Edizione provvisoria

SENTENZA DELLA CORTE (Grande Sezione)

2 marzo 2021 (*)

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Fornitori di servizi di comunicazioni elettroniche – Riservatezza delle comunicazioni – Limitazioni – Articolo 15, paragrafo 1 – Articoli 7, 8 e 11, nonché articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea – Normativa che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione da parte dei fornitori di servizi di comunicazioni elettroniche – Accesso delle autorità nazionali ai dati conservati per finalità di indagine – Lotta contro la criminalità in generale – Autorizzazione concessa dal pubblico ministero – Utilizzazione dei dati nel quadro del processo penale come elementi di prova – Ammissibilità»

Nella causa C-746/18,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Riigikohus (Corte suprema, Estonia), con decisione del 12 novembre 2018, pervenuta in cancelleria il 29 novembre 2018, nel procedimento penale contro

H.K.,

con l'intervento di:

Prokuratuur,

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, R. Silva de Lapuerta, vicepresidente, J.-C. Bonichot, A. Arabadjiev, A. Prechal e L. Bay Larsen, presidenti di sezione, T. von Danwitz (relatore), M. Safjan, K. Jürimäe, C. Lycourgos e P.G. Xuereb, giudici,

avvocato generale: G. Pitruzzella

cancelliere: C. Strömholm, amministratrice

vista la fase scritta del procedimento e in seguito all'udienza del 15 ottobre 2019,

considerate le osservazioni presentate:

– per H.K., da S. Reinsaar, vandeadvokaat;

– per il Prokuratuur, da T. Pern e M. Voogma, in qualità di agenti;

– per il governo estone, da N. Grünberg, in qualità di agente;

– per il governo danese, da J. Nymann-Lindegren e M.S. Wolff, in qualità di agenti;

– per l'Irlanda, da M. Browne, G. Hodge e J. Quaney nonché da A. Joyce, in qualità di agenti, assistiti da D. Fennelly, barrister;

– per il governo francese, inizialmente da D. Dubois, D. Colas, E. de Moustier e A.-L. Desjonquères, successivamente da D. Dubois, E. de Moustier e A.-L. Desjonquères, in qualità di agenti;

– per il governo lettone, inizialmente da V. Kalniņa e I. Kucina, successivamente da V. Soņeca e V. Kalniņa, in qualità di agenti;

– per il governo ungherese, da M.Z. Fehér e A. Pokoraczki, in qualità di agenti;

– per il governo polacco, da B. Majczyna, in qualità di agente;

– per il governo portoghese, da L. Inez Fernandes, P. Barros da Costa, L. Medeiros e I. Oliveira, in qualità di agenti;

– per il governo finlandese, da J. Heliskoski, in qualità di agente;

– per il governo del Regno Unito, da S. Brandon e Z. Lavery, in qualità di agenti, assistiti da G. Facenna, QC, e da C. Knight, barrister;

– per la Commissione europea, inizialmente da H. Kranenborg, M. Wasmeier, P. Costa de Oliveira e K. Toomus, successivamente da H. Kranenborg, M. Wasmeier e E. Randvere, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 21 gennaio 2020,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'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 2002/58»), 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 Tale domanda è stata presentata nell'ambito di un procedimento penale instaurato a carico di H.K. per le imputazioni di furto, di uso della carta bancaria di un terzo e di violenza nei confronti di persone partecipanti ad un procedimento giudiziario.

Contesto normativo

Diritto dell'Unione

3 I considerando 2 e 11 della direttiva 2002/58 enunciano quanto segue:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(...)

(11) La presente direttiva, analogamente alla direttiva [95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31)], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto [dell'Unione]. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza, la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali [firmata a Roma il 4 novembre 1950], come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali».

4 L'articolo 2 della direttiva 2002/58, intitolato «Definizioni», recita:

«Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva [95/46] e alla direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro) [(GU 2002, L 108, pag. 33)].

Si applicano inoltre le seguenti definizioni:

a) "utente": qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;

(...)».

5 L'articolo 5 della direttiva 2002/58, intitolato «Riservatezza delle comunicazioni», recita:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite [una] rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

(...)

3. Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

6 L'articolo 6 della direttiva 2002/58, dal titolo «Dati sul traffico», così dispone:

«1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica [di comunicazioni] o di un servizio [di comunicazioni elettroniche accessibili al pubblico] devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi (...) o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia espresso preliminarmente il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

(...)

