

CLASSIFICAZIONE

DIRETTIVA 2016/680/UE –PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI A FINI DI PREVENZIONE, INDAGINE, ACCERTAMENTO O PERSEGUIMENTO DI REATI –RINVIO PREGIUDIZIALE DA PARTE DI TRIBUNALE AMMINISTRATIVO AUSTRIACO –ART. 4 –PRINCIPIO DELLA «MINIMIZZAZIONE DEI DATI» – ARTT. 7, 8, 47 E 52, PAR. 1, CDFUE –RISPETTO DELLA VITA PRIVATA E FAMILIARE – PROTEZIONE DEI DATI DI CARATTERE PERSONALE – PRINCIPIO DI LEGALITÀ – PRINCIPIO DI PROPORZIONALITÀ –TENTATIVO DI SBLOCCO DI UN TELEFONO CELLULARE DA PARTE DELLE AUTORITÀ DI POLIZIA PER ACCEDERE AI DATI CONTENUTI NEL TELEFONO–NON NECESSITÀ DELLA GRAVITÀ DEL REATO – NECESSITÀ DI AUTORIZZAZIONE PREVENTIVA DA PARTE DI UN GIUDICE O DI UN’AUTORITÀ AMMINISTRATIVA INDIPENDENTE – ART. 13 E 54 DELLA DIRETTIVA 2016/680/UE – DIRITTO ALL’INFORMAZIONE DELL’IMPUTATO – NECESSITÀ –LIMITAZIONI TEMPORALI PER LA SALVAGUARDIA DELLE INDAGINI.

PRONUNCIA SEGNALATA

Corte di giustizia, GrandeCamera,C.G. c. *Bezirkshauptmannschaft Landeck* del 4 ottobre 2024 (C-548/21).

RIFERIMENTI NORMATIVIEUROUNITARI

Artt.1,3,5 e 15, paragrafo 1, direttiva 2002/58/CE,1, paragrafi 1 e 2, 2, paragrafi 1 e 3, 3,4, paragrafo 1, 6, 10, 13, 54, direttiva 2016/680/UE, 7, 8, 11, 41, 47 e 52, paragrafo 1, CDFUE.

RIFERIMENTI NORMATIVI COSTITUZIONALI

Artt. 15, 24 e 111 Cost.

RIFERIMENTI GIURISPRUDENZIALI

SENTENZE DELLA CORTE DI GIUSTIZIA.

CGUE, 18 giugno 2024, Bundesrepublik Deutschland, C-753/22; CGUE, 18 giugno 2024, Generalstaatsanwaltschaft Hamm, C-352/22; CGUE, 30 gennaio 2024, Direktor na Glavna direktsia "Natsionalna politsia" pri MVR -Sofia, C-118/22; CGUE, 21 dicembre 2023, European Superleague Company, C-333/21; CGUE, 16 novembre 2023, Ligue des droits humains, C-333/22; CGUE, 31 gennaio 2023, Puig Gordi e a., C-158/21; CGUE, 17 novembre 2022, Spetsializirana prokuratura, C-350/21; CGUE, 2 marzo 2021, Prokurator, C-746/18; CGUE, 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18; CGUE, 2 ottobre 2019, Ministerio Fiscal, C-270/16.

ABSTRACT

La Corte di Giustizia, adita in sede di rinvio pregiudiziale dal Tribunale amministrativo regionale del Tirolo, ha ritenuto che:

-l'articolo 4, paragrafo 1, lettera c), della Direttiva 2016/680/UE (sulla tutela delle persone fisiche riguardo al trattamento dei dati personali in ambito penale), letto alla luce degli articoli 7, 8 e 52, paragrafo 1, CDFUE, **non osta ad una normativa nazionale che riconosca alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, per scopi di prevenzione, indagine, accertamento e perseguimento di reati, anche non necessariamente gravi, purché tale normativa definisca in modo sufficientemente preciso la natura o le categorie dei reati interessati, garantisca il rispetto del principio di proporzionalità e sottoponga l'esercizio di tale facoltà – salvi i casi di urgenza debitamente motivati – ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente;**

-gli artt. 13 e 54 della direttiva 2016/680/UE ostano ad una normativa nazionale che autorizzi le autorità competenti a tentare l'accesso ai dati contenuti in un telefono cellulare senza informare la persona interessata dei motivi posti a fondamento dell'autorizzazione ad accedere a tali dati, rilasciata da un giudice o da un organo amministrativo indipendente, a partire dal momento in cui la comunicazione di tali informazioni non sia più tale da compromettere le indagini.

