SENTENZA DELLA CORTE (Prima Sezione)

7 settembre 2023 (*)

«Rinvio pregiudiziale – Telecomunicazioni – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 15, paragrafo 1 – Dati conservati dai fornitori di servizi di comunicazione elettronica e messi a disposizione delle autorità competenti in procedimenti penali – Uso successivo di tali dati nel corso di un'indagine su una condotta illecita»

Nella causa C-162/22,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema di Lituania), con decisione del 24 febbraio 2022, pervenuta in cancelleria il 3 marzo 2022, nel procedimento avviato da

A.G.

con l'intervento di:

Lietuvos Respublikos generalinė prokuratūra,

LA CORTE (Prima Sezione),

composta da A. Arabadjiev, presidente di sezione, P.G. Xuereb (relatore), T. von Danwitz, A. Kumin e I. Ziemele, giudici,

avvocato generale: M. Campos Sánchez-Bordona

cancelliere: A. Lamote, amministratrice

vista la fase scritta del procedimento e in seguito all'udienza del 2 febbraio 2023,

considerate le osservazioni presentate:

– per A.G., da G. Danėlius, advokatas;

– per il governo lituano, da S. Grigonis, V. Kazlauskaitė-Švenčionienė e V. Vasiliauskienė, in qualità di agenti;

– per il governo ceco, da O. Serdula, M. Smolek e J. Vláčil, in qualità di agenti;

– per il governo estone, da M. Kriisa, in qualità di agente;

– per l'Irlanda, da M. Browne, A. Joyce e M. Tierney, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo francese, da R. Bénard, in qualità di agente;

– per il governo italiano, da G. Palmieri, in qualità di agente, assistita da A. Grumetto, avvocato dello Stato;

– per il governo ungherese, da Zs. Biró-Tóth e M.Z. Fehér, in qualità di agenti;

– per la Commissione europea, da S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal e F. Wilman, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 30 marzo 2023,

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»).

2 Tale domanda è stata presentata nell'ambito di un procedimento promosso da A.G. in merito alla legittimità di decisioni con cui la Lietuvos Respublikos generalinė prokuratūra (Procura generale della Repubblica di Lituania; in prosieguo: la «Procura generale») ha disposto la revoca delle sue funzioni di procuratore.

Contesto normativo

Diritto dell'Unione

3 L'articolo 1 della direttiva 2002/58, intitolato «Finalità e campo d'applicazione», così dispone:

«1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con

riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

(...)

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti 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) o alle attività dello Stato in settori che rientrano nel diritto penale».

4 L'articolo 5 di tale direttiva, intitolato «Riservatezza delle comunicazioni», al paragrafo 1 prevede quanto segue:

«Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la 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».

5 L'articolo 15 di detta direttiva, intitolato «Applicazione di alcune disposizioni della direttiva 95/46/CE», al paragrafo 1 così recita:

«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/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)], 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 comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE]».

Diritto lituano

Legge sulle comunicazioni elettroniche

6 L'articolo 65, paragrafo 2, del Lietuvos Respublikos elektroninių ryšių įstatymas (legge della Repubblica di Lituania sulle comunicazioni elettroniche), del 15 aprile 2004 (Žin., 2004, n. 69-2382), nella sua versione applicabile ai fatti di cui al procedimento principale (in prosieguo: la «legge sulle comunicazioni elettroniche»), obbliga i fornitori di servizi di comunicazione elettronica a conservare i dati di cui all'allegato 1 alla stessa legge e, se del caso, di metterli a disposizione delle autorità competenti affinché queste ultime possano utilizzarli nella lotta alla criminalità grave.

7 A sensi dell'allegato 1 alla legge sulle comunicazioni elettroniche, le categorie di dati che devono essere conservati sono le seguenti:

«1. I dati necessari per trovare e identificare l'origine di una comunicazione: (...) 2. I dati necessari per determinare la destinazione di una comunicazione: (...) 3. I dati necessari per determinare la data, l'ora e la durata di una comunicazione: (...) 4. I dati necessari per determinare il tipo di comunicazione: (...) 5. I dati necessari per determinare gli strumenti di comunicazione degli utenti o quelli che si presume essere i loro strumenti: (...) 6. I dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: (...)».

8 A norma dell'articolo 77, paragrafo 4, di tale legge, qualora esista una decisione giudiziaria motivata o un'altra base giuridica prevista dalla legge, i fornitori di servizi di comunicazione elettronica devono rendere tecnicamente possibile, in particolare agli organi di indagine penale e alle autorità istruttorie, secondo le modalità previste dal Lietuvos Respublikos baudžiamojo proceso kodeksas (codice di procedura penale della Repubblica di Lituania; in prosieguo: il «codice di procedura penale»), il controllo del contenuto delle informazioni trasmesse sulle reti di comunicazione elettronica.

Legge sull'intelligence criminale

9 L'articolo 6, paragrafo 3, punto 1, del Lietuvos Respublikos kriminalinės žvalgybos įstatymas (legge della Repubblica di Lituania sull'intelligence criminale), del 2 ottobre 2012 (Žin., 2012, n. 122-6093), nella versione applicabile ai fatti di cui al procedimento principale (in prosieguo: la «legge sull'intelligence criminale»), dispone che, qualora siano soddisfatte le condizioni previste da tale legge per giustificare un'operazione di indagine penale e previa autorizzazione del pubblico ministero o di un organo giurisdizionale, gli organi di indagine penale hanno il potere, in aggiunta a quelli elencati ai paragrafi 1 e 2 del medesimo articolo, di ottenere informazioni dai fornitori di servizi di comunicazione elettronica.