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori dell[e] ret[i] pubblic[he] di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività.

(...)».

7 L'articolo 9 della direttiva 2002/58, dal titolo «Dati relativi all'ubicazione diversi dai dati relativi al traffico», prevede, al paragrafo 1, quanto segue:

«Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. (...)».

8 L'articolo 15 di detta direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», recita, al paragrafo 1:

«Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], 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; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea».

Diritto estone

Legge relativa alle comunicazioni elettroniche

9 L'articolo 111[1] dell'elektroonilise side seadus (legge relativa alle comunicazioni elettroniche, RT I 2004, 87, 593; RT I, 22.05.2018, 3), nella versione applicabile ai fatti di cui al procedimento principale (in prosieguo: la «legge relativa alle comunicazioni elettroniche»), intitolato «Obbligo di conservare i dati», prevede quanto segue:

«(...)

(2) I fornitori di servizi di telefonia fissa e di telefonia mobile nonché di servizi di rete di telefonia fissa e di telefonia mobile sono obbligati a conservare i seguenti dati:

1) il numero telefonico del chiamante nonché il nome e il recapito dell'abbonato;

2) il numero telefonico del chiamato nonché il nome e il recapito dell'abbonato;

3) in caso di utilizzo di servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero selezionato nonché il nome e il recapito dell'abbonato;

4) la data e l'ora di inizio e fine di una chiamata;

5) il servizio di telefonia fissa o mobile utilizzato;

6) il codice identificativo internazionale di abbonato di telefonia mobile (*International Mobile Subscriber Identity* – IMSI) del soggetto chiamante e del soggetto chiamato;

7) il codice identificativo internazionale di apparecchiatura di telefonia mobile (*International Mobile Equipment Identity* – IMEI) del soggetto chiamante e del soggetto chiamato;

8) l'etichetta di ubicazione all'inizio della chiamata;

9) i dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione nel periodo in cui vengono conservati i dati sulle comunicazioni;

10) nel caso di servizi prepagati anonimi, la data e l'ora della prima attivazione della carta e l'etichetta di ubicazione del luogo in cui è stata effettuata l'attivazione;

(…)

(4) I dati indicati nei paragrafi 2 e 3 del presente articolo vengono conservati per un periodo di un anno dalla data della comunicazione, se tali dati vengono creati o trattati nell'ambito della fornitura di un servizio di comunicazione. (...)

(...)

(11) I dati indicati nei paragrafi 2 e 3 del presente articolo vengono comunicati:

1) ai sensi del kriminaalmenetluse seadustik [(codice di procedura penale)], a un'autorità inquirente, a un'autorità autorizzata ad applicare misure di sorveglianza, al pubblico ministero e al giudice;

(...)».

Codice di procedura penale

10 L'articolo 17 del codice di procedura penale (kriminaalmenetluse seadustik, RT I 2003, 27, 166; RT I, 31.05.2018, 22) dispone quanto segue:

«(1) Sono parti del procedimento giudiziario: il pubblico ministero, (...).

(...)».

11 L'articolo 30 del codice suddetto ha il seguente tenore:

«(1) Il pubblico ministero dirige il procedimento istruttorio, di cui assicura la legittimità e l'efficacia, e rappresenta la pubblica accusa in giudizio.

(2) I poteri del pubblico ministero nel procedimento penale vengono esercitati, in nome del pubblico ministero, da un procuratore, il quale agisce in modo indipendente ed è soggetto soltanto alla legge».

12 L'articolo 90^1 del medesimo codice prevede quanto segue:

«(...)

(2) L'autorità incaricata dell'indagine può, con l'autorizzazione del pubblico ministero nel corso del procedimento istruttorio, o con l'autorizzazione del giudice nel corso del processo, richiedere a un fornitore di servizi di comunicazione elettronica i dati elencati nell'articolo 111^1, paragrafi 2 e 3, della legge relativa alle comunicazioni elettroniche, non menzionati nel precedente paragrafo 1. Nella suddetta autorizzazione alla richiesta di dati viene specificato il periodo con riferimento al quale la richiesta di dati viene autorizzata, con l'esatta indicazione delle date.

(3) Ai sensi del presente articolo, i dati possono essere richiesti soltanto laddove ciò sia indispensabile al fine di raggiungere lo scopo del procedimento penale».