IL CASO

Nel corso di un controllo, **la polizia austriaca ha sequestrato il telefono cellulare** di C.G., destinatario di un pacco contenente 85 grammi di *cannabis*. Al fine di accedere ai dati in esso contenuti, le autorità straniere **hanno tentato ripetutamente di sbloccare il dispositivo**, agendo in **assenza di qualsivoglia autorizzazione giudiziale**, senza documentare in alcun modo i tentativi di sblocco e **mancando di informare di ciò l'interessato**, venutone a conoscenza soltanto nell'ambito del procedimento di impugnazione del provvedimento di sequestro.

Secondo gli artt. 18 e 99 del codice di procedura penale austriaco, infatti, nell'ambito di un'indagine penale, la polizia giudiziaria può ottenere, senza l'autorizzazione di un giudice o di un organo amministrativo, l'accesso completo ed incontrollato a tutti i dati contenuti in un telefono cellulare, senza alcun obbligo di documentare le misure adottate né di informare il proprietario in ordine all'esistenza di tali misure.

Il giudice del rinvio pregiudiziale ha evidenziato alla Corte di giustizia che, nel caso di specie, il reato contestato costituisce una contravvenzione ed ha sollevato **una prima questione** pregiudiziale, riferita alla necessità, o meno, di limitare l'accesso da parte delle autorità pubbliche ai dati memorizzati nei telefoni cellulari – a fini di prevenzione, indagine, accertamento e perseguimento dei reati – alla sola lotta contro **reati gravi**.

Il Tribunale austriaco ha sollevato anche **una seconda questione** pregiudiziale, inerente alla conformità al diritto dell'Unione di una normativa nazionale che consenta alle autorità preposte alla sicurezza di accedere in maniera incontrollata e completa ai dati conservati in un dispositivo elettronico, senza **l'autorizzazione di un giudice o di un'autorità amministrativa indipendente**. Si sottolinea, infatti, che, alla luce del combinato disposto tra gli artt. 18 e 99 del codice di procedura penale austriaco, nell'ambito di un procedimento di indagine penale, la polizia giudiziaria può ottenere, senza alcuna autorizzazione, l'accesso completo ed incontrollato a tutti i dati contenuti in un telefono cellulare.

Infine, il giudice del rinvio, con **una terza questione**, ha chiesto di conoscere se, in osservanza al diritto dell'Unione, vi sia necessità o meno che **l'indagato sia informato** dei tentativi di accesso ai dati contenuti nel suo telefono cellulare, al fine di poter esercitare il diritto ad un ricorso effettivo previsto dall'art. 47 CDFUE.

LA DECISIONE

La Corte di Giustizia, esaminando congiuntamente le prime due questioni sollevate, **ha ritenuto che l'articolo 4, par. 1, lettera c), della direttiva 2016/680/UE non ostia** una normativa nazionale che riconosca alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, a fini di prevenzione e perseguimento di reati, **anche non necessariamente gravi, a condizione che:** **a)** tale normativa definisca in modo sufficientemente preciso la categoria dei reati in questione; **b)** rispetti il principio di proporzionalità; **c)** subordini l'esercizio di tale facoltà al controllo preventivo di un giudice o di un organo amministrativo indipendente.

I giudici di Lussemburgo, muovendo dall'**art. 4, paragrafo 1, lettera c), della Direttiva 2016/680/UE, che fissa il principio di «minimizzazione dei dati», quale corollario del principio di proporzionalità**, e dalla **ratio della direttiva 2016/460/UE** – che, letta alla luce degli artt. 7 e 8 CDFUE, mira a **garantire, nello specifico, un elevato livello di protezione dei dati personali delle persone fisiche – hanno fissato alcuni importanti punti interpretativi**, così sintetizzabili:

