Corte di giustizia dell'Unione europea
COMUNICATO STAMPA n. 58/22
Lussemburgo, 5 aprile 2022

Stampa e Informazione

Sentenza nella causa C-140/20
Commissioner of the Garda Síochána e a.

La Corte conferma che il diritto dell'Unione osta alla conservazione generalizzata e indifferenziata, per finalità di lotta ai reati gravi, dei dati relativi al traffico e dei dati relativi all'ubicazione riguardanti le comunicazioni elettroniche

Un giudice nazionale non può limitare nel tempo gli effetti della declaratoria d'invalidità di una normativa nazionale che prevede tale conservazione

Nel marzo 2015 G.D. è stato condannato all'ergastolo per l'omicidio di una donna in Irlanda. Nell'appello presentato contro la sua condanna dinanzi alla Corte d'appello d'Irlanda, l'interessato ha contestato, in particolare, al giudice di primo grado di avere erroneamente ammesso come elementi di prova i dati relativi al traffico e i dati relativi all'ubicazione afferenti a chiamate telefoniche. Per poter contestare l'ammissibilità di tali prove nel procedimento penale, G.D. ha intentato, in parallelo, un'azione civile presso l'Alta Corte d'Irlanda, diretta a far dichiarare l'invalidità di talune disposizioni della legge irlandese del 2011 che disciplina la conservazione di tali dati e l'accesso agli stessi, adducendo che detta legge violava i diritti conferitigli dal diritto dell'Unione. Con decisione del 6 dicembre 2018, l'Alta Corte ha accolto l'argomento di G.D. L'Irlanda ha interposto appello avverso tale decisione dinanzi alla Corte suprema d'Irlanda, che è il giudice del rinvio nella presente causa.

Con il suo rinvio pregiudiziale, la Corte suprema ha chiesto delucidazioni sui requisiti che il diritto dell'Unione impone in materia di conservazione di detti dati per finalità di lotta ai reati gravi e sulle garanzie necessarie in materia di accesso a questi stessi dati. Detto giudice si chiede, inoltre, quali siano la portata e l'effetto nel tempo di un'eventuale declaratoria d'incompatibilità che dovesse essere tenuto a pronunciare, posto che la legge irlandese del 2011 è stata adottata per recepire la direttiva 2006/24/CE [1], dichiarata invalida dalla Corte con la sentenza dell'8 aprile 2014, Digital Rights Ireland e a. [2] .

Nella sua sentenza, la Corte, riunita in grande sezione, conferma, in primo luogo, la propria costante giurisprudenza [3] secondo la quale il diritto dell'Unione [4] **osta a misure legislative che prevedano, a titolo preventivo, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione afferenti alle comunicazioni elettroniche, per finalità di lotta ai reati gravi**.

---

[1] 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).
[2] Sentenza dell'8 aprile 2014, Digital Rights Ireland, C-293/12, (v. comunicato stampa n. 54/14).
[3] Sentenze dell'8 aprile 2014, Digital Rights Ireland, C-293/12 ; del 21 dicembre 2016, Tele2 Sverige et Watson e a., C-203/15 e C-698/15 (v. comunicato stampa n. 145/16); del 6 ottobre 2020, Privacy International, C-623/17, e La Quadrature du Net e a., C-511/18, C-512/18 ,Ordre des barreaux francophones et germanophone e.a., C-520/18 (v. comunicato stampa n. 123/20); e del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18 (v. comunicato stampa n. 29/21).
[4] 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, p. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, p. 11) (in prosieguo: la «direttiva relativa alla vita privata e alle comunicazioni elettroniche»), letta alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in proseguio la «Carta»).

Infatti, la direttiva relativa alla vita privata e alle comunicazioni elettroniche non si limita a disciplinare l'accesso a simili dati mediante garanzie dirette a prevenire gli abusi, ma sancisce, in particolare, il **principio del divieto della memorizzazione** dei dati relativi al traffico e all'ubicazione. La conservazione di tali dati costituisce quindi, da un lato, una deroga a tale divieto di memorizzazione e, d'all'altro, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta.

