**Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza *Tele2 Sverige* della Corte di giustizia UE**

di Oreste Pollicino* e Giulio Enea Vigevani**
(16 gennaio 2017)

«Se gli uomini fossero angeli, nessun governo sarebbe necessario. Se gli angeli governassero gli uomini, nessun controllo – esterno o interno – sul governo sarebbe necessario. Nel prefigurare un governo di uomini nei confronti di altri uomini, questa è la difficoltà più grande: prima bisogna permettere al governo di controllare i governati, poi obbligare il governo a controllare se stesso».

È con questa celeberrima citazione di James Madison che l'Avvocato generale apre le sue conclusioni alle cause riunite C-203/15 e C-698/15, *Tele2 Sverige e Watson*, decise dalla Grande Sezione della Corte di giustizia di Lussemburgo con la sentenza del 21 dicembre 2016 in materia di conservazione di dati di traffico. Si tratta di una pronuncia di grande portata sul tema dei nostri tempi, l'equilibrio tra sicurezza pubblica e diritti individuali, *in primis* quello alla vita privata in ambito digitale.

In estrema sintesi, la Corte era chiamata da due rinvii pregiudiziali della Corte d'appello amministrativa di Stoccolma e della divisione per le cause in materia civile Corte d'appello di Inghilterra e Galles a verificare la compatibilità con il diritto dell'Unione di normative nazionali, spesso di carattere emergenziale, che impongono ai fornitori di servizi di comunicazione elettronica di conservare in maniera sistematica e continua, per un determinato periodo di tempo, i dati relativi alle comunicazioni e che prevedono l'accesso generalizzato ai dati stessi delle autorità nazionali.

La risposta è stata netta: la Grande Sezione ha stabilito che, ai sensi della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, interpretata alla luce degli artt. 7 e 8 della Carta dei diritti dell'UE, gli Stati membri non possono prescrivere un obbligo generale e indifferenziato di conservazione dei dati relativi al traffico e all'ubicazione degli utenti, in assenza del consenso degli stessi. Si può solo prevedere, a titolo preventivo, una conservazione mirata allo scopo esclusivo di combattere gravi fenomeni di criminalità, a condizione che essa sia limitata allo stretto necessario per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone implicate, nonché la durata di conservazione prevista. Inoltre, l'accesso ai dati conservati deve essere assoggettato a determinate condizioni, tra cui, in particolare, un controllo preventivo da parte di un'autorità indipendente.

Alla base del bilanciamento operato dal giudice europeo vi è proprio la grande difficoltà individuata dal padre costituente americano. Da una parte, la conservazione dei dati relativi alle comunicazioni consente «al governo di controllare i governati», mettendo a disposizione delle autorità un mezzo di indagine che presenta un'utilità certa nella lotta contro i reati gravi, e in particolare il terrorismo. Dall'altra, non può non porsi il problema dell'esigenza «di obbligare il governo a controllare se stesso», per quanto concerne sia la conservazione, sia l'accesso ai dati conservati, tenuto conto dei gravi rischi di lesione del diritto, sempre più a "trazione costituzionale" in ambito europeo, alla protezione dei dati personali.

Alla base della "difficoltà più grande", per citare ancora Madison, vi è quindi il quesito, alla base del costituzionalismo contemporaneo, su quale debba essere il punto di equilibrio tra

tutela della sicurezza pubblica, specie con riferimento all'esigenza di prevenire attacchi terroristici da una parte e protezione della privacy digitale degli utenti dall'altra.

Vi è poi un convitato di pietra che gioca un ruolo da protagonista assoluto lungo tutto il percorso argomentativo della decisione in commento. Il riferimento è alla ormai quasi leggendaria decisione dell'8 aprile 2014, nella causa *Digital Rights Ireland*, in cui la Corte di giustizia ha considerato illegittima, perché in contrasto con disposizioni della Carta dei diritti fondamentali, la direttiva Frattini del 2006 sulla *data retention*. In tale pronuncia, la Corte aveva statuito che il periodo ivi previsto di conservazione di dati per fini di prevenzione anti-terroristica era eccessivo e non proporzionato, anche per la vaghezza delle condizioni cui la possibilità di tale ulteriore conservazione era legata (su tale decisione si rinvia a L. Trucco, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. it.,* 2014, 8-9, 1850 ss., M. Rubechi, *Sicurezza, tutela dei diritti fondamentali nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 2016, 18 ss. e, se consentito, O. Pollicino, *Diritto all'oblio e conservazione di dati. la Corte di giustizia a piedi uniti: verso un "digital right to privacy"*, *in Giur. cost.*, 2014, 2949 ss.). La ragione dell'importanza della decisione del 2014 per la risoluzione del dilemma, prima richiamato, alla base della pronuncia che si commenta emerge già dai quesiti che i giudici svedesi e britannici pongono alla Corte di giustizia.

