Corte di giustizia dell'Unione europea
COMUNICATO STAMPA n. 145/16
Lussemburgo, 21 dicembre 2016

Stampa e Informazione

Sentenza nelle cause riunite C-203/15, Tele2 Sverige AB / Post-och telestyrelsen, e C-698/15, Secretary of State for the Home Department / Tom Watson e a.

Gli Stati membri non possono imporre un obbligo generale di conservazione di dati ai fornitori di servizi di comunicazione elettronica

Il diritto dell'Unione osta ad una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, ma è consentito agli Stati membri prevedere, a titolo preventivo, la conservazione mirata di tali dati al solo scopo di lottare contro gravi fenomeni di criminalità, a condizione che tale conservazione di dati 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. L'accesso delle autorità nazionali ai dati conservati deve essere assoggettato a condizioni, tra cui in particolare un controllo preventivo da parte di un'autorità indipendente e la conservazione dei dati nel territorio dell'Unione

Nella sua sentenza Digital Rights Ireland del 2014 [1], la Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati [2], a motivo del fatto che l'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, determinata dall'obbligo generale di conservazione dei dati relativi al traffico e all'ubicazione, non era limitata allo stretto necessario.

A seguito di detta sentenza, la Corte è stata investita di due controversie vertenti sull'obbligo generale imposto, in Svezia e nel Regno Unito, ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi a tali comunicazioni, sulla base della direttiva dichiarata invalida.

All'indomani della pronuncia della sentenza Digital Rights Ireland, l'impresa di telecomunicazioni Tele2 Sverige ha notificato all'autorità svedese di vigilanza sulle poste e telecomunicazioni la propria decisione di cessare di effettuare la conservazione dei dati, nonché la propria intenzione di cancellare i dati già registrati (causa C-203/15). Il diritto svedese obbliga, infatti, i fornitori di servizi di comunicazione elettronica a conservare in maniera sistematica e continua, senza alcuna eccezione, l'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti i loro abbonati ed utenti iscritti, con riferimento a tutti i mezzi di comunicazione elettronica.

Nella causa C-698/15, i sigg. Tom Watson, Peter Brice e Geoffrey Lewis hanno proposto dei ricorsi contro la normativa britannica di conservazione dei dati, che consente al Ministro dell'Interno di obbligare gli operatori di telecomunicazioni pubbliche a conservare tutti i dati relativi a comunicazioni per una durata massima di dodici mesi, fermo restando che è esclusa la conservazione del contenuto di tali comunicazioni.

Mediante il rinvio pregiudiziale effettuato dal Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile), Regno Unito], la Corte viene sollecitata a precisare se siano compatibili con il diritto dell'Unione (nella fattispecie la direttiva relativa alla vita privata e alle comunicazioni elettroniche [3], letta alla luce della Carta dei

[1] Sentenza della Corte dell'8 aprile 2014, *Digital Rights Ireland e Seitlinger e.a.* (cause riunite C-293/12 e C-594/12; v. comunicato stampa n. 54/14).
[2] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, 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 (GU 2006, L 105, pag. 54).
[3] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e

diritti fondamentali dell'UE [4]) i regimi nazionali che impongono ai fornitori di servizi di comunicazione elettronica un obbligo generale di conservazione dei dati e che prevedono l'accesso delle autorità nazionali competenti ai dati conservati, senza segnatamente limitare tale accesso alle sole finalità di lotta contro la criminalità grave e senza subordinare l'accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

Nella sua sentenza odierna, **la Corte risponde che il diritto dell'Unione osta a una normativa nazionale che preveda una conservazione generalizzata e indifferenziata dei dati.**

La Corte conferma, anzitutto, che **le misure nazionali** in questione **rientrano nell'ambito di applicazione della direttiva.** Infatti, la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico, garantita dalla direttiva, si applica alle misure adottate da qualsiasi soggetto diverso dagli utenti, indipendentemente dal fatto che si tratti di persone fisiche o di enti privati o pubblici.

La Corte constata, poi, che, se certo la direttiva suddetta consente agli Stati membri di limitare la portata dell'obbligo di principio di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati, essa non può però giustificare che la deroga a tale obbligo di principio e, in particolare, al divieto di memorizzare tali dati, prevista dalla direttiva stessa, divenga la regola.

Inoltre, la Corte ricorda la propria costante giurisprudenza secondo cui la tutela del diritto fondamentale al rispetto della vita privata esige che **le deroghe** alla protezione dei dati personali **intervengano entro i limiti dello stretto necessario**. La Corte applica tale giurisprudenza alle norme disciplinanti la conservazione dei dati e a quelle disciplinanti l'accesso ai dati conservati.

