IL BILANCIAMENTO TRA I DIRITTI FONDAMENTALI ALLA RISERVATEZZA E ALLA PROTEZIONE DEI DATI E LE ESIGENZE DI GIUSTIZIA E DI SICUREZZA PUBBLICA NELLA DIRETTIVA 2002/58/CE

Tentiamo di verificare se la normativa nazionale dei Paesi membri dell'UE, che obbliga i fornitori di servizi di comunicazione a conservare una massa notevole di dati molto delicati, violi o meno la norma comunitaria.

Luigi MONTUORI è Direttore del Servizio relazioni comunitarie e internazionali e del Servizio segreteria del collegio del Garante della Privacy. Docente all'Università degli studi "La Sapienza", Istituto di teoria dell'interpretazione e di informatica giuridica, nel master in diritto dell'informatica e teoria e tecnica della normazione, alla università RomaTre nel Master di II livello in "*Responsabile della protezione dei dati personali: data protection officer e privacy expert*". È autore di molteplici pubblicazioni, in particolare in materia di privacy e di contrattualistica della PA.

Il dibattito sul bilanciamento tra i diritti fondamentali alla riservatezza e alla protezione dei dati personali e le esigenze di prevenzione dai gravi rischi per la sicurezza pubblica, di contrasto e repressione degli atti di criminalità grave e di **lotta contro la criminalità organizzata ed il terrorismo** ha visto oscillare l'ago della bilancia negli ultimi decenni influenzato spesso dall'emotività del momento.

Anche all'interno dell'Unione Europea le differenze delle discipline in tale settore sono marcate facendo prevalere un diritto rispetto all'altro risentendo dei differenti contesti sociali e storici dei singoli Paesi. Un esempio evidente di tale differente approccio è dato dall'obbligo in capo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di conservare i dati relativi al traffico e all'ubicazione degli utenti finali di detti servizi.

Con questo breve scritto si vuole tentare di verificare se la normativa nazionale dei Paesi membri dell'UE, che obbliga i suddetti fornitori di servizi di comunicazione a conservare una massa notevole di dati molto delicati, violi o meno la norma comunitaria che lascia un margine di flessibilità agli Stati membri, articolo 15 della direttiva 2002/58/CE. Tale norma deve essere letta alla luce degli articoli 7, 8 e 11, nonché 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, da un lato, e dell'articolo 6 della Carta medesima, nonché dell'articolo 4 del trattato sull'Unione europea.

Come sopra già detto l'art. 15, par. 1, della direttiva 2002/58/CE consente agli Stati membri di adottare normative, d'implementazione del diritto europeo, che prevedono a titolo preventivo la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità organizzata, purché tale conservazione sia "mirata" (e non ingiustificata) e limitata allo stretto necessario per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione utilizzati, le persone interessate , nonché la prevista durata della conservazione(v. il punto 108 della sentenza *Tele 2*).
Per tentare di comprendere l'articolo 15, par. 1, della direttiva 2002/58 si deve, ad avviso dello scrivente, partire dall'importante contributo fornito dalla sentenza *Tele2 Sverige e Watson* e a. (di seguito: sentenza *Tele 2)*, della Corte di giustizia dell'Unione europea nelle cause riunite C-203/15 e C-698/15.

La sentenza, nell'affrontare il tema relativo alla questione relativa dall'art. 15, par. 1, della direttiva 2002/58 ha chiarito[1] che l'articolo 15, par. 1, della direttiva 2002/58/CE, prevede che non vi possa essere ingerenza nei diritti alla protezione dei dati personali e alla vita privata quando questa ne risulta grave e non limitata a quanto strettamente necessario e, quindi, non può essere considerata giustificata all'interno di una società democratica malgrado con tale operazione si persegua un obiettivo legittimo. Pertanto una normativa nazionale che contempla "*una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica*"[2] rientrerebbe in tale divieto come previsto all'art. 15, par. 1, della direttiva 2002/58/CE, letto alla luce degli articoli 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE[3](di seguito Carta).
L'art. 52, della Carta mira a fissare la portata dei diritti e dei principi contenuti nella stessa e a definire norme per la loro interpretazione ed il paragrafo 1, tratta il sistema delle limitazioni e si ispira alla giurisprudenza della Corte di giustizia: `...

