Raccolta della giurisprudenza

Cause riunite C-203/15 e C-698/15

Tele2 Sverige AB
contro
Post- och telestyrelsen
e

Secretary of State for the Home Department
contro
Tom Watson e a.

[domande di pronuncia pregiudiziale proposte dal Kammarrätten i Stockholm e dalla Court of Appeal (England & Wales) (Civil Division)]

«Rinvio pregiudiziale – Comunicazioni elettroniche – Trattamento dei dati personali – Riservatezza delle comunicazioni elettroniche – Tutela – Direttiva 2002/58/CE – Articoli 5, 6 e 9, nonché articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11, nonché articolo 52, paragrafo 1 – Normativa nazionale – Fornitori di servizi di comunicazione elettronica – Obbligo riguardante la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Autorità nazionali – Accesso ai dati – Assenza di controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente – Compatibilità con il diritto dell'Unione»

Massime – Sentenza della Corte (Grande Sezione) del 21 dicembre 2016

1. *Ravvicinamento delle legislazioni – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Ambito di applicazione – Misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione degli utenti – Inclusione*

   (Direttiva del Parlamento europeo e del Consiglio 2002/58, come modificata dalla direttiva 2009/136, artt. 5, § 1, e 15, § 1)

2. *Ravvicinamento delle legislazioni – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Interpretazione restrittiva – Motivi idonei a giustificare l'adozione di una limitazione – Tassatività*

   (Direttiva del Parlamento europeo e del Consiglio 2002/58, come modificata dalla direttiva 2009/136, artt. 5, § 1, e 15, § 1)

3. *Ravvicinamento delle legislazioni – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Normativa nazionale che prevede una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti, per finalità di lotta contro la criminalità – Inammissibilità – Grave ingerenza nei diritti al rispetto della vita privata, alla protezione dei dati personali e alla libertà di espressione*

   (Carta dei diritti fondamentali dell'Unione europea, artt. 7, 8, 11 e 52, § 1; direttiva del Parlamento europeo e del Consiglio 2002/58, come modificata dalla direttiva 2009/136, art. 15, § 1)

4. *Ravvicinamento delle legislazioni – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Normativa nazionale che permette la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti, per finalità di lotta contro la criminalità grave – Ammissibilità – Presupposti*

   (Carta dei diritti fondamentali dell'Unione europea, artt. 7, 8, 11 e 52, § 1; direttiva del Parlamento europeo e del Consiglio 2002/58, come modificata dalla direttiva 2009/136, art. 15, § 1)

5. *Ravvicinamento delle legislazioni – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Normativa nazionale disciplinante la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti – Possibilità per le autorità nazionali di accedere ai dati suddetti senza un previo controllo giurisdizionale o amministrativo – Inammissibilità – Assenza di un obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare tali dati nel territorio dell'Unione – Inammissibilità*

   (Carta dei diritti fondamentali dell'Unione europea, artt. 7, 8, 11 e 52, § 1; direttive del Parlamento europeo e del Consiglio 95/46, art. 22, e 2002/58, come modificata dalla direttiva 2009/136, art. 15, §§ 1 e 2)

6. *Diritti fondamentali – Convenzione europea dei diritti dell'uomo – Strumento non formalmente integrato nel sistema giuridico dell'Unione*

   (Art. 6, § 3, TUE; Carta dei diritti fondamentali dell'Unione europea, art. 52, § 3)

7. *Questioni pregiudiziali – Competenza della Corte – Limiti – Questioni di carattere generale o ipotetico – Questione avente carattere astratto e meramente ipotetico in relazione all'oggetto della controversia principale – Irricevibilità*

   (Art. 267 TFUE)

1. L'articolo 15, paragrafo 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136, autorizza gli Stati membri ad adottare, nel rispetto delle condizioni da esso previste, disposizioni legislative volte a limitare la portata dei diritti e degli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della citata direttiva.

Rientra, in particolare, nell'ambito di applicazione della citata disposizione una misura legislativa la quale imponga ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, in quanto una siffatta attività implica necessariamente un trattamento, da parte di tali soggetti, di dati personali. Rientra del pari nel suddetto ambito di applicazione una misura legislativa riguardante l'accesso delle autorità nazionali ai dati conservati dai suddetti fornitori. Infatti, la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico afferenti alle stesse, garantita dall'articolo 5, paragrafo 1, della direttiva 2002/58, si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di persone o di entità private oppure di entità statali.

(v. punti 71, 75-77)

2. L'articolo 15, paragrafo 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136, consente agli Stati membri di introdurre eccezioni all'obbligo di principio, enunciato all'articolo 5, paragrafo 1, di detta direttiva, di garantire la riservatezza dei dati personali, nonché ai corrispondenti obblighi, menzionati segnatamente negli articoli 6 e 9 della medesima direttiva. Nondimeno, l'articolo 15, paragrafo 1, della direttiva 2002/58, consentendo agli Stati membri di limitare la portata del suddetto obbligo di principio, deve essere interpretato in maniera restrittiva. Pertanto, una disposizione siffatta non può giustificare che la deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati, previsto dall'articolo 5 della citata direttiva, divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata.