Per quanto riguarda la conservazione, la Corte constata che i dati conservati considerati nel loro insieme **sono tali da consentire di ricavare conclusioni assai precise sulla vita privata delle persone** i cui dati sono stati conservati.

Pertanto, l'ingerenza risultante da una normativa nazionale che preveda la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione deve essere considerata particolarmente grave. Il fatto che la conservazione dei dati venga effettuata senza che gli utenti dei servizi di comunicazione elettronica ne siano informati è idoneo a ingenerare, nello spirito delle persone riguardate, la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua. Di conseguenza, **soltanto la lotta contro la criminalità grave è idonea a giustificare un'ingerenza siffatta.**

La Corte rileva che **una normativa la quale preveda una conservazione generalizzata e indifferenziata dei dati non richiede alcuna correlazione tra i dati di cui si prevede la conservazione ed una minaccia per la sicurezza pubblica** e non si limita in particolare a prevedere una conservazione dei dati afferenti un periodo temporale e/o una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una violazione grave. **Una siffatta normativa nazionale eccede dunque i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come richiesto dalla direttiva letta alla luce della Carta**.

La Corte chiarisce, per contro, che **la direttiva non osta ad una normativa nazionale che imponga una conservazione mirata dei dati** per finalità di lotta contro gravi fenomeni di criminalità, **a condizione che tale conservazione dei dati sia**, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone implicate, nonché la durata di conservazione prevista, **limitata allo stretto necessario**. Secondo la Corte, **qualsiasi normativa nazionale che vada in tal senso deve essere chiara e precisa** e **prevedere garanzie sufficienti** al fine di proteggere i dati contro i rischi di abuso. Essa deve indicare le circostanze e le condizioni in presenza delle quali una misura che disponga la conservazione di dati possa, a titolo preventivo, essere adottata, in modo da garantire che l'ampiezza di tale misura sia, in pratica,

---

alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11).

[4] Articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea.

effettivamente limitata allo stretto necessario. In particolare, una normativa siffatta deve essere **fondata su elementi oggettivi**, che consentano di prendere in considerazione le persone i cui dati siano idonei a presentare un collegamento con atti di criminalità grave, a contribuire alla lotta contro la criminalità grave o a prevenire un rischio grave per la sicurezza pubblica.

Per quanto riguarda **l'accesso delle autorità nazionali competenti ai dati conservati**, la Corte conferma che la normativa nazionale in questione non può limitarsi ad esigere che l'accesso risponda ad uno degli obiettivi previsti dalla direttiva, quand'anche questo fosse la lotta contro la criminalità grave, ma deve altresì prevedere le condizioni sostanziali e procedurali disciplinanti l'accesso delle autorità nazionali competenti ai dati conservati. Tale normativa deve fondarsi su **criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali l'accesso ai dati deve essere concesso alle autorità nazionali competenti**. L'accesso può, in linea di principio, essere accordato, in relazione all'obiettivo della lotta contro la criminalità, unicamente 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. Tuttavia, in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone potrebbe essere parimenti concesso quando sussistano elementi oggettivi che consentano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro simili attività.

Oltre a ciò, la Corte dichiara **che è essenziale che l'accesso ai dati conservati sia subordinato, salvo in casi di urgenza, ad un controllo preventivo** effettuato da un giudice o da un'entità amministrativa indipendente. Inoltre, le autorità nazionali competenti cui sia stato consentito l'accesso ai dati conservati devono darne comunicazione alle persone interessate.

Tenuto conto della quantità di dati conservati, del carattere sensibile di tali dati, nonché del rischio di accesso illecito a questi ultimi, **la normativa nazionale deve prevedere che i dati siano conservati nel territorio dell'Unione** e che essi vengano irreversibilmente distrutti al termine della durata della loro conservazione.

IMPORTANTE: Il rinvio pregiudiziale consente ai giudici degli Stati membri, nell'ambito di una controversia della quale sono investiti, di interpellare la Corte in merito all'interpretazione del diritto dell'Unione o alla validità di un atto dell'Unione. La Corte non risolve la controversia nazionale. Spetta al giudice nazionale risolvere la causa conformemente alla decisione della Corte. Tale decisione vincola egualmente gli altri giudici nazionali ai quali venga sottoposto un problema simile.

Il testo integrale della sentenza è pubblicato sul sito CURIA il giorno della pronuncia

Contatto stampa: Eleonora Montserrat Pappalettere ☎ (+352) 4303 8575

Immagini della pronuncia della sentenza sono disponibili su «Europe by Satellite» ☎ (+32) 2 2964106