1 Si vedano segnatamente i punti da 110 a 112 della sentenza Tele 2 Sverige e Watson e a.;

2 Così il punto 112 della sentenza Tele 2.

3 In proposito, si veda anche l'art. 23 del RGPD.

secondo una giurisprudenza costante, restrizioni all'esercizio dei diritti fondamentali possono essere operate, in particolare nell'ambito di un'organizzazione comune di mercato, purché tali restrizioni rispondano effettivamente a finalità di interesse generale perseguite dalla Comunità e non si risolvano, considerato lo scopo perseguito, in un intervento sproporzionato ed inammissibile che pregiudicherebbe la stessa sostanza di tali diritti` (sentenza del 13 aprile 2000, causa C-292/97, punto 45 della motivazione). Di fatto indica le condizioni che deve rispettare la legislazione con cui si intende introdurre eventuali limitazioni all'esercizio dei diritti fondamentali previsti dalla stessa e, quindi, determinare la misura in cui i diritti possono essere effettivamente goduti (previsione di legge rispetto del contenuto essenziale dei diritti; rispetto del principio di necessità; rispetto del principio di proporzionalità[4]; raggiungimento di obiettivi di interesse generale, riconosciuti dall'Unione europea o necessità di proteggere i diritti e le libertà altrui).

In applicazione dei suesposti principi normativi, a la sentenza Tele2 precisa che *"una normativa nazionale [...] la quale riguarda in maniera generalizzata tutti gli abbonati ed utenti iscritti e ha ad oggetto tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico"* e che "*non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito*" travalica i limiti dello stretto necessario[5].

Il giudice di Lussemburgo sottolinea come *"Essa concerne in maniera globale l'insieme delle persone che si avvalgono di servizi di comunicazione elettronica, senza che tali persone si trovino, anche solo indirettamente, in una situazione suscettibile di dar luogo ad azioni penali. Essa si applica dunque finanche a persone per le quali non esiste alcun indizio di natura tale da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi"* (così il punto 105 della sentenza *Tele 2*; v., per analogia, per quanto riguarda la direttiva 2006/24, la sentenza *Digital Rights,* punti 57 e 58).

Analoghe considerazioni si rinvengono nella sentenza *Digital rights Ireland Ltd*[6] sentenza ricordata soprattutto per aver dichiarato invalida la direttiva 2006/24/CE sulla conservazione dei dati di traffico.

È evidente come l'ingerenza di una tale normativa nei diritti fondamentali di cui agli artt. 7 e 8 della Carta[7] risulti di vasta portata ed è particolarmente grave, atteso che tali dati, presi nel loro insieme, consentono di trarre conclusioni, e quindi informazioni varie nonché molto precise riguardo alla vita privata delle persone interessate, gli ambienti sociali da esse frequentati, le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate e le loro relazioni sociali aspetti questi ripresi al punto 27 della sentenza *Digital Rights.*

Tali dati forniscono gli strumenti per poter ricostruire il profilo degli interessati, informazione assai rilevante e delicata in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle co-

4 Sul cosiddetto test di proporzionalità applicabile nel giudizio ai diritti, v., ex ceterbus: R. ALEXY, Teoria dei diritti fondamentali, Bologna, Il Mulino,2012 e A. BARAK, Proportionality, Cambridge, Cambridge University Press, 2012.