Infatti, seppure nel caso più recente oggetto diretto dell'interpretazione della Corte è una diversa direttiva, adottata nel 2002 che, con specifico riguardo al settore delle comunicazioni elettroniche prevede, in via eccezionale, la possibilità per gli stati membri di conservare dati personali degli utenti per ragioni legate alla tutela della sicurezza pubblica e alla difesa nazionale, i giudici nazionali si chiedono se una legislazione nazionale che preveda una conservazione generalizzata ed indifferenziata dei dati degli abbonati, utilizzando il margine di manovra fornito da quanto previsto dalla direttiva, appena richiamata, del 2002, si ponga o meno in contrasto con quanto affermato dalla Corte di giustizia nel 2014 nella sentenza *Digital Rights Ireland*.

La risposta della Corte non lascia spazio ad equivoci. Il margine di manovra riguardo alla conservazione dei dati che l'articolo 15 della direttiva del 2002 concede agli stati, trattandosi di una deroga al regime ordinario di tutela della riservatezza e in specie al divieto di memorizzare dati di traffico senza il consenso dell'interessato, deve essere interpretato in modo restrittivo. Altrimenti, le misure che tale disposizione autorizza a titolo di eccezione finirebbero per divenire la regola, rovesciando l'ordine di priorità indicato dal legislatore europeo e non rispettando il principio di proporzionalità che deve orientare ogni restrizione dei diritti fondamentali.

Si tratta, in altre parole, di una lettura della direttiva del 2002 alla luce non solo delle stelle comete di matrice costituzionale della Corte di giustizia in materia di protezione della privacy digitale, vale a dire gli articoli 7 ed 8 della Carta di Nizza, che tutelano, rispettivamente, riservatezza e dati personali, ma anche, e forse soprattutto, della stessa giurisprudenza, anch'essa di tono costituzionale, della Corte di giustizia, a cominciare appunto da *Digital Rights Ireland* prima richiamata.

In conclusione, però, al fine di apprezzare fino in fondo l'affondo della Corte di giustizia nella decisione che si commenta, può forse ricondursi quest'ultima ad uno "scacco matto" alla prevalenza delle ragioni di sicurezza pubblica su quelle di protezione della privacy digitale che i giudici comunitari ottengono in tre mosse.

La prima è quella che si è concretizzata nella decisione della primavera del 2014 in cui la Corte europea, come si è visto, “lava i panni sporchi in casa” ed annulla per intero la direttiva Frattini, che sacrificava la tutela dei dati personali sull’altare della lotta al terrorismo internazionale.

La seconda mossa è dell’autunno del 2015, con la altrettanto celebrata e discussa sentenza della Grande Sezione del 6 ottobre 2015 nel caso Schrems (su cui si rinvia alla nota di S. Sileoni su questa *Rivista*, 2015, 1027 ss. nonché a O. Pollicino - M. Bassini, *La Carta dei diritti fondamentali dell’Unione europea nel* reasoning *dei giudici di Lussemburgo*, in *Dir. inform. e informatica*, 2015, 741-777). In questo caso, la Corte europea si concentra sui rapporti tra Unione europea e ordinamento statunitense, pretendendo, una volta alzata, con la prima mossa, l’asticella dello standard europeo di tutela della privacy digitale, che una protezione equivalente sia fornita anche dagli USA in caso di trasferimento, in quel paese, di dati appartenenti a cittadini europei.

Infine, la terza mossa quella che qui si è commentata: non solo le istituzioni comunitarie (*Digital Rights Ireland*) e quelle statunitensi (*Schrems*) ma anche, e specialmente, i legislatori degli Stati membri dell’Unione europea hanno l’obbligo di prendere sul serio la tutela della privacy digitale,. Scacco matto, dunque, alla proiezione normativa, sempre crescente, e per certi versi comprensibile, dell’ossessione connessa alle esigenze di tutela della sicurezza pubblica, e affermazione, anche nel tempo drammatico che ci troviamo a vivere, della protezione della sfera privata degli individui come regola dello spazio costituzionale europeo.

* Professore ordinario di Diritto costituzionale – Università “Bocconi” di Milano
** Professore associato di diritto costituzionale – Università di Milano Bicocca