definire il periodo di conservazione in un tempo non superiore a due anni dalla data della comunicazione.

In attuazione di tale direttiva veniva emanato il già citato D. Lgs. 109/2008, il quale modificava nuovamente l'art.132 del codice privacy stabilendo un termine di conservazione di 24 mesi per i dati di traffico telefonico, di 12 mesi per il traffico telematico e di 30 giorni per le chiamate senza risposta.

La direttiva sulla data retention, considerata la tragica situazione nostrana, veniva accolta con grande favore in Italia in quanto finalmente veniva fissato un tetto massimo inderogabile di conservazione in ventiquattro mesi.

Molto diversa, invece, la sensibilità di altri Stati membri, che sin da subito considerarono la direttiva lesiva dei diritti umani fondamentali, tanto che le Corti costituzionali rumena (nel 2009), tedesca (nel 2010) e ceca (nel 2011) dichiararono incostituzionali le rispettive leggi nazionali di recepimento.

La direttiva Frattini veniva anche sottoposta al vaglio della Corte di Giustizia dell'Unione europea: una prima volta su ricorso (respinto) dell'Irlanda che lamentava la violazione dell'art.95 del Trattato in quanto, pur essendo formalmente volta all'armonizzazione del mercato interno, la direttiva di fatto era stata emanata, in un'epoca pre-Lisbona, al solo scopo di assicurare alle autorità pubbliche dati che altrimenti avrebbero dovuto essere cancellati - ed

una seconda volta, su ricorso di Digital Rights Ireland Ltd. che ha portato, nel 2014, ad un intervento giurisprudenziale senza precedenti.

Le sentenze CGUE dell'8 aprile 2014 e del 21 dicembre 2016 e le successive norme antiterrorismo

Con sentenza 8 aprile 2014, infatti, la Corte di Giustizia dell'Unione europea, con una storica decisione, ha dichiarato invalida l'intera direttiva Frattini.

Nelle motivazioni della sentenza si legge che la direttiva è invalida in quanto legittima la sorveglianza di massa, ipotesi che non può essere avallata in una società democratica.

Non solo. Il fatto che le comunicazioni elettroniche coinvolgano la stragrande maggioranza dei cittadini europei e la circostanza che la retention avvenga *ex lege* e dunque senza il consenso dell'interessato, ad avviso della Corte, genera nelle persone la sensazione che la loro vita privata sia continuamente monitorata con conseguente inibizione dei loro comportamenti abituali, specie considerando che i metadati di traffico possono rivelare informazioni sulla vita privata delle persone anche più precise ed intime del contenuto delle comunicazioni stesse.

Giuridicamente parlando, la CGUE ha ravvisato una violazione del principio di proporzionalità tra l'interesse perseguito (sicurezza) ed diritti fondamentali lesi (privacy e data protection) in quanto la retention prevista dalla direttiva è indiscriminata (prescinde da specifiche necessità di indagine su specifici soggetti riguardando in modo indifferenziato tutti i cittadini), che non vengono indicate le autorità che possono avere accesso ai dati, né le modalità di accesso, che non vengono individuati i "gravi reati" che legittimerebbero la retention, che non vengono giustificati i tempi di conservazione (da 6 a 24 mesi) e, infine, che non è previsto che i dati siano conservati nell'Unione europea.

Alla luce di tale pronuncia, parecchi Stati membri hanno sospeso l'applicazione o dichiarato incostituzionali le rispettive leggi nazionali di recepimento della direttiva.

Ma non l'Italia la quale, anzi, con l'art.4-*bis* del D.L. 7/2015 (c.d. decreto antiterrorismo) ha stabilito, come già aveva fatto il decreto Pisanu, un obbligo di conservazione generalizzata di tutti i meta-dati fino al 31 dicembre 2016, termine successivamente prorogato al 30 giugno 2017, non solo nonostante l'annullamento della direttiva Frattini ma anche in spregio di quanto stabilito dalla successiva sentenza della Grande Sezione della CGUE del 21 dicembre 2016 (c.d. sentenza Tele 2).

In tale procedimento sono, infatti, state sollevate innanzi alla Corte di Lussemburgo due questioni pregiudiziali sull'interpretazione da dare all'articolo 15 della direttiva 2002/58/CE il quale consente agli Stati membri di derogare al principio di riservatezza per adottare misure necessarie, opportune e proporzionate, in una società democratica, per la salvaguardia di alcuni rilevanti interessi, fra cui la sicurezza dello Stato, articolo su cui Regno Unito e Svezia fondavano la loro normativa interna afferente alla conservazione generalizzata dei dati di traffico e ubicazione degli abbonati a servizi di comunicazione elettronica.

