



L'avvocato generale Saugmandsgaard Øe propone alla Corte di dichiarare che anche i reati non particolarmente gravi possono giustificare l'accesso ai metadati di base delle comunicazioni elettroniche, purché tale accesso non attenti gravemente alla vita privata

Nel contesto di un'indagine su un caso di rapina di un portafoglio e di un telefono cellulare, la polizia giudiziaria spagnola ha chiesto al giudice istruttore di consentirle di accedere ai dati identificativi degli utenti dei numeri di telefono attivati dal telefono rubato per un periodo di dodici giorni a partire dal giorno della rapina. Il giudice istruttore ha respinto tale domanda con la motivazione, in particolare, che i fatti all'origine dell'indagine penale non avrebbero costituito un reato «grave» – ossia, secondo il diritto spagnolo, un reato sanzionato con pena detentiva superiore a cinque anni –, mentre in Spagna l'accesso ai dati d'identificazione sarebbe stato possibile solo per questo tipo di reati. Il Ministerio Fiscal (pubblico ministero spagnolo) ha interposto appello avverso tale decisione dinanzi all'Audiencia Provincial de Tarragona (Corte provinciale di Tarragona, Spagna).

La direttiva relativa alla vita privata e alle comunicazioni elettroniche¹ prevede che gli Stati membri possano limitare i diritti dei cittadini qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica o per assicurare la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.

Nelle sue sentenze Digital Rights² e Tele2 Sverige³, la Corte di giustizia ha utilizzato la nozione di «reati gravi» per valutare la legittimità e la proporzionalità di un'ingerenza nel diritto al rispetto della vita privata e della vita familiare nonché nel diritto alla protezione dei dati di carattere personale, diritti sanciti nella Carta dei diritti fondamentali dell'Unione europea.

1 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 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).

2 Sentenza dell'8 aprile 2014, Digital Rights Ireland ([C-293/12](#) e [C-594/12](#), v. comunicato stampa n. [54/14](#)). In tale sentenza la Corte ha dichiarato invalida la 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 Sentenza del 21 dicembre 2016, Tele2 Sverige ([C-203/15](#) e [C-698/15](#), v. comunicato stampa n. [145/16](#)). In tale sentenza la Corte ha dichiarato che il diritto dell'Unione, da una parte, «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» e, dall'altra, «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».

L'Audiencia Provincial de Tarragona indica che, dopo l'adozione della decisione da parte del giudice istruttore, il legislatore spagnolo ha introdotto due criteri alternativi per determinare il livello di gravità di un reato relativamente al quale le conservazioni e la comunicazione dei dati personali sono autorizzate. Il primo è un criterio materiale, che si riferisce ai reati di terrorismo e a quelli commessi nell'ambito di un'organizzazione criminale. Il secondo è un criterio normativo formale, che stabilisce una soglia minima di tre anni di reclusione. Il giudice spagnolo sottolinea che tale soglia potrebbe comprendere la maggior parte delle fattispecie di reato. L'Audiencia Provincial de Tarragona interroga quindi la Corte riguardo alla fissazione della soglia di gravità dei reati a partire dalla quale può essere giustificata, alla luce delle sentenze sopra citate, un'ingerenza nei diritti fondamentali, in occasione dell'accesso, da parte delle autorità nazionali competenti, a dati personali conservati da fornitori di servizi di comunicazione elettronica.

Nelle sue conclusioni presentate in data odierna, l'avvocato generale Henrik Saugmandsgaard Øe constata anzitutto che una misura come quella chiesta dalla polizia giudiziaria nel caso di specie costituisce un'ingerenza nel diritto al rispetto della vita privata e della vita familiare nonché nel diritto alla protezione dei dati di carattere personale. Tuttavia, l'avvocato generale ritiene che, **nelle sentenze Digital rights e Tele2, la Corte abbia stabilito un collegamento tra la gravità dell'ingerenza constatata e la gravità del motivo che consente di giustificare quest'ultima.** Pertanto, per esigere, nella fase della giustificazione di una siffatta ingerenza, che sussista un «reato grave», che consenta di derogare al principio della riservatezza delle comunicazioni elettroniche, occorre che **l'ingerenza sia grave. Secondo l'avvocato generale tale elemento essenziale non ricorre nella fattispecie.**