Sebbene la direttiva relativa alla vita privata e alle comunicazioni elettroniche consenta agli Stati membri di limitare tali diritti e obblighi per finalità, segnatamente, di lotta ai reati, siffatte limitazioni devono tuttavia rispettare, in particolare, il principio di proporzionalità. Questo principio impone il rispetto non solo dei requisiti di idoneità e di necessità, ma anche di quello relativo al **carattere proporzionato** di tali misure in relazione all'obiettivo perseguito. Infatti, la Corte ha già statuito che l'obiettivo della lotta alla criminalità grave, per quanto fondamentale, non può di per sé giustificare il fatto che una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, come quella introdotta dalla direttiva 2006/24, sia considerata necessaria. Nello stesso ordine di idee, anche gli obblighi positivi degli Stati membri sull'istituzione di norme che consentano una lotta effettiva ai reati non possono avere l'effetto di giustificare ingerenze tanto gravi quanto quelle che una normativa nazionale che prevede una simile conservazione comporta nei diritti fondamentali della quasi totalità della popolazione, senza che i dati degli interessati siano idonei a rivelare una connessione, almeno indiretta, con l'obiettivo perseguito.

La Corte ricorda, poi, che vari obblighi positivi sono a carico dei pubblici poteri in forza della Carta, come per esempio l'adozione di misure giuridiche dirette a tutelare la vita privata e familiare, la protezione del domicilio e delle comunicazioni, ma anche la tutela dell'integrità fisica e psichica delle persone, nonché il divieto di tortura e di trattamenti inumani e degradanti. Ad essi spetta pertanto **conciliare i vari interessi legittimi e diritti in gioco**. Infatti, un obiettivo d'interesse generale non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un **contemperamento equilibrato** tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi, verificando che l'importanza di detto obiettivo sia correlata alla gravità dell'ingerenza provocata da tale misura.

Le predette considerazioni portano la Corte a respingere segnatamente l'argomento secondo cui la criminalità particolarmente grave potrebbe essere assimilata a una minaccia per la sicurezza nazionale che si riveli reale e attuale o prevedibile e che sia in grado di giustificare, per un periodo limitato, una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Infatti, una minaccia del genere si distingue per natura, gravità e specificità delle circostanze che la costituiscono, dal rischio generale e permanente rappresentato dal verificarsi di tensioni o di perturbazioni, anche gravi, della pubblica sicurezza o da quello di reati gravi.

Per contro, la Corte stabilisce, in secondo luogo e confermando la propria giurisprudenza anteriore, che il diritto dell'Unione non osta a misure legislative che prevedano, alle condizioni elencate nella sentenza, ai fini della lotta alle forme gravi di criminalità e della prevenzione delle minacce gravi alla sicurezza pubblica:

- **la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione** in funzione delle categorie di persone interessate o mediante un criterio geografico;

- **la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione**;

- **la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica**, e

- la **conservazione** rapida (*quick freeze*) dei dati relativi al traffico e dei dati relativi all'ubicazione di cui tali fornitori di servizi dispongono.

La Corte fornisce varie precisazioni riguardanti tali differenti categorie di misure.

Innanzitutto, le autorità nazionali competenti possono adottare una misura di conservazione mirata basata su un criterio geografico, come in particolare il tasso medio di criminalità in una data zona geografica, senza necessariamente disporre di indizi concreti relativi alla preparazione o alla commissione, nelle zone interessate, di atti di criminalità grave. Essa aggiunge che una simile misura di conservazione riguardante luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone o luoghi strategici, quali aeroporti, stazioni, porti marittimi o zone di pedaggio, consente alle autorità competenti di ottenere informazioni sulla presenza, in tali luoghi o zone geografiche, delle persone che ivi utilizzano un mezzo di comunicazione elettronica e di trarne conclusioni sulla loro presenza e sulla loro attività in tali luoghi o zone geografiche, ai fini della lotta alla criminalità grave.