13 L'articolo 211 del codice di procedura penale dispone quanto segue:

«(1) Lo scopo del procedimento istruttorio è di raccogliere prove e di predisporre le altre condizioni necessarie per lo svolgimento di un processo.

(2) Nel procedimento istruttorio l'autorità incaricata dell'indagine e il pubblico ministero verificano gli elementi a carico e quelli a discarico raccolti nei confronti del sospettato o dell'indagato».

Legge relativa al pubblico ministero

14 L'articolo 1 della prokuratuuriseadus (legge relativa al pubblico ministero, RT I 1998, 41, 625; RT I, 06.07.2018, 20), nella versione applicabile ai fatti di cui al procedimento principale, prevede quanto segue:

«(1) Il pubblico ministero è un'autorità soggetta alla sfera di competenza del Ministero della Giustizia, la quale partecipa alla pianificazione delle misure di sorveglianza necessarie per la lotta e l'accertamento dei reati, dirige la fase istruttoria, di cui assicura la legittimità e l'efficacia, rappresenta la pubblica accusa in giudizio ed esercita le ulteriori funzioni assegnategli dalla legge.

(1^1) Il pubblico ministero, nell'esercizio delle funzioni assegnategli dalla legge, è indipendente e agisce conformemente alla presente legge, alle altre leggi e agli atti normativi emanati sulla base di tali leggi.

(...)».

15 L'articolo 2, paragrafo 2, di detta legge è così formulato:

«Il procuratore, nell'esercizio delle proprie funzioni, è indipendente e agisce esclusivamente secondo la legge e secondo il proprio convincimento».

Procedimento principale e questioni pregiudiziali

16 Con decisione del 6 aprile 2017, H.K. è stata condannata dal Viru Maakohus (Tribunale di primo grado di Viru, Estonia) a una pena detentiva di due anni per aver commesso, tra il 17 gennaio 2015 e il 1° febbraio 2016, vari furti di beni (di valore compreso tra EUR 3 e EUR 40) nonché di somme di denaro (per importi compresi tra EUR 5,20 e EUR 2 100, per aver utilizzato la carta bancaria di un terzo, causando a quest'ultimo un danno di EUR 3 941,82, e per aver compiuto atti di violenza nei confronti di persone partecipanti ad un procedimento giudiziario a suo carico.

17 Ai fini della condanna di H.K. per tali reati, il Viru Maakohus (Tribunale di primo grado di Viru) si è fondato, tra l'altro, su vari processi verbali redatti in base a dati relativi a comunicazioni elettroniche, ai sensi dell'articolo 111^1, paragrafo 2, della legge relativa alle comunicazioni elettroniche, che l'autorità incaricata dell'indagine aveva raccolto presso un fornitore di servizi di telecomunicazioni elettroniche nel corso del procedimento istruttorio, dopo aver ottenuto, ai sensi dell'articolo 90^1 del codice di procedura penale, varie autorizzazioni a tal fine dal Viru Ringkonnaprokuratuur (Procura distrettuale di Viru, Estonia). Tali autorizzazioni, concesse il 28 gennaio e il 2 febbraio 2015, il 2 novembre 2015, nonché il 25 febbraio 2016, riguardavano i dati relativi a vari numeri di telefono di H.K. e diversi codici internazionali di identificazione di apparecchiatura di telefonia mobile di quest'ultima, per il periodo dal 1º gennaio al 2 febbraio 2015, per il giorno 21 settembre 2015, nonché per il periodo dal 1º marzo 2015 al 19 febbraio 2016.

18 H.K. ha proposto appello contro la sentenza del Viru Maakohus (Tribunale di primo grado di Viru) dinanzi alla Tartu Ringkonnakohus (Corte d'appello di Tartu, Estonia), che ha respinto tale appello con decisione del 17 novembre 2017.

19 H.K. ha proposto un ricorso per cassazione avverso quest'ultima decisione dinanzi alla Riigikohus (Corte suprema, Estonia), contestando, tra l'altro, l'ammissibilità dei processi verbali redatti in base ai dati ottenuti presso il fornitore di servizi di comunicazioni elettroniche. A suo avviso, risulterebbe dalla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970; in prosieguo: la «sentenza Tele2»), che le disposizioni dell'articolo 111^1 della legge relativa alle comunicazioni elettroniche che prevedono l'obbligo dei fornitori di servizi di conservare dati relativi alle comunicazioni, nonché l'utilizzazione di tali dati ai fini della sua condanna, sono contrari all'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.