1) l'accesso **all'insieme dei dati** contenuti in un telefono cellulare **può costituire un'ingerenza** grave, o addirittura particolarmente grave, nei diritti fondamentali della persona interessata, potendo tali dati includere messaggi, fotografie ed altre informazioni di vario tipo che potrebbero, se del caso, consentire di trarre conclusioni molto precise riguardo alla **vita privata** di una persona, anche relativamente a dati particolarmente sensibili;

2) l'accesso ai dati contenuti in un telefono cellulare **non può essere necessariamente limitato alla lotta contro i reati gravi**. Ritenere che solo la lotta contro i reati gravi possa giustificare l'accesso a dati contenuti in un telefono cellulare limiterebbe indebitamente i poteri di indagine delle autorità competenti, così determinando un possibile aumento del rischio di

impunità per i reati in generale, e, dunque, un rischio per la creazione di uno spazio di libertà, sicurezza e giustizia nell'Unione;

3) qualsiasi limitazione all'esercizio di un diritto fondamentale, pur consentita nell'ottica del necessario bilanciamento degli interessi, **deve essere prevista dalla legge e proporzionata**, spettando dunque al legislatore nazionale definire in modo sufficientemente preciso, in particolare, la natura o le categorie dei reati in relazione ai quali è possibile consentirla;

4) per garantire il rispetto del principio di proporzionalità in ciascun caso concreto, l'accesso ai dati personali da parte delle autorità nazionali competenti, che comporti il rischio di un'ingerenza grave nei diritti fondamentali della persona interessata, deve essere sottoposto ad un **controllo preventivo effettuato da un organo giurisdizionale o da un organo amministrativo indipendente**, avente lo scopo di garantire un giusto equilibrio tra gli interessi legittimi connessi alle esigenze investigative nell'ambito della lotta alla criminalità e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali;

5) la pertinente normativa dell'Unione si applica non solo in caso di accesso riuscito ai dati personali contenuti in un telefono cellulare, ma anche al tentativo di accesso;

6) gli artt. 13 e 54 della direttiva 2016/680/UE, letti alla luce dell'art. 47 e dell'art. 52, paragrafo 1, CDFUE, **ostano ad una normativa nazionale che autorizza** le autorità competenti a **tentare di accedere ai dati contenuti in un telefono cellulare senza informare** la persona interessata dei motivi posti a base dell'autorizzazione all'accesso, rilasciata da un giudice o da un organo amministrativo indipendente, a partire dal momento in cui la comunicazione di tali informazioni non sia più tale da compromettere le indagini condotte da tali autorità.

Infatti, sottolinea la Corte, il diritto ad un ricorso giurisdizionale effettivo, quale quello garantito dall'art. 47 CDFUE, esige, in linea di principio, che l'interessato – al fine di poter difendere i propri diritti nelle migliori condizioni possibili e di poter ottenere, eventualmente, un vaglio di legittimità di tale decisione – sia in grado di conoscere le argomentazioni su cui si fonda la decisione adottata nei suoi confronti, ivi comprese quelle informazioni aggiuntive necessarie all'esercizio dei propri diritti di difesa, cui fa riferimento, soprattutto nei casi in cui i dati personali siano raccolti all'insaputa del titolare, l'art. 13 della direttiva in esame.

Ne deriva che **nessuna normativa nazionale che escluda, in generale, qualsiasi diritto di ottenere informazioni potrà ritenersi conforme al diritto dell'Unione**: tale affermazione di radicale incompatibilità era stata già formulata nella sentenza CGUE, 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21.

OSSERVAZIONI

La Corte di giustizia, con la sentenza in commento, ha chiarito quale sia l'interpretazione corretta del diritto dell'Unione europea sui poteri di accesso ai dati personali contenuti in un dispositivo elettronico (cellulare) in caso di indagine penale e lo ha fatto probabilmente meglio

che in altre occasioni e, pare anche, con una maggior consapevolezza generale degli interessi in gioco e dei diritti fondamentali da bilanciare.

La Corte ha inequivocabilmente affermato, infatti, che **l'accesso, o anche il solo tentativo di accesso, delle autorità di polizia**, impegnate in indagini per l'accertamento o la prevenzione di reati, **ai dati contenuti in un telefono cellulare non è necessariamente limitato alla lotta contro i reati gravi**, segnalando, parallelamente, i requisiti che la legislazione nazionale deve avere per rispettare il diritto dell'Unione coinvolto nel bilanciamento di interessi inevitabilmente da valutare.