La Corte precisa poi che né la direttiva relativa alla vita privata e alle comunicazioni elettroniche né alcun altro atto del diritto dell'Unione ostano a una normativa nazionale, avente ad oggetto la lotta alla criminalità grave, ai sensi della quale l'acquisizione di un mezzo di comunicazione elettronica, quale una carta SIM prepagata, sia subordinata alla verifica di documenti ufficiali che provino l'identità dell'acquirente e alla registrazione, da parte del venditore, delle informazioni che ne derivano, essendo il venditore eventualmente tenuto a consentire l'accesso a tali informazioni alle autorità nazionali competenti.

Infine, la Corte rileva che la direttiva relativa alla vita privata e alle comunicazioni elettroniche non osta a che le autorità nazionali competenti dispongano una misura di conservazione rapida fin dalla prima fase dell'indagine relativa a una minaccia grave per la sicurezza pubblica o a un eventuale atto di criminalità grave, ossia dal momento in cui tali autorità, secondo le pertinenti disposizioni del diritto nazionale, possono avviare una siffatta indagine. Una misura di questo tipo può essere estesa ai dati relativi al traffico e ai dati relativi all'ubicazione afferenti a persone diverse da quelle sospettate di avere progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati possano contribuire, sulla base di elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale, quali i dati della vittima o del suo ambiente sociale o professionale.

Tali diverse misure possono, a scelta del legislatore nazionale e nel rispetto dei limiti dello stretto necessario, essere applicate congiuntamente.

La Corte respinge poi l'argomento secondo il quale le autorità nazionali competenti dovrebbero poter accedere, ai fini della lotta alla criminalità grave, ai dati relativi al traffico e ai dati relativi all'ubicazione che sono stati conservati in modo generalizzato e indifferenziato, conformemente alla sua giurisprudenza, per fronteggiare una grave minaccia per la sicurezza nazionale che si riveli reale e attuale o prevedibile. Infatti, questo argomento fa dipendere tale accesso da circostanze estranee all'obiettivo di lotta alla criminalità grave. Inoltre, secondo detto argomento, l'accesso potrebbe essere giustificato da un obiettivo d'importanza minore rispetto a quello che ha giustificato la conservazione, vale a dire la salvaguardia della sicurezza nazionale, il che sarebbe contrario alla gerarchia degli obiettivi di interesse generale nel cui ambito deve essere valutata la proporzionalità di una misura di conservazione. Oltre a ciò, autorizzare un accesso del genere rischierebbe di privare di ogni effetto utile il divieto di procedere a una conservazione generalizzata e indifferenziata per finalità di lotta alla criminalità grave.

In terzo luogo, la Corte conferma che il diritto dell'Unione osta a una normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, anche qualora quest'ultimo sia assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale. La Corte conferma infatti, al riguardo, la sua giurisprudenza secondo la quale, al fine di garantire, nella pratica, il pieno rispetto delle rigide condizioni di accesso a dati personali quali i dati relativi al traffico e i dati relativi all'ubicazione, l'accesso da parte delle autorità nazionali competenti ai dati conservati deve essere subordinato ad un controllo preventivo effettuato o da un

giudice o da un organo amministrativo indipendente, e la decisione di tale giudice o di tale organo deve intervenire a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di azione penale. Ebbene, un funzionario di polizia non è un giudice e non presenta tutte le garanzie d'indipendenza e di imparzialità richieste per poter essere qualificato come organo amministrativo indipendente.

In quarto e ultimo luogo, la Corte conferma la sua giurisprudenza secondo la quale il diritto dell'Unione osta al fatto che un giudice nazionale limiti nel tempo gli effetti di una declaratoria d'invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con la direttiva relativa alla vita privata e alle comunicazioni elettroniche.

Ciò posto, la Corte ricorda che l'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

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.

Contatto stampa: Cristina Marzagalli ☎ (+352) 4303 8575.