20 Secondo il giudice del rinvio, si pone la questione se i processi verbali redatti in base ai dati contemplati dall'articolo 111^1, paragrafo 2, della legge relativa alle comunicazioni elettroniche possano essere considerati come costituenti elementi di prova ammissibili. Detto giudice fa osservare che l'ammissibilità

dei processi verbali in discussione nel procedimento principale quali elementi di prova impone di stabilire in quale misura la raccolta dei dati in base ai quali i suddetti processi verbali sono stati redatti sia stata conforme all'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.

21 Detto giudice considera che la risposta a tale questione presuppone di stabilire se il suddetto articolo 15, paragrafo 1, letto alla luce della Carta, debba essere interpretato nel senso che l'accesso delle autorità nazionali a dati che consentano di identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile di un sospettato, di determinare la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare il materiale di comunicazione mobile utilizzato, costituisce un'ingerenza nei diritti fondamentali in questione di gravità tale che tale accesso dovrebbe essere limitato alla lotta contro le forme gravi di criminalità, indipendentemente dal periodo per il quale le autorità nazionali hanno richiesto l'accesso ai dati conservati.

22 Il giudice del rinvio ritiene tuttavia che la durata di tale periodo costituisca un elemento essenziale per valutare la gravità dell'ingerenza consistente nell'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione. Pertanto, qualora detto periodo sia molto breve o la quantità di dati raccolti sia molto limitata, occorrerebbe chiedersi se l'obiettivo della lotta contro la criminalità in generale, e non soltanto della lotta contro le forme gravi di criminalità, possa giustificare una siffatta ingerenza.

23 Infine, il giudice del rinvio nutre dubbi quanto alla possibilità di considerare il pubblico ministero estone come un'autorità amministrativa indipendente, ai sensi del punto 120 della sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), che può autorizzare l'accesso dell'autorità incaricata dell'indagine a dati relativi alle comunicazioni elettroniche come quelli di cui all'articolo 111[1], paragrafo 2, della legge relativa alle comunicazioni elettroniche.

24 Il pubblico ministero dirigerebbe il procedimento istruttorio, garantendo al contempo la legalità e l'efficacia di quest'ultimo. Poiché l'obiettivo di tale procedimento è, in particolare, la raccolta di prove, l'autorità incaricata dell'indagine e il pubblico ministero verificherebbero gli elementi a carico e gli elementi a discarico raccolti contro qualsiasi persona sospettata o indagata. Se il pubblico ministero è convinto che siano state raccolte tutte le prove necessarie, esso eserciterebbe l'azione penale nei confronti dell'accusato. Le competenze del pubblico ministero verrebbero esercitate in suo nome da un procuratore che agisce in modo indipendente, così come risulterebbe dall'articolo 30, paragrafi 1 e 2, del codice di procedura penale, nonché dagli articoli 1 e 2 della legge relativa al pubblico ministero.

25 In tale contesto, il giudice del rinvio rileva che i suoi dubbi riguardo all'indipendenza richiesta dal diritto dell'Unione sono principalmente dovuti al fatto che il pubblico ministero non solo dirige il procedimento istruttorio, ma rappresenta anche la pubblica accusa nel processo, essendo tale autorità, ai sensi del diritto nazionale, parte nel procedimento penale.

26 Alla luce di tali circostanze, il Riigikohus (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1, della direttiva [2002/58] debba essere interpretato, alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della [Carta], nel senso che, in un procedimento penale, l'accesso di autorità nazionali a dati che consentano di rintracciare e identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile del sospettato, di determinare la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare il materiale di comunicazione mobile utilizzato, costituisce un'ingerenza nei diritti fondamentali sanciti dai suddetti articoli della Carta di gravità tale che detto accesso debba essere limitato, nel contesto della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati, alla lotta contro le forme gravi di criminalità, indipendentemente dal periodo al quale si riferiscono i dati conservati cui le autorità nazionali hanno accesso.