5 Così il punto 105 della sentenza Tele 2; cfr. anche il punto 97 della medesima sentenza.

6 Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital RightsIreland, Seitlinger e a. Per un commento a questa importante sentenza. v. fra gli altri: S. BONFIGLIO, Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo, in Democrazia e Sicurezza, n. 3/2014; C. M. CASCIONE, I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della corte di giustizia e gli echi del datagate, in Nuova Giur. Civ., 11/2014, p. 11039.

7 Interessante risulta il contributo di L. Trucco, Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea. Un'analisi delle strategie argomentative e delle tecniche decisorie a Lussemburgo, Torino, Giappichelli, 2013, pp. X-238, Fonte preziosa quanto autorevole è S. RODOTÀ, Nel silenzio della politica i giudici fanno l'Europa, in (a cura di) G. Bronzini, V. Piccone, La Carta e le Corti, Chimienti, 2007, p.23

municazioni[8]. Inoltre, tale conservazione ingiustificata potrebbe avere un'incidenza sull'utilizzazione dei mezzi di comunicazione elettronica e, dunque, sull'esercizio, da parte degli utenti, attraverso tali mezzi, della loro libertà di espressione, garantita dall'articolo 11 della Carta (v., per analogia, per quanto concerne la direttiva 2006/24, la sentenza *Digital Rights*, punto 28).
La Corte prosegue evidenziando come *"una normativa siffatta non richiede alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica. In particolare, essa non è limitata ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità"* (così il punto 106 della sentenza *Tele 2*; v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza *Digital Rights*, punto 59).

Interessante notare come la Corte[9] sottolinei che - al fine di garantire che la conservazione a titolo preventivo dei dati relativi al traffico e dei dati relativi all'ubicazione rispetti tale condizione (sia limitata allo stretto necessario e sia proporzionata) - la normativa nazionale deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione di una siffatta misura di conservazione dei dati e fissino un minimo di requisiti, di modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti tali da poter proteggere in modo efficace i loro dati personali contro i rischi di abuso; - indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati possa, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario; - prevedere che la conservazione dei dati risponda sempre a criteri oggettivi, tali da assicurare la sussistenza di una connessione tra i dati da conservare e l'obiettivo perseguito e da delimitare in modo effettivo la portata della misura e, quindi, il pubblico interessato.

8 v. i punti 99-101della sentenza Tele 2

9 v. punti 109-111 della sentenza Tele 2.

In particolare, in relazione al pubblico interesse, fondarsi su elementi oggettivi, tali da prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, e contribuire così alla lotta contro la criminalità organizzata, o a prevenire un grave rischio per la sicurezza pubblica, mediante. per esempio, il ricorso ad un criterio geografico, qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esista, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di reati.

> La normativa nazionale deve prevedere norme chiare e precise

Con riguardo all'accesso generale a tutti i dati conservati, - indipendentemente da una qualche connessione, almeno indiretta, con la finalità perseguita - la Corte di giustizia afferma come lo stesso non possa essere considerato limitato allo stretto necessario e che la normativa nazionale in questione debba fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali l'accesso va concesso alle autorità nazionali competenti[10].
In definitiva, ad avviso della Corte, *"il sistema istituito dalla direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione"* (così il punto 104 della sentenza *Tele 2*) e che l'art. 15, par. 1, della direttiva 2002/58/CE debba essere interpretato, conformemente alla consolidata giurisprudenza della Corte, in maniera restrittiva (cfr. il punto 89 della sentenza *Tele 2*).

10 Secondo la Corte, "A questo proposito, un accesso può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta (v., per analogia, Corte EDU, 4 dicembre 2015, Zakharov c. Russia, CE:ECHR:2015:1204JUD004714306, § 260)" (punto 119 della sentenza Tele2).