La sentenza chiude il cerchio lasciato aperto due anni prima (caduta la direttiva Frattini, la base legale di riferimento per un'eventuale normativa in materia di data retention poteva infatti essere rinvenuta nell'art.15 della direttiva e-privacy), ribadendo che una raccolta indiscriminata di dati non è compatibile con la normativa comunitaria, in particolare i diritti fondamentali di riservatezza e data protection tutelati dagli artt.7 e 8 della Carta del diritti fondamentali UE.

Il termine del 30 giugno 2017 previsto dal D.L. 7/2015 non è stato ulteriormente prorogato per cui dal 1° luglio, in Italia, da un lato è tornata in vigore la retention ordinaria prevista dall'art.132 del codice privacy (come modificato dalla legge di attuazione della direttiva Frattini), dall'altro gli operatori dovrebbero (il condizionale è d'obbligo!) aver provveduto a cancellare tutti i dati più vecchi di 12 e 24 mesi, non foss'altro che per scongiurare il rischio di incorrere nelle sanzioni previste dal codice privacy per il trattamento illecito di dati personali (sul punto si vedano anche le puntuali prescrizioni in tema di cancellazione impartite alle TELCO dal Garante privacy nel provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008).

L'emendamento Verini

In questa cornice, normativamente complessa, ma ben chiara nella sua interpretazione comunitaria, si inserisce l'emendamento di cui in premessa, approvato dalla Camera in data 19 luglio 2017, il quale prevede che: "*In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficaci tenuto conto delle straordinarie esigenze di contrasto al fenomeno del terrorismo, anche internazionale, per le finalità di accertamento e repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n.?7, convertito, con modificazioni, dalla legge 17 aprile 2015, n.?43, è stabilito, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del decreto legislativo 30 giugno 2003, n. 196, in settantadue mesi*".

A parte serie perplessità di metodo (emendamento proposto in corso di seduta, inserito in calce ad una norma sulla sicurezza degli ascensori ed approvato senza alcuna discussione parlamentare), forti dubbi sulla legittimità della norma attingono il merito.

Innanzitutto, il richiamato art.20 della direttiva n.541 del 2017 prevede, in via del tutto generica, che gli Stati membri possano dotarsi di strumenti di indagine efficaci per contrastare il terrorismo, ma non vi è alcun (né potrebbe esserci dopo la sentenza della Corte di Giustizia) alcun riferimento all'eventualità di adottare misure di data retention indiscriminata.

In secondo luogo, se la finalità è quella della lotta al terrorismo, non è dato comprendere perché il testo dell'emendamento faccia riferimento ai reati di cui all'art.407, comma 2, lett. a), c.p.p. tra cui, oltre ai delitti di strage e guerra civile, sono annoverati l'associazione mafiosa ed il contrabbando dei tabacchi lavorati esteri (sic!).

In ogni caso, in merito ai gravi reati per i quali la retention sarebbe finalizzata, va detto che non esiste nessuna norma processuale che sancisca l'inutilizzabilità dei dati di traffico qualora essi siano prodotti in giudizio in procedimenti relativi a reati diversi da quelli individuati dalla legge per cui è verosimile ipotizzare che le Procure si serviranno di tali dati per qualsivoglia indagine relativa a qualsivoglia reato.

Da ultimo, pare doveroso sottolineare come l'emendamento non distingua più i dati di traffico telefonico, dai dati di traffico telematico, dalle chiamate senza risposta per cui la conservazione salirebbe a sei anni - con buona pace del tetto massimo di due anni previsto dalla peraltro invalida direttiva Frattini - indistintamente e senza giustificazione apparente per tutte le tipologie di dati.

Non a caso, sulla norma è intervenuto con fermezza il Garante privacy che ne ha immediatamente ravvisato il palese contrasto con l'ordinamento e con la giurisprudenza dell'Unione europea, sottolineando come neppure indiscusse esigenze investigative per la lotta al terrorismo possano giustificare forme di sorveglianza massiva e generalizzata.

Concludendo questa lunga disamina, l'auspicio è che in Senato questo brutto pasticcio normativo venga sottoposto ad una seria e profonda discussione politica che non si riduca alla solita, inarrestabile rincorsa al popolare vessillo della sicurezza pubblica ma tenga finalmente in debito conto la tutela dei diritti fondamentali dell'uomo.

Qualora l'emendamento venisse approvato, non ci resterebbe che sperare, come raccomandato da Privacy International in un suo recentissimo rapporto sullo stato delle legislazioni nazionali dopo la sentenza Tele 2, che siano le TELCO a farsi carico di sollevare l'illegittimità della norma rispetto agli standard europei.

A cura di: **Monica A. Senor**