2) Se l'articolo 15, paragrafo 1, della direttiva [2002/58] debba essere interpretato, sulla scorta del principio di proporzionalità enunciato nella [sentenza del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788)], punti da 55 a 57, nel senso che, qualora la quantità dei dati menzionati nella prima questione, ai quali le autorità nazionali hanno accesso, non sia grande (sia per il tipo di dati che per la loro estensione nel tempo), la conseguente ingerenza nei diritti fondamentali può essere giustificata, in generale, dall'obiettivo della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati, e che quanto più notevole è la quantità di dati cui le autorità nazionali hanno accesso, tanto più gravi devono essere i reati perseguiti mediante tale ingerenza.

3) Se il requisito indicato nel secondo punto del dispositivo della [sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)], secondo cui l'accesso ai dati da parte delle autorità nazionali competenti dev'essere soggetto ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, implichi che l'articolo 15, paragrafo 1, della direttiva [2002/58] deve essere interpretato nel senso che può considerarsi come un'autorità amministrativa indipendente il pubblico ministero, il quale dirige il procedimento istruttorio e che, per legge, è tenuto ad agire in modo indipendente, restando soggetto soltanto alla legge e verificando, nell'ambito del procedimento istruttorio, sia gli elementi a carico sia quelli a discarico relativi all'indagato, ma che successivamente, nel procedimento giudiziario, rappresenta la pubblica accusa».

Sulle questioni pregiudiziali

Sulla prima e sulla seconda questione

27 Con le sue questioni pregiudiziali prima e seconda, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se 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, debba essere interpretato nel senso che esso osta a una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di 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, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità e dalla natura dei dati disponibili per tale periodo.

28 A questo proposito, risulta dalla domanda di pronuncia pregiudiziale che, come confermato dal governo estone all'udienza, i dati ai quali l'autorità nazionale incaricata dell'indagine ha avuto accesso nella causa di cui al procedimento principale sono quelli indicati ai sensi dell'articolo 111[1], paragrafi 2 e 4, della legge relativa alle comunicazioni elettroniche, i quali impongono ai fornitori di servizi di comunicazioni elettroniche un obbligo di conservare in maniera generalizzata e indifferenziata i dati relativi al traffico e i dati relativi all'ubicazione per quanto riguarda la telefonia fissa e mobile, per un periodo di un anno. Tali dati consentono, in particolare, di rintracciare e di identificare la fonte e la destinazione di una comunicazione a partire dal telefono fisso o mobile di una persona, di stabilire la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare il telefono mobile senza che una comunicazione sia necessariamente trasmessa. Inoltre, i dati suddetti offrono la possibilità di accertare la frequenza delle comunicazioni dell'utente con determinate persone in un dato periodo. Peraltro, come confermato dal governo estone all'udienza, l'accesso ai dati suddetti può, quando si tratti di lotta contro la criminalità, essere richiesto per qualsiasi tipo di reato.

29 Per quanto riguarda le condizioni alle 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 dell'articolo 15, paragrafo 1, della direttiva 2002/58, la Corte

ha statuito che tale accesso può essere concesso soltanto se e in quanto tali dati siano stati conservati da detti fornitori in un modo conforme al citato articolo 15, paragrafo 1 (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 167).

30 A questo proposito, la Corte ha altresì statuito che il citato articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, osta a misure legislative che prevedano, per finalità siffatte, a titolo preventivo, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 168).

31 Quanto agli obiettivi idonei a giustificare un accesso delle autorità pubbliche ai dati conservati dai fornitori di servizi di comunicazione elettronica in applicazione di una misura conforme alle disposizioni sopra menzionate, risulta, da un lato, dalla giurisprudenza della Corte che un siffatto accesso può essere giustificato soltanto dall'obiettivo di interesse generale per il quale tale conservazione è stata imposta ai suddetti fornitori di servizi (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 166).

32 Dall'altro lato, la Corte ha statuito che la possibilità per gli Stati membri di giustificare una limitazione ai diritti e agli obblighi previsti, segnatamente, dagli articoli 5, 6 e 9 della direttiva 2002/58 deve essere valutata misurando la gravità dell'ingerenza che una limitazione siffatta comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito mediante questa limitazione sia correlata alla gravità dell'ingerenza suddetta (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 131 e la giurisprudenza ivi citata).

