La *Data retention* va in ascensore

di Lucia Scaffardi *
(28 luglio 2017)

La conservazione dei dati di traffico esterni alle conversazioni telefoniche, per finalità di lotta al terrorismo, oggetto di questa nota, richiama il tema dai significati contrapposti del contemperamento delle esigenze operative degli organi inquirenti e quello della ricerca di tutele in ambito nazionale per il diritto alla privacy "sempre più a tradizione costituzionale in ambito europeo" (O. Pollicino, M. Bassini, *La Corte di giustizia e una trama ormai nota: la sentenza tele2 sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico, in Dir. Pen. Contemp.,* 9 gennaio 2017, p. 2). Si tratta di un argomento ben noto, che ha visto l'Italia prevedere, fin dal 2003, un'apposita disciplina, contenuta nell'art. 132 del "Codice della privacy" (D.Lgs 196/2003). Detto articolo è stato, nel tempo, derogato svariate volte, a riprova di quanto sia difficile e controverso il bilanciamento tra diritto alla riservatezza e interesse collettivo alla sicurezza. Questi interventi sono stati tesi, nella stragrande maggioranza dei casi, ad ampliare il margine di operatività della norma, anche in favore del fatto che il cd. *tracing* sia strumento di particolare importanza rispetto alla risoluzione dei reati, in ispecie quelli terroristici. Insomma, l'ampliamento dei tempi di conservazione dei dati, conseguenti a momenti di particolari emergenze terroristiche, che si sono succedute purtroppo negli ultimi 15 anni nel mondo, e in Europa in modo particolare, ha determinato in Italia quello che è stato definito, in maniera assolutamente condivisibile, un "pasticcio normativo" (P. Caputo, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo,* in *Archivio Penale*, 1/2016, p.36).

Il presente scritto dà atto dei più recenti sviluppi sul tema, stigmatizzando un ultimo, purtroppo illuminante caso. Il 19 luglio scorso, infatti, durante le votazioni sul Disegno di Legge "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea 2017 – la cd. legge comunitaria 2017 - è stato approvato alla Camera dei Deputati un emendamento di particolare rilevanza (A.C. 4505-A), con una modalità che si potrebbe definire, in prima analisi, quantomeno "furtiva".

Nello specifico, gli onorevoli Verini, Berretta e Mucci hanno presentato un emendamento volto a prolungare fino a 72 mesi, ovvero sei anni, il termine di conservazione dei dati telefonici e telematici imposto ai *provider*, con un inasprimento delle regole tale da essere duramente criticata sui media (L. Vendemiale, *Lo Stato ci spia: telefoni e web saranno controllati per 6 anni*, in *il Fatto Quotidiano*, 23 luglio 2017, pagina 2/3; F. SARZANA, *6 anni! E' il termine di conservazione dei dati telefonici e telematici di tutti i cittadini appena approvato alla Camera. In una direttiva sugli ascensori*, in *il Sole 24 ore*, 21 luglio 2017) oltre ad aprire un interessante dibattito anche in rete tra esperti e giuristi.