In proposito, l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 stabilisce che le misure legislative che esso prevede e che derogano al principio della riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati debbono avere come obiettivo la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, o la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica, oppure devono perseguire uno degli altri obiettivi contemplati dall'articolo 13, paragrafo 1, della direttiva 95/46, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Una siffatta elencazione di obiettivi presenta carattere esaustivo, come risulta dall'articolo 15, paragrafo 1, seconda frase, della citata direttiva 2002/58, a mente del quale le misure legislative devono essere giustificate sulla scorta di uno dei motivi enunciati nella prima frase del medesimo articolo 15, paragrafo 1. Pertanto, gli Stati membri non possono adottare misure siffatte per finalità diverse da quelle elencate in quest'ultima disposizione.

(v. punti 88-90)

3. L'articolo 15, paragrafo 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, 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.

Infatti, presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati. In particolare, tali dati forniscono gli strumenti per stabilire il profilo delle persone interessate,

informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni. L'ingerenza che una normativa siffatta determina nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta risulta essere di vasta portata e deve essere considerata particolarmente grave. La circostanza che la conservazione dei dati venga effettuata senza che gli utenti dei servizi di comunicazione elettronica ne siano informati è idonea a ingenerare nello spirito delle persone riguardate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua. Anche se una normativa siffatta non autorizza la conservazione del contenuto di una comunicazione e, di conseguenza, non è idonea a pregiudicare il contenuto essenziale dei suddetti diritti, la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione potrebbe nondimeno avere un'incidenza sull'utilizzazione dei mezzi di comunicazione elettronica e, dunque, sull'esercizio, da parte degli utenti, di tali mezzi della loro libertà di espressione, garantita dall'articolo 11 della Carta.

Tenuto conto della gravità dell'ingerenza nei diritti fondamentali in questione derivante da una siffatta normativa nazionale, soltanto la lotta contro la criminalità grave è idonea a giustificare una misura del genere. Tuttavia, anche se l'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine, un siffatto obiettivo di interesse generale, per quanto fondamentale esso sia, non vale di per sé solo a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta. Da un lato, una normativa siffatta porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, quando invece il sistema istituito dalla direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione. Dall'altro lato, una normativa nazionale siffatta, 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, non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito. Essa si applica 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. Una normativa del genere travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta.

(v. punti 99-105, 107, 112, dispositivo 1)

4. L'articolo 15, paragrafo 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario.

Per soddisfare tali requisiti, la suddetta normativa nazionale deve, in primo luogo, 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 permettere di proteggere efficacemente i loro dati personali contro i rischi di abuso. Essa deve in particolare indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario.

In secondo luogo, per quanto riguarda le condizioni sostanziali che devono essere soddisfatte da una siffatta normativa nazionale, al fine di garantire che essa sia limitata allo stretto necessario, se certo tali condizioni possono variare in funzione delle misure adottate ai fini della prevenzione, della ricerca, dell'accertamento e del perseguimento della criminalità grave, la conservazione dei dati deve comunque rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato. Per quanto riguarda tale delimitazione, la normativa nazionale deve essere fondata su elementi oggettivi, che permettano di prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica. Una siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo.

(v. punti 108-111)

5. L'articolo 15, paragrafo 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione.

A questo proposito, al fine di garantire che l'accesso delle autorità nazionali competenti ai dati conservati sia limitato allo stretto necessario, spetta senza dubbio al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazione elettronica devono consentire tale accesso. Tuttavia, la normativa nazionale in questione non può limitarsi ad esigere che l'accesso risponda ad uno degli obiettivi contemplati dall'articolo 15, paragrafo 1, della direttiva 2002/58, quand'anche questo fosse la lotta contro la criminalità grave. Infatti, una normativa nazionale siffatta deve prevedere anche le condizioni sostanziali e procedurali che disciplinano l'accesso delle autorità nazionali competenti ai dati conservati. Pertanto, e poiché un accesso generale a tutti i dati conservati, indipendentemente da una qualche connessione, almeno indiretta, con la finalità perseguita, non può essere considerato limitato allo stretto necessario, la normativa nazionale in questione deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati degli abbonati o degli utenti iscritti. 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. Tuttavia, in situazioni particolari, come quelle in cui gli 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.

Al fine di garantire, in pratica, il pieno rispetto di tali condizioni, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale. Allo stesso modo, occorre che le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate. Infatti, tale informazione è, de facto, necessaria per consentire a dette persone di esercitare, in particolare, il diritto di ricorso, esplicitamente previsto dall'articolo 15, paragrafo 2, della direttiva 2002/58, letto in connessione con l'articolo 22 della direttiva 95/46, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in caso di violazione dei loro diritti.

Inoltre, tenuto conto della quantità di dati conservati, del carattere sensibile dei dati stessi, nonché del rischio di accesso illecito a questi ultimi, i fornitori di servizi di comunicazione elettronica devono, al fine di assicurare la piena integrità e la riservatezza dei dati suddetti, garantire un livello particolarmente elevato di protezione e di sicurezza mediante misure tecniche e organizzative appropriate. In particolare, la normativa nazionale deve prevedere la conservazione nel territorio dell'Unione nonché la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi.

(v. punti 118-122, 125, dispositivo 2)

6. V. il testo della decisione.

(v. punti 127-129)

7. V. il testo della decisione.

(v. punto 130)