33 Per quanto riguarda l'obiettivo, cui mira la normativa in discussione nel procedimento principale, della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati, conformemente al principio di proporzionalità, soltanto la lotta contro le forme gravi di criminalità e la prevenzione di gravi minacce alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, come quelle che comporta la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione, sia questa generalizzata e indifferenziata oppure mirata. Pertanto, soltanto ingerenze nei suddetti diritti fondamentali che non presentino un carattere grave possono essere giustificate dall'obiettivo, cui mira la normativa in discussione nel procedimento principale, della prevenzione, della ricerca, dell'accertamento e del perseguimento di reati in generale (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 140 nonché 146).

34 A questo proposito, è stato statuito, in particolare, che le misure legislative riguardanti il trattamento dei dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica come tali, e segnatamente la conservazione di tali dati e l'accesso agli stessi, al solo scopo di identificare l'utente interessato, e senza che tali dati possano essere associati ad informazioni relative alle comunicazioni effettuate, possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale, al quale fa riferimento l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58. Infatti, tali dati non consentono, di per sé soli, di conoscere la data, l'ora, la durata e i destinatari delle comunicazioni effettuate, né i luoghi in cui tali comunicazioni sono avvenute o la frequenza delle stesse con determinate persone nel corso di un dato periodo, cosicché essi non forniscono, a parte le coordinate degli utenti dei mezzi di comunicazione elettronica, quali i loro indirizzi, alcuna informazione sulle comunicazioni effettuate e, di conseguenza, sulla loro vita privata. Pertanto, l'ingerenza causata da una misura riguardante questi dati non può, in linea di principio, essere qualificata come grave (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 157 e 158 nonché la giurisprudenza ivi citata).

35 Date tali circostanze, soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono atti a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo e tali da permettere di trarre

precise conclusioni sulla vita privata delle persone interessate (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 54), 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 tali dati, possano avere come effetto che l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale sia idoneo a giustificare tale accesso.

36 Occorre rilevare che l'accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, come quelli conservati sul fondamento dell'articolo 111[1] della legge relativa alle comunicazioni elettroniche, può effettivamente consentire di trarre conclusioni precise, o addirittura molto precise, sulla 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 (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 117).

37 Certamente, come suggerisce il giudice del rinvio, maggiore è la durata del periodo per il quale viene richiesto l'accesso, più grande è, in linea di principio, la quantità di dati che possono essere conservati dai fornitori di servizi di comunicazioni elettroniche, relativi alle comunicazioni elettroniche effettuate, ai luoghi di soggiorno frequentati, nonché agli spostamenti compiuti dall'utente di un mezzo di comunicazione elettronica, consentendo in tal modo di ricavare, a partire dai dati consultati, un maggior numero di conclusioni sulla vita privata di tale utente. Una constatazione analoga può essere effettuata anche per quanto riguarda le categorie di dati richiesti.

38 Mira dunque a soddisfare il requisito di proporzionalità, in virtù del quale le deroghe alla protezione dei dati personali e le limitazioni di quest'ultima devono compiersi entro i limiti dello stretto necessario (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 130 nonché la giurisprudenza ivi citata), il fatto che le autorità nazionali competenti siano tenute a garantire, in ciascun caso di specie, che tanto la categoria o le categorie di dati interessati, quanto la durata per la quale è richiesto l'accesso a questi ultimi, siano, in funzione delle circostanze del caso di specie, limitate a quanto è strettamente necessario ai fini dell'indagine in questione.

39 Tuttavia, l'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, derivante dall'accesso, da parte di un'autorità pubblica, a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da esso utilizzate, presenta in ogni caso un carattere grave indipendentemente dalla durata del periodo per il quale è richiesto l'accesso a tali dati e dalla quantità o dalla natura dei dati disponibili per un periodo siffatto, qualora, come nella fattispecie di cui al procedimento principale, questo insieme di dati sia tale da permettere di trarre precise conclusioni sulla vita privata della persona o delle persone interessate.

40 A tale riguardo, anche l'accesso a un quantitativo limitato di dati relativi al traffico o di dati relativi all'ubicazione, oppure l'accesso a dati per un breve periodo, possono essere idonei a fornire precise informazioni sulla vita privata di un utente di un mezzo di comunicazione elettronica. Inoltre, la quantità dei dati disponibili e le informazioni concrete sulla vita privata della persona interessata che ne derivano sono circostanze che possono essere valutate solo dopo la consultazione dei dati suddetti. Orbene, l'autorizzazione all'accesso concessa dal giudice o dall'autorità indipendente competente interviene necessariamente prima che i dati e le informazioni che ne derivano possano essere consultati. Pertanto, la valutazione della gravità dell'ingerenza costituita dall'accesso si effettua necessariamente in funzione del rischio generalmente afferente alla categoria di dati richiesti per la vita privata delle persone interessate, senza che rilevi, peraltro, sapere se le informazioni relative alla vita privata che ne derivano abbiano o meno, concretamente, un carattere sensibile.