Nel dettaglio, i tre parlamentari hanno avanzato la loro proposta emendativa prevista all'art.12-ter, che così recita: *"Art. 12-ter. – (Termini di conservazione dei dati di traffico telefonico e telematico). – 1. 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”.
Cosa ha generato una simile azione, per lo più in un contesto normativo a prima vista di dubbia opportunità? E’ necessario un breve excursus, che parte proprio da quel decreto legge n. 7 del 18 febbraio 2015 con cui il Governo aveva adottato un provvedimento in materia di lotta al terrorismo, introducendo deroghe al Codice della privacy ed in ispecie a quell'art. 132 richiamato all’inizio di questa nota. In particolare, la legge n. 43 di conversione del Decreto legge 7/2015 approvata il 17 aprile 2015, prevedeva al suo art. 4 bis (Disposizioni in materia di conservazione dei dati di traffico telefonico e telematico) che i dati relativi al traffico telefonico e telematico dovessero essere conservati sino al 31 dicembre 2016 a far data dalla entrata in vigore della legge di conversione (quindi per poco più di un anno e mezzo) e così parimenti per i dati relativi alle chiamate senza risposta. La *ratio* dell’estensione temporale rispetto alla normativa previgente, si può desumere dalle schede di lettura che accompagnavano l'atto, vale a dire “mettere a disposizione dell'autorità investigativa strumenti efficaci contro una *minaccia* (corsivo nostro), quella del terrorismo, sempre più grave ed estesa, che i mezzi informatici rendono pervasiva annullando i confini temporali e territoriali”. Questa che doveva essere dunque una limitazione temporanea della tutela della privacy nasceva a seguito della necessità e dell'urgenza di contrastare il terrorismo che nelle settimane precedenti aveva mostrato tutta la sua ferocia a Parigi con l’attacco alla redazione del settimanale satirico Charlie Hebdo.
Nel cosiddetto Decreto milleproroghe del dicembre 2015 veniva poi ulteriormente ampliato il tempo di applicazione della norma fino al 30 giugno 2017, ancora una volta senza pensare ad un intervento complessivo sulla materia, continuando ad agire in deroga a quanto previsto dal Codice e utilizzando una legge *omnibus* per incidere sui diritti individuali.
Tornando al cuore della questione, ovvero la recentissima scelta del legislatore di triplicare il periodo di conservazione dei dati telefonici per finalità di contrasto al terrorismo rispetto a quanto stabilito fino ad oggi, è evidente che tale “giro di vite” non può che derivare da una “lettura” politico-emergenziale della situazione, non ravvisandosi alcun’altra spiegazione giuridicamente sostenibile. Il 30 giugno scorso, infatti, è scaduto l’obbligo di conservazione dei dati del traffico telefonico e telematico che ritornerebbero per così dire in "modalità ordinaria" (art. 132 Codice Privacy). Ma dei due casi l'una: o l'emergenza terroristica è finita ed allora potremmo a buona ragione accettare di ritornare alla normativa pre decretazione d'urgenza, oppure la realtà che viviamo necessità di norme specifiche e ponderate: ma da quel lontano 21 aprile 2015, fino appunto al 30 giugno 2017, il legislatore nulla ha fatto per approvare una complessiva normativa in tema e si ritrova oggi ad inserire una nuova "toppa" che, come si suol dire, risulta essere "peggiore del buco".
Restando all’analisi del testo, risulta evidente da subito come vengano equiparati i dati telematici a quelli telefonici e come più volte detto, che tutti questi dati sarebbero mantenuti per 72 mesi (6 anni). Attualmente i tempi di conservazione previsti nel nostro ordinamento, regolati dal Codice della privacy, sono per il traffico telefonico di 24 mesi dalla data della comunicazione (art. 132 comma 1 del Codice della privacy) e di 30 giorni per le chiamate senza risposta (art. 132 comma 1*bis* del Codice della privacy). Diversamente, per quanto riguarda il traffico telematico, i dati possono essere conservati e quindi messi a disposizione dell’autorità giudiziaria per 12 mesi dalla data della comunicazione (art. 132 comma 1 del Codice della privacy). Se invece anche in Senato dovesse passare il recente emendamento, come opportunamente commentato, da Ugo Mattei, “le aziende saranno in possesso di una massa di dati privati enorme, che ha ovviamente un valore economico alto, visto l’uso commerciale improprio che spesso ne viene fatto e che è molto difficile da controllare. Mentre lo Stato si assicura la possibilità di fare un *profiling* dei cittadini per un periodo di una lunghezza esorbitante. Praticamente ci stanno schedando”(così riportato da L. Vendemiale, *Lo Stato ci spia: telefoni e web*