L'avvocato generale aggiunge che la natura dell'ingerenza di cui trattasi nel caso di specie è diversa da quelle ravvisate nelle due sentenze sopra citate. **Si tratta infatti di una misura mirata e finalizzata ad una possibilità di accesso, da parte delle autorità competenti e per le esigenze di un'indagine penale, a dati detenuti a fini commerciali da fornitori di servizi e che riguarda unicamente l'identità (nome, cognome ed eventualmente indirizzo) di una categoria ristretta di abbonati o utenti di uno specifico mezzo di comunicazione, vale a dire quelli il cui numero di telefono è stato attivato dal telefono cellulare il cui furto costituisce l'oggetto dell'indagine, e per un periodo limitato, vale a dire una dozzina di giorni. L'avvocato generale considera che gli effetti potenzialmente nocivi, per le persone interessate dalla richiesta di accesso in questione, sono nel contempo moderati e circoscritti,** in quanto i dati richiesti non sono destinati ad essere divulgati al pubblico e la facoltà di accesso offerta alle autorità di polizia è circondata da garanzie procedurali, poiché essa dà luogo ad un controllo giurisdizionale. **Di conseguenza, l'ingerenza causata dalla comunicazione di tali dati di identità civile non riveste un carattere di particolare gravità,** dal momento che, in tali circostanze particolari, dati siffatti non pregiudicano direttamente e fortemente l'intimità della vita privata della persona interessata.

L'avvocato generale indica che, secondo la direttiva, una deroga al principio di riservatezza delle comunicazioni elettroniche può essere giustificata dall'obiettivo di interesse generale di prevenire e perseguire reati, senza alcuna precisazione quanto alla natura di questi ultimi. Non è necessario che i reati che legittimano la misura restrittiva in questione possano essere qualificati come «gravi», ai sensi delle sentenze Digital Rights e Tele2. Secondo l'avvocato generale, **soltanto quando l'ingerenza subita presenta una particolare gravità i reati idonei a giustificare una siffatta ingerenza devono presentare essi stessi una particolare gravità. Per contro, nell'ipotesi di un'ingerenza non grave (ossia quando i dati di cui è richiesta la comunicazione non pregiudicano gravemente il diritto al rispetto della vita privata), anche i reati che non presentano una particolare gravità possono giustificare tale ingerenza (ossia l'accesso ai dati richiesti).**

In particolare, l'avvocato generale considera che **il diritto dell'Unione non osta a che le autorità competenti possano avere accesso ai dati di identificazione, detenuti da fornitori di servizi di comunicazione elettronica, qualora tali dati consentano di rintracciare i presunti autori di un reato che non presenta un carattere grave. L'avvocato generale ne conclude che, alla luce della direttiva, la misura richiesta dalla polizia giudiziaria nel caso di specie comporta un'ingerenza nei diritti fondamentali garantiti dalla direttiva e dalla Carta che non raggiunge**

un livello di gravità sufficiente affinché occorra riservare un tale accesso ai casi in cui il reato in questione presenti un carattere grave.

IMPORTANTE: Le conclusioni dell'avvocato generale non vincolano la Corte di giustizia. Il compito dell'avvocato generale consiste nel proporre alla Corte, in piena indipendenza, una soluzione giuridica nella causa per la quale è stato designato. I giudici della Corte cominciano adesso a deliberare in questa causa. La sentenza sarà pronunciata in una data successiva.

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.

Documento non ufficiale ad uso degli organi d'informazione che non impegna la Corte di giustizia.

Il [testo integrale](#) delle conclusioni è pubblicato sul sito CURIA il giorno della lettura.

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

Immagini della lettura delle conclusioni sono disponibili su « [Europe by Satellite](#) » ☎ (+32) 2 2964106