41 Infine, tenuto conto del fatto che il giudice del rinvio è investito di una domanda con cui viene dedotta l'inammissibilità dei processi verbali redatti in base ai dati relativi al traffico e ai dati relativi all'ubicazione, in quanto le disposizioni dell'articolo 111[1] della legge relativa alle comunicazioni

elettroniche sarebbero contrarie all'articolo 15, paragrafo 1, della direttiva 2002/58 sotto il profilo sia della conservazione dei dati sia dell'accesso a questi ultimi, occorre ricordare che, allo stato attuale del diritto dell'Unione, spetta, in linea di principio, al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati in questione, contraria al diritto dell'Unione (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 222), od anche mediante un accesso delle autorità nazionali ai dati suddetti, contrario a tale diritto dell'Unione.

42 Infatti, secondo una consolidata giurisprudenza, in assenza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro, in virtù del principio dell'autonomia procedurale, stabilire le regole di procedura applicabili ai ricorsi giurisdizionali destinati a garantire la tutela dei diritti riconosciuti ai singoli dal diritto dell'Unione, a condizione però che le regole suddette non siano meno favorevoli di quelle disciplinanti situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano impossibile in pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività) (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 223 nonché la giurisprudenza ivi citata).

43 Per quanto riguarda più in particolare il principio di effettività, occorre ricordare che le norme nazionali relative all'ammissibilità e all'utilizzazione delle informazioni e degli elementi di prova hanno come obiettivo, in virtù delle scelte operate dal diritto nazionale, di evitare che informazioni ed elementi di prova ottenuti in modo illegittimo arrechino indebitamente pregiudizio a una persona sospettata di avere commesso dei reati. Orbene, tale obiettivo può, a seconda del diritto nazionale, essere raggiunto non solo mediante un divieto di utilizzare informazioni ed elementi di prova siffatti, ma anche mediante norme e prassi nazionali che disciplinino la valutazione e la ponderazione delle informazioni e degli elementi di prova, o addirittura tenendo conto del loro carattere illegittimo in sede di determinazione della pena (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 225).

44 La necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di informazioni ed elementi di prova siffatti comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto ad un processo equo. Orbene, un organo giurisdizionale, il quale consideri che una parte non è in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo ad influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione siffatta. Pertanto, il principio di effettività impone al giudice penale nazionale di escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, od anche mediante un accesso dell'autorità competente a tali dati in violazione del diritto dell'Unione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti di criminalità, qualora tali persone non siano in grado di svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili ad una materia estranea alla conoscenza dei giudici e idonei ad influire in maniera preponderante sulla valutazione dei fatti (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 226 e 227).

45 Alla luce delle considerazioni che precedono, occorre rispondere alla prima e alla seconda questione dichiarando che 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, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di 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, 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, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

Sulla terza questione

46 Con la sua terza questione pregiudiziale, il giudice del rinvio chiede, in sostanza, se 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, debba essere interpretato nel senso che esso osta a una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

47 Il giudice del rinvio precisa al riguardo che, se è pur vero che il pubblico ministero estone è tenuto, conformemente al diritto nazionale, ad agire in modo indipendente, è soggetto soltanto alla legge e deve esaminare gli elementi a carico e quelli a discarico nel corso del procedimento istruttorio, l'obiettivo di tale procedimento resta nondimeno quello di raccogliere elementi di prova nonché di pervenire al soddisfacimento degli altri presupposti necessari per lo svolgimento di un processo. Sarebbe questa stessa autorità a rappresentare la pubblica accusa nel processo, ed essa dunque sarebbe altresì parte nel procedimento. Inoltre, risulta dal fascicolo a disposizione della Corte, come confermato anche dal governo estone e dal Prokuratuur all'udienza, che il pubblico ministero estone è organizzato in modo gerarchico e che le domande di accesso ai dati relativi al traffico e ai dati relativi all'ubicazione non sono soggette ad un requisito di forma particolare e possono essere presentate dal procuratore stesso. Infine, le persone ai cui dati può essere accordato l'accesso non sarebbero soltanto quelle sospettate di essere coinvolte in un reato.