saranno controllati per 6 anni, in *il Fatto Quotidiano*, cit.).
Questa improvvisa estensione temporale, non inserita per di più in una disciplina organica della materia, è inoltre a rischio di incompatibilità con il Diritto comunitario, in quanto –come notorio –con la sentenza *Digital Rights Ireland* (Corte di Giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a.*) la Corte di Giustizia ha dichiarato invalida la Direttiva 2006/24/EC sulla *Data retention* (cd Direttiva Frattini), proprio perché prevedeva un obbligo indiscriminato di mantenimento di dati. La Corte di Giustizia fin da allora ha esplicitato chiaramente come in Europa la conservazione dei dati per fini legati alla protezione dell'ordine pubblico possa divenire eccessivo se non proporzionato al fine che si vuole raggiungere, fine che nella norma *de qua* appare identificato nell'estremamente ampia ragione "*di garantire strumenti di indagine efficaci tenuto conto delle straordinarie esigenze di contrasto al fenomeno del terrorismo"*. Il Diritto comunitario *conosce* oggi poi un nuovo tassello fondamentale in tema, rappresentato dalla sentenza *Tele2 Sverige/Watson* del 21 dicembre 2016 (Corte Giustizia UE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 e Watson*). Questa giurisprudenza ha apportato ulteriori indicazioni, spostando l'attenzione dal piano legislativo europeo a quello nazionale e determinando così una complessiva rilettura in senso garantistico del tema. Ed anche qui l'emendamento di cui si discute non sembra rispondere ai criteri richiesti soprattutto per ciò che attiene la conoscibilità dei dati trattenuti. Infatti, secondo il giudice di Lussemburgo i soggetti che vedono "scandagliati" i propri dati devono essere informati il più presto possibile (tema evidentemente assente nell'emendamento), introducendo così una sorta di obbligo di informativa - nel momento ovviamente in cui queste notificazioni non siano più suscettibili di danneggiare l'inchiesta giudiziaria - e dando in questo modo la possibilità ai singoli individui di agire nel caso si verifichi una lesione dei propri diritti fondamentali.
Come si vede, anche senza qui voler ancora una volta richiamare la lunghezza esorbitante del trattenimento del dato, a cui auspicabilmente il Senato potrà a breve porre rimedio, riducendo tale tempistica, rimangono molte e inquietanti le altre criticità aperte, dalle procedure di accesso e di acquisizione delle informazioni, all'individuazione dei "gravi" reati che sono secondo la giurisprudenza UE, presupposto oggettivo tale da giustificare l'intero procedimento di *data retention* e richiamati troppo sbrigativamente nell'emendamento.
Viene dunque a manifestarsi sempre più la necessità, a parere di chi scrive, della previsione di un organismo indipendente giurisdizionale (sull'esempio di quanto previsto e in corso di attuazione in altri ordinamenti, in Gran Bretagna o in Svizzera) che attraverso un agile *iter* "consenta comunque un accertamento concreto sulla sussistenza del reato 'presupposto', basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire *ex post*, in un lasso di tempo comunque breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici**),** purché vi sia una definizione: a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento**;** b) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del 'principio di necessità' nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità)" (R. FLOR, *Data retention ed art. 132 cod. privacy: vexata quaestio(?)*, in *Dir. Pen. Contemp.*, 29 marzo 2017).
E' di tutta evidenza, dunque, come un intervento come quello attuale e cioè la

previsione di un articolo nella legge comunitaria sia del tutto improprio se non improvvido. Auspicabile, invece, un intervento complessivo del legislatore italiano che possa porre in linea la disciplina con quanto previsto dalla giurisprudenza europea, ma soprattutto che garantisca non solo a parole, ma anche attraverso le leggi, quella lotta al terrorismo sempre più "emergenza ordinaria" delle nostre quotidianità. Non si può forse auspicare un intervento come quello svolto nelle oltre 300 pagine della nuova legge del Regno Unito, su cui per altro si sono espresse perplessità (L. Scaffardi, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato***,** in *Quad. Cost.*, 2/2017, p.412**)**, ma pretendere che un emendamento di questa importanza non sia innervato all'interno di un articolo, il 12 che riguarda appunto gli adempimenti comunitari, al cui comma precedente si parla di "Disposizioni per l'integrale attuazione della direttiva 2014/33/UE relativa agli ascensori e ai componenti di sicurezza degli ascensori nonché per l'esercizio degli ascensori" sembra più che doveroso. Inoltre questa "tecnica" legislativa porta con se anche possibili critiche in chiave di legittimità costituzionale poiché è apparsa "in contrasto con l'articolo 117, primo comma della Costituzione, in quanto la disomogeneità tra Direttiva da recepire (quella sugli ascensori) e contenuto del recepimento (la disciplina della *retention* dei dati di traffico) potrebbe porsi in contrasto con il canone di esercizio di potestà legislativa in conformità con i "*vincoli dell'ordinamento dell'Unione Europea*", oggi disciplinati sul piano interno dalla legge 234 del 2012". (L. SCUDIERO, *La Camera porta di soppiatto la Data retention a sei anni,* in *Lex Digital,* 21 luglio 2016, consultabile at http://www.lexdigital.it/2017/07/la-camera-porta-di-soppiatto-la-data-retention-a-sei-anni/).
Per concludere, certo non può essere dimenticato, al netto delle preoccupanti "originalità" del legislatore italiano, come anche quello europeo potrebbe e dovrebbe intervenire cercando di dare sempre più forma a quella necessaria politica anticrimine dell'Unione (R. FLOR, *Data retention ed art. 132 cod. privacy: vexata quaestio(?)*, cit.) che continua a trovare resistenze, ma su cui siamo chiamati a riflettere in tempi di cronicizzazione del terrorismo.

* Professoressa di Diritto pubblico comparato, Università di Parma