I requisiti sono di immediata evidenza quanto alle ricadute sulla **tutela, anzitutto del principio di legalità e di proporzionalità** (quest'ultimo espresso anche attraverso il **principio di cd. "minimizzazione dei dati"**, vale a dire che i dati personali siano adeguati, pertinenti e **non eccessivi rispetto alle finalità** per le quali sono trattati: cfr. § 79 e la sentenza CGUE, 30 gennaio 2024, Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia, C-118/22), entro l'ambito dei quali devono muoversi attività che la Corte non esita a definire foriere di ingerenze anche particolarmente gravi nei diritti fondamentali individuali.

Anzitutto, **il legislatore**, ancorché possa prevedere l'accesso ai dati personali a fini di accertamento di qualsiasi tipologia di reato, anche non soltanto di quelli "gravi", **deve individuare normativamente** in modo chiaro la natura o le categorie dei reati in relazione ai quali è possibile consentire l'attività di indagine.

Quindi, **è necessario che tali attività siano preventivamente autorizzate da un organo giurisdizionale o da un organo amministrativo indipendente**: il provvedimento di "previa autorizzazione", proveniente da un soggetto "qualificato" secondo i caratteri indicati dalla CGUE, costituisce strumento di tutela del principio di proporzionalità e del giusto equilibrio tra gli interessi legittimi connessi alle esigenze investigative nell'ambito della lotta alla criminalità e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali.

Infine, **deve essere garantito legislativamente il diritto alla comunicazione all'interessato** di tali attività di indagine potenzialmente lesive della tutela della vita privata, prevedendo l'obbligo di darne notizia, **una volta che non vi siano più rischi di compromissione delle indagini**; l'obbligo di comunicazione, infatti, è strumentale alla garanzia del diritto ad un ricorso giurisdizionale effettivo.

Nel caso di specie, la Corte ha sottolineato che l'interessato sapeva che il suo telefono cellulare era stato sequestrato, quando le autorità di polizia austriache hanno tentato invano di sbloccarlo al fine di accedere ai dati in esso contenuti, sicché informarlo del fatto che tali autorità avrebbero cercato di accedere ai suoi dati non avrebbe rischiato di compromettere le indagini.

Egli, dunque, avrebbe dovuto essere "preventivamente" informato (così si esprime la sentenza in commento al par. 122). Tale sottolineatura, invero, pur rapida nella motivazione della decisione, apre scenari ulteriori di tipo procedurale sulla necessità di distinguere tra casi nei quali la comunicazione possa essere successiva e casi nei quali debba essere preventiva.

E ciò, in qualche modo, andrà coordinato con l'affermazione, presente nel dispositivo ed in più punti della motivazione della decisione, secondo cui l'obbligo di informazione deve avvenire "nell'ambito delle procedure nazionali applicabili", che lascerebbe intendere una certa libertà del legislatore nazionale di prevedere il modo in cui si attingerà in concreto detto obbligo.

In passato, si ricorderà che la Corte di giustizia aveva espresso la propria idea di "bilanciamento di interessi" in materia di trattamento dati e indagini penali nella **sentenza del 2 marzo 2021, Prokuratuur C-746/18**, riferita alla **Direttiva 2002/58/CE** del Parlamento europeo e del Consiglio del 12 luglio 2002 (**trattamento dei dati personali** e alla tutela della vita privata nel **settore delle comunicazioni elettroniche**, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009).

La sentenza *Prokuratuur*, rispondendo ad un rinvio pregiudiziale, ha affermato che il diritto dell'Unione (in particolare, l'articolo 15 della direttiva 2002/58/UE relativa alla vita privata e alle comunicazioni elettroniche, letto alla luce degli articoli 7, 8, 11 e 52 della Carta di Nizza) osta a una disciplina nazionale che: a) non circoscriva **l'accesso da parte delle autorità pubbliche ai dati relativi alle comunicazioni telematiche o telefoniche effettuate da un utente** o quelli relativi alla ubicazione delle apparecchiature da costui utilizzate alle sole ipotesi di «procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica»; b) affidi, nel corso di un procedimento penale, la competenza ad autorizzare l'accesso a tali dati al pubblico ministero, organo che – per quanto garante della legalità nella fase delle indagini, dovendo esso ricercare anche gli elementi favorevoli all'indagato – non è ritenuto terzo ed imparziale in quanto è comunque parte nel procedimento.