Nel quadro normativo attuale, venutosi a formare grazie alla entrata in vigore del Regolamento (UE) 2016/679 assume rilevanza l'art. 95, che nel disciplinare il rapporto con la direttiva 2002/58/CE, chiarisce che lo stesso "*non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE*" (v. anche il considerando 173). Importante sottolineare che le misure restrittive e le cautele relative all'accesso ai dati riguardino un momento distinto e successivo rispetto alla precedente attività di conservazione dei dati, nonché a quella relativa alla prima raccolta, e deve anche per essa avvenire nel pieno rispetto dei principi di necessità e proporzionalità per risultare compatibile con il combinato disposto di cui agli artt. 15, par. 1, della direttiva 2002/58/CE, 7, 8, 11 e 52, par. 1, della Carta. La correttezza di tali trattamenti è presupposto di legittimità anche per i trattamenti ulteriori di dati, quale, ad esempio, la successiva comunicazione di tali dati a soggetti terzi.

> Nelle attuali bozze del Regolamento e.privacy non si rinvengono spunti utili a meglio delineare i confini dei due diritti nel settore delle tlc e della conservazione di tali dati per fini di prevenzione e repressione dei reati.

Dall'esame della normativa e della giurisprudenza della Corte, appare che dal combinato di cui agli artt. 15, par. 1, della direttiva 2002/58/CE e agli artt. 7, 8, 11 e 52, par. 1, della Carta non si pervenga alla legittimazione della conservazione massiva (e ingiustificata) dei dati in parola, considerato che tale conservazione (ingiustificata) non sarebbe compatibile con i principi di necessità e proporzionalità dei dati. Questi principi rappresentano, infatti, un duplice essenziale requisito che qualsiasi misura legislativa che comporti una limitazione dei diritti fondamentali alla riservatezza e alla protezione dei dati personali deve soddisfare per assicurare la legittimità stessa delle limitazioni, nella consapevolezza che la ricerca dell'opportuno ed equo equilibrio tra le contrapposte esigenze è rimessa segnatamente ai legislatori europeo e nazionali, nei limiti posti dalla giurisprudenza della Corte di giustizia. Anche perché, come ricordato costantemente dalla stessa Corte CEDU, i diritti fondamentali non vanno intesi in assoluto, ma bilanciati nelle singole e varie fattispecie concrete, al fine di assicurarne un corretto bilanciamento che consenta, a fronte di un ragionevole limite-pregiudizio, la salvaguardia dell'essenza degli stessi.

Un simile approccio è rinvenibile anche nei lavori del Gruppo "Articolo 29" sulla tutela dei dati personali (organo prettamente consultivo che riuniva le Autorità di protezione dati europee, poi sostituito dal Comitato europeo per la protezione dei dati previsto dal Regolamento (UE) 2016/679), che ha sottolineato più volte come le disposizioni nazionali in materia di conservazione dei dati di traffico devono rispettare i parametri contenuti all'art. 15, par. 1 della direttiva 2002/58/CE, e che questo a sua volta, deve essere interpretato in maniera compatibile con i principi sanciti dalla Carta e i principi generali dell'Unione europea, alla luce della giurisprudenza della Corte di Giustizia. Il Gruppo "Articolo 29" ha in varie occasioni richiamato l'attenzione degli Stati membri e della Commissione europea sulla necessità che tali discipline assicurino che non vi sia una conservazione indiscriminata di dati di traffico di ogni tipo, ma che i dati oggetto di conservazione siano soggetti ad appropriate differenziazioni, limitazioni o eccezioni. Inoltre, l'accesso e la *disclosure* dei dati conservati e il loro utilizzo devono essere limitati a ciò che è strettamente necessario in termini di categorie di dati e di persone interessate e devono essere individuate specifiche condizioni sostanziali e procedurali da rispettare[11].

