Corte di giustizia dell'Unione europea
COMUNICATO STAMPA n. 29/21
Lussemburgo, 2 marzo 2021

Stampa e Informazione

Sentenza nella causa C-746/18
H.K. / Prokuratuur

L'accesso, per fini penali, ad un insieme di dati di comunicazioni elettroniche relativi al traffico o all'ubicazione, che permettano di trarre precise conclusioni sulla vita privata, è autorizzato soltanto allo scopo di lottare contro gravi forme di criminalità o di prevenire gravi minacce alla sicurezza pubblica

Il diritto dell'Unione osta, peraltro, ad una normativa nazionale che attribuisca al pubblico ministero la competenza ad autorizzare l'accesso di un'autorità pubblica ai dati suddetti al fine di condurre un'istruttoria penale

In Estonia è stato instaurato un procedimento penale nei confronti di H.K. per le imputazioni di furto, utilizzazione della carta bancaria di un terzo e violenza nei confronti di persone partecipanti a un procedimento giudiziario. H.K. è stato condannato per questi reati da un tribunale di primo grado ad una pena detentiva di due anni. Tale decisione è stata successivamente confermata in appello.

I verbali sui quali si fonda la constatazione dei reati suddetti sono stati redatti, segnatamente, sulla base di dati personali generati nel quadro della fornitura di servizi di comunicazioni elettroniche. La Riigikohus (Corte suprema, Estonia), dinanzi alla quale H.K. ha proposto un ricorso per cassazione, ha sollevato dei dubbi riguardo alla compatibilità con il diritto dell'Unione [1] dei presupposti in presenza dei quali gli organi inquirenti hanno avuto accesso ai dati suddetti.

Tali dubbi riguardano, in primo luogo, la questione se la durata del periodo per il quale gli organi inquirenti hanno avuto accesso ai dati costituisca un criterio atto a permettere di valutare la gravità dell'ingerenza che tale accesso determina nei diritti fondamentali delle persone interessate. Così, per il caso in cui questo periodo sia molto breve o la quantità di dati raccolti sia assai limitata, il giudice del rinvio si è chiesto se l'obiettivo della lotta contro la criminalità in generale, e non soltanto contro le forme gravi di criminalità, sia idoneo a giustificare una siffatta ingerenza. In secondo luogo, il giudice del rinvio ha formulato dei dubbi quanto alla possibilità di considerare il pubblico ministero estone, alla luce dei diversi compiti che gli sono affidati dalla normativa nazionale, come un'autorità amministrativa «indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. [2], idonea ad autorizzare l'accesso dell'autorità incaricata dell'indagine ai dati in questione.

Con la sua sentenza, la Corte, riunita in Grande Sezione, giudica che la direttiva «vita privata e comunicazioni elettroniche», letta alla luce della Carta, osti ad una normativa nazionale, la quale permetta l'accesso delle autorità pubbliche a dati relativi al traffico o a dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca,

[1] Più precisamente, con l'articolo 15, paragrafo 1, della 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) (in prosieguo: la «direttiva "vita privata e comunicazioni elettroniche"»), letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).
[2] Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, punto 120; v. anche comunicato stampa n. 145/16.

accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica. Secondo la Corte, la durata del periodo per il quale l'accesso a tali dati è stato richiesto e la quantità o la natura dei dati disponibili per tale periodo non hanno alcuna incidenza al riguardo. Inoltre, la Corte considera che questa medesima direttiva, letta alla luce della Carta, osti ad una normativa nazionale che renda il pubblico ministero competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione al fine di condurre un'istruttoria penale.

Giudizio della Corte

Per quanto riguarda i presupposti in presenza dei quali l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione conservati dai fornitori di servizi di comunicazioni elettroniche può, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, essere concesso ad autorità pubbliche, in applicazione di una misura adottata ai sensi della direttiva «vita privata e comunicazioni elettroniche» [3], la Corte ricorda quanto da essa statuito nella sua sentenza La Quadrature du Net e a. [4]. Infatti, detta direttiva autorizza gli Stati membri ad adottare, tra l'altro agli scopi suddetti, misure legislative intese a limitare la portata dei diritti e degli obblighi previsti dalla direttiva medesima, e segnatamente l'obbligo di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico [5], unicamente a condizione che vengano rispettati i principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e i diritti fondamentali garantiti dalla Carta [6]. In tale contesto, la direttiva osta a misure legislative che impongano ai fornitori di servizi di comunicazione elettronica, in via preventiva, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

Per quanto concerne l'obiettivo della prevenzione, della ricerca, dell'accertamento e del perseguimento di reati, perseguito dalla normativa in questione, conformemente al principio di proporzionalità, la Corte considera che soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono idonei a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di permettere di trarre precise conclusioni sulla vita privata delle persone di cui trattasi, senza che altri fattori attinenti alla proporzionalità di una domanda di accesso, come la durata del periodo per il quale viene richiesto l'accesso a dati siffatti, possano avere come effetto che l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale sia tale da giustificare un accesso del genere.

Per quanto riguarda la competenza conferita al pubblico ministero ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione al fine di dirigere un'istruttoria penale, la Corte ricorda che spetta al diritto nazionale stabilire i presupposti in presenza dei quali i fornitori di servizi di comunicazioni elettroniche devono concedere alle autorità nazionali competenti l'accesso ai dati di cui essi dispongono. Tuttavia, per soddisfare il requisito di proporzionalità, tale normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino dei requisiti minimi, di modo che le persone i cui dati personali vengono in discussione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi. Tale normativa deve essere legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni sostanziali e procedurali possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario.

Secondo la Corte, 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 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

[3] Articolo 15, paragrafo 1, della direttiva «vita privata e comunicazioni elettroniche».
[4] Sentenza del 6 ottobre 2020, La Quadrature du Net e a.,C-511/18, C-512/18 e C-520/18, punti da 166 a 169; v. anche comunicato stampa n. 123/20
[5] Articolo 5 paragrafo 1, della direttiva «vita privata e comunicazioni elettroniche».
[6] In particolare, gli articoli 7, 8 e 11 nonché l'articolo 52, paragrafo 1, della Carta.

presentata, segnatamente, nel quadro di procedure di prevenzione o di accertamento di reati o di azioni penali instaurate. In caso di urgenza debitamente giustificata, il controllo deve intervenire entro breve termine.

A questo proposito, la Corte precisa che il controllo preventivo esige, tra l'altro, che il giudice o l'entità incaricata di effettuare tale controllo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie al fine di assicurare una conciliazione dei diversi interessi e diritti in gioco. Per quanto riguarda più in particolare un'indagine penale, un controllo siffatto esige che tale giudice o tale entità sia in grado di garantire un giusto equilibrio tra, da un lato, gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso. Qualora tale controllo venga effettuato non da un giudice bensì da un'entità amministrativa indipendente, quest'ultima deve godere di uno status che le permetta di agire nell'assolvimento dei propri compiti in modo obiettivo e imparziale, e deve a tale scopo essere al riparo da qualsiasi influenza esterna.

A giudizio della Corte, ne consegue che il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale. Orbene, ciò non si verifica nel caso di un pubblico ministero che, come nel caso del pubblico ministero estone, diriga il procedimento di indagine ed eserciti, se del caso, l'azione penale. Ne consegue che il pubblico ministero non è in grado di effettuare il suddetto controllo preventivo.

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: Eleonora Montserrat Pappalettere ☎ (+352) 4303 8575