Dopo tale pronuncia, il governo italiano è intervenuto con un decreto-legge (30 settembre 2021 n. 132, poi convertito in legge) a disciplinare, dunque, l'articolo 132 del d.lgs. 196/2003 – norma fondamentale in materia – che prevede oggi, in sintesi, l'autorizzazione all'acquisizione dei dati relativi alle comunicazioni telematiche o telefoniche da parte del giudice e non più solo del pubblico ministero (il quale, tuttavia, può agire d'urgenza con necessità di convalida, a pena di inutilizzabilità, entro 48 ore da parte del giudice) ed in presenza di sufficienti indizi circa la commissione di reati puniti con pena detentiva non inferiore nel massimo a tre anni oppure e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi.

Successivamente alla sentenza *Prokuratuur*, un'altra pronuncia della **Grande Sezione della Corte di giustizia, del 30 aprile 2024, causa C-178/22 nel rinvio pregiudiziale proposto dal GIP del Tribunale di Bolzano**, ha stabilito che la disciplina italiana può considerarsi compatibile con la normativa europea, a condizione che, di fronte a una richiesta di acquisizione di dati «idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente di un mezzo di comunicazione elettronica», il giudice «abbia la possibilità di negare detto accesso se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato

manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato».

Ebbene, rispetto a tali due pronunce, nella sentenza più recente del 4 ottobre 2024, oggi in commento, la Corte di Lussemburgo – sebbene nel **diverso ambito** della possibilità di accedere ai dati contenuti in un telefono cellulare e non in relazione alle **acquisizioni di dati da gestori di servizi telefonici o telematici** – sembra aver ulteriormente affinato la sua interpretazione, quanto al necessario bilanciamento tra esigenze pubbliche, collegate alla necessità di garantire la risposta penale dello Stato dinanzi al crimine, ed esigenze individuali di tutela del diritto alla riservatezza ed alla vita privata di chi possa essere comunque coinvolto nelle indagini.

Secondo la CGUE deve essere riconosciuta **la possibilità di accedere ai dati contenuti in un telefono cellulare, per scopi di prevenzione, indagine, accertamento e perseguimento di reati, anche non necessariamente gravi**, ribadendo le condizioni di legittimità dell'acquisizione da un punto di vista generale: è necessario che la normativa interna definisca in modo sufficientemente preciso la natura o le categorie dei reati interessati, garantisca il rispetto del principio di proporzionalità e sottoponga l'esercizio di tale facoltà – salvi i casi di urgenza debitamente motivati – ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

Riserva di legge, riserva di intervento giurisdizionale e proporzionalità, dunque, si rivelano in modo chiaro i parametri essenziali ai quali abbinare la legalità dell'azione investigativa in materia di acquisizione dei dati telefonici o informatici.

Gli echi delle indicazioni ermeneutiche della Corte di giustizia si ritrovano nella giurisprudenza della Corte di cassazione, soprattutto nelle recenti sentenze Sez. U, n. 23755 del 29/2/2024, Gjuzi Ermal, Rv. 286573 e Sez. U, n. 23756 del 29/2/2024, Giorgi, Rv. 286589.

La giurisprudenza di legittimità ha già collegato sanzioni di inutilizzabilità dei dati acquisiti in violazione degli obblighi di legge introdotti a seguito delle pronunce della Corte di giustizia (in particolare, Sez. 6, n. 15836 del 11/1/2023, Berera, Rv. 284590 ha affermato l'inutilizzabilità nel giudizio abbreviato dei **dati di geolocalizzazione** relativi a utenze telefoniche o telematiche, contenuti **nei tabulati** acquisiti dalla polizia giudiziaria in assenza del decreto di autorizzazione dell'Autorità giudiziaria, **in violazione dell'art. 132, comma 3, d.lgs. 30 giugno 2003, n. 196**, in quanto prove lesive del diritto alla segretezza delle comunicazioni costituzionalmente tutelato e, pertanto, affette da inutilizzabilità patologica, non sanata dalla richiesta di definizione del giudizio con le forme del rito alternativo).