11 WP 220, Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive;

In conclusione la questione da porre riguarda l'aspetto della conservazione generalizzata e indifferenziata di dati personali ("dati di comunicazione di massa") così come definita nella sentenza *Tele2*. In particolare, occorre chiedersi se questo divieto possa essere superato quando la conservazione sia limitata per un periodo determinato e differenziato rispetto a determinate categorie di dati assolutamente indispensabili per il fine di prevenzione, repressione della criminalità organizzata e del terrorismo e per la salvaguardia della sicurezza nazionale e vengano, al contempo, assicurate ulteriori garanzie e tutele relativamente all'accesso limitato ai dati personali comunque soggetto a un controllo preventivo da parte di un giudice (o di un'entità amministrativa indipendente), all'informazione delle persone interessate, senza compromettere le indagini in corso, e all'adozione di norme che evitino l'uso indebito e l'accesso illecito ai dati[12].

Questo è un tema attuale ancor più in presenza di normative, come quella italiana, che, con specifico riferimento alla finalità pur grave di contrasto al fenomeno terroristico, prevedono termini elevati di durata della conservazione dei dati (sei anni)[13] [14] che risultano "*in palese contrasto con l'ordinamento e con la giurisprudenza dell'Unione europea, che precludono una raccolta generale e indiscriminata dei dati di traffico telefonico e telematico, in quanto non proporzionata alle esigenze investigative e al nucleo essenziale del diritto alla protezione dati*"[15].
Non vi sono dubbi circa la rilevanza e anche l'urgenza degli obiettivi ultimi della restrizione dei diritti fondamentali di cui trattasi.

La lacuna lasciata dall'avvenuto riconoscimento dell'invalidità della direttiva 2006/2204/CE nelle attuali bozze del Regolamento **e.privacy** non sembra essere colmata, sulla stessa oramai da anni il legislatore comunitario sta lavorando nel tentativo di aggiornare la disciplina dedicata al settore delle comunicazioni elettroniche, e allo stato sulla bozza non si rinvengono spunti utili a meglio delineare i confini dell'ambito dei due diritti nel settore delle tlc e della conservazione di tali dati per fini di prevenzione e repressione dei reati. La Corte e le sue pronunce diventano pertanto la bussola utile per orientarsi e in tal senso si segnala che comunque, nelle more, avremo a breve ulteriori pronunce del giudice comunitario, in funzione di interpretazione ed applicazione uniforme del superiore diritto europeo, che toccheranno alcuni dei punti sin qui affrontati in quanto vi sono stati ulteriori rinvii pregiudiziali le cui cause pendono ancora dinnanzi alla Corte di Giustizia[16]. ©

12 Al proposito si ricorda che né il Regolamento 2016/679, né la Direttiva 2016/680, hanno affrontato la questione del trattamento dei dati personali con finalità di prevenzione di reati legati al terrorismo o più generalmente ai reati gravi.

13 L'art. 24 della legge 20 novembre 2017, n. 167 per la conservazione dei dati di traffico telefonico e telematico e dei dati relativi a tutte le chiamate senza risposta per finalità di lotta al terrorismo in attuazione della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, che sostituisce la decisione quadro 2002/475/GAI del Consiglio -che deroga significativamente a quanto previsto dall'art. 132, co. 1 e 1-bis, del Codice in materia di protezione dei dati personali (d.lgs. n.30.06.2003, n. 196).

14 Per una lettura comparata di testi recenti che si interrogano sulle misure adottate in Europa ed America riguardo al fenomeno del terrorismo, v. fra gli altri: L. MAYALI, J. YOO, A Comparative Examination of Counter-Terrorism Law and Policy, in UC Berkeley Public Law Research,Paper No. 2949078/2016; G. DE MINICO, Costituzione emergenza e terrorismo, Napoli, Iovene,2016.

15 (cfr. la nota indirizzata il 22 dicembre 2017 al Governo e al Parlamento in tema di disciplina di dati di traffico dal Presidente di questa Autorità, Antonello Soro su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7464029;

16 proposte dal Conseil d'État, cause riunite C-511/18 e C-512/18, riguardanti la legislazione francese; dall'Investigatory Powers Tribunal, causa C-623/17, concernente il Regno Unito e, da ultimo, dalla Cour constitutionnelle belga, causa C-520/18, riguardante il Belgio.