48 È vero, come già dichiarato dalla Corte, che spetta al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazioni elettroniche devono accordare 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 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 (v., in tal senso, sentenze del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 117 e 118; del 6 ottobre 2020, Privacy International, C-623/17, EU:C:2020:790, punto 68, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 132 e la giurisprudenza ivi citata).

49 In particolare, una normativa nazionale che disciplini l'accesso delle autorità competenti a dati relativi al traffico e a dati relativi all'ubicazione conservati, adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, non può limitarsi a esigere che l'accesso delle autorità ai dati risponda alla finalità perseguita da tale normativa, ma deve altresì prevedere le condizioni sostanziali e procedurali che disciplinano tale utilizzo (sentenze del 6 ottobre 2020, Privacy International, C-623/17, EU:C:2020:790, punto 77, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, e C-512/18, e a., punto 176 e la giurisprudenza ivi citata).

50 Pertanto, e poiché un accesso generale a tutti i dati conservati, indipendentemente da un qualche collegamento, almeno indiretto, con la finalità perseguita, non può considerarsi 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 in questione. A questo proposito, un accesso siffatto 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 un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere. Tuttavia, in situazioni particolari, come quelle in cui 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 qualora sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo (v., in tal senso, sentenze del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 119, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 188).

51 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 presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate. In caso di urgenza debitamente giustificata, il controllo deve intervenire entro termini brevi (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 189 e la giurisprudenza ivi citata).

52 Tale controllo preventivo richiede, tra l'altro, come rilevato, in sostanza, dall'avvocato generale al paragrafo 105 delle sue conclusioni, che il giudice o l'entità incaricata di effettuare il controllo medesimo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per garantire una conciliazione dei diversi interessi e diritti in gioco. Per quanto riguarda, più in particolare, un'indagine penale, tale controllo preventivo richiede che detto giudice o detta 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.

53 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 [v., in tal senso, sentenza del 9 marzo 2010, Commissione/Germania, C-518/07, EU:C:2010:125, punto 25, nonché parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 229 e 230].

54 Dalle considerazioni che precedono risulta che il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare, ricordato al punto 51 della presente sentenza, 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, come rilevato in sostanza dall'avvocato generale al paragrafo 126 delle sue conclusioni, 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.

55 Ciò non si verifica nel caso di un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale. Infatti, il pubblico ministero non ha il compito di dirimere in piena indipendenza una controversia, bensì quello di sottoporla, se del caso, al giudice competente, in quanto parte nel processo che esercita l'azione penale.

56 La circostanza che il pubblico ministero sia tenuto, conformemente alle norme che disciplinano le sue competenze e il suo status, a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento non può essere sufficiente per conferirgli lo status di terzo rispetto agli interessi in gioco nel senso descritto al punto 52 della presente sentenza.

57 Ne consegue che il pubblico ministero non è in grado di effettuare il controllo preventivo di cui al punto 51 della presente sentenza.

58 Poiché il giudice del rinvio ha sollevato, peraltro, la questione se si possa supplire all'assenza di un controllo effettuato da un'autorità indipendente mediante un controllo successivo, da parte di un giudice, della legittimità dell'accesso di un'autorità nazionale ai dati relativi al traffico e ai dati relativi all'ubicazione, occorre rilevare che il controllo indipendente deve intervenire, come richiesto dalla giurisprudenza richiamata al punto 51 della presente sentenza, previamente a qualsiasi accesso, salvo situazioni di urgenza debitamente giustificate, nel qual caso il controllo deve avvenire entro termini brevi. Come rilevato dall'avvocato generale al paragrafo 128 delle sue conclusioni, un siffatto controllo successivo non consentirebbe di rispondere all'obiettivo di un controllo preventivo, consistente nell'impedire che venga autorizzato un accesso ai dati in questione eccedente i limiti dello stretto necessario.

59 In tali circostanze, occorre rispondere alla terza questione pregiudiziale dichiarando che 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, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

Sulle spese

60 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) **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), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, 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 consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di 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, 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, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.**

2) **L'articolo 15, paragrafo 1, della direttiva 2002/58, 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, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.**

Firme

* Lingua processuale: l’estone.