10 L’articolo 8, paragrafo 1, di tale legge prevede che gli organi di indagine penale conducano un’indagine quando, in particolare, sono disponibili informazioni sulla preparazione o sulla commissione di un reato molto grave, grave o relativamente grave o su persone che stanno preparando, commettendo o hanno commesso un siffatto reato. L’articolo 8, paragrafo 3, di detta legge precisa che, se detta indagine rileva la presenza di indizi di reato, viene avviata immediatamente un’istruttoria penale.

11 In base all’articolo 19, paragrafo 1, punto 5, della legge sull’intelligence criminale, le informazioni provenienti da operazioni di indagine penale possono essere utilizzate nei casi indicati ai paragrafi 3 e 4 del medesimo articolo, e negli altri casi previsti dalla legge. Ai sensi del paragrafo 3, del suddetto articolo, le informazioni provenienti da operazioni di indagine penale relative a un fatto che presenta caratteristiche di reato di natura corruttiva possono essere declassificate, d’accordo con il pubblico ministero, e utilizzate nell’ambito di un’indagine su illeciti disciplinari o condotte illecite.

Codice di procedura penale

12 L’articolo 154 del codice di procedura penale prevede che, su provvedimento di un giudice istruttore adottato su richiesta del pubblico ministero, un inquirente possa ascoltare le conversazioni inoltrate attraverso le reti di comunicazione elettronica, farle trascrivere, controllare altre informazioni trasmesse attraverso le reti di comunicazione elettronica e registrarle e conservarle, se vi è, in particolare, motivo di ritenere che si possano così ottenere informazioni su un reato molto grave o grave in fase di preparazione o di commissione o in relazione a un reato relativamente grave o non grave.

13 L’articolo 177, paragrafo 1, di tale codice dispone che i dati risultanti dalle indagini sono riservati e che, fino alla fase giudiziale della causa, possono essere divulgati solo con l’autorizzazione del pubblico ministero e solo nella misura in cui ciò sia giustificato.

14 Ai fini dell’attuazione dell’articolo 177 di detto codice, si applicano le Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (raccomandazioni relative alla trasmissione e all’utilizzo dei dati risultanti dalle indagini a fini diversi dall’azione penale nonché alla protezione di tali dati), approvate dal decreto n. I-279 del Procuratore generale del 17 agosto 2017 (TAR, 2017, n. 2017-13413), come modificate da ultimo dal decreto n. I-211 del 25 giugno 2018.

15 Il punto 23 di queste raccomandazioni prevede che, quando riceve una richiesta di accesso ai dati risultanti dalle indagini, il pubblico ministero decida se è opportuno fornire tali dati. Se decide di fornirli, il pubblico ministero deve specificare la misura in cui i dati oggetto della richiesta possono essere forniti.

Procedimento principale e questione pregiudiziale

16 La Procura generale ha avviato un'indagine amministrativa nei confronti del ricorrente nel procedimento principale, che all'epoca esercitava le funzioni di procuratore presso una procura lituana, con la motivazione che esistevano indizi secondo i quali quest'ultimo, nell'ambito di un'indagine da lui diretta, avrebbe illegittimamente fornito informazioni rilevanti ai fini di tale indagine all'indagato e al suo avvocato.

17 Nella sua relazione su tale indagine, la commissione della Procura generale ha constatato che il ricorrente nel procedimento principale aveva effettivamente tenuto una condotta illecita.

18 Secondo detta relazione, tale condotta illecita era dimostrata dagli elementi raccolti durante l'indagine amministrativa. In particolare, le informazioni ottenute durante le operazioni di indagine penale e i dati raccolti nel corso di due istruttorie penali avrebbero confermato l'esistenza di comunicazioni telefoniche tra il ricorrente nel procedimento principale e l'avvocato dell'indagato nell'ambito dell'indagine nei confronti di quest'ultimo che era diretta dal ricorrente nel procedimento principale. Detta relazione ha inoltre rilevato che un'ordinanza giudiziaria aveva autorizzato l'intercettazione e la registrazione del contenuto delle informazioni trasmesse tramite reti di comunicazione elettronica riguardanti l'avvocato in questione e che un'altra ordinanza giudiziaria aveva autorizzato la stessa misura riguardante il ricorrente nel procedimento principale.

19 Sulla base della medesima relazione, la Procura generale ha adottato due decreti con i quali, da un lato, ha inflitto al ricorrente nel procedimento principale una sanzione consistente nella revoca delle sue funzioni e, dall'altro, ha rimosso quest'ultimo dal suo incarico.

20 Il ricorrente nel procedimento principale ha adito il Vilniaus apygardos administracinis teismas (Tribunale amministrativo regionale di Vilnius, Lituania) con un ricorso diretto, in particolare, all'annullamento dei suddetti due decreti.

21 Con sentenza del 16 luglio 2021, tale giudice ha respinto il ricorso del ricorrente nel procedimento principale con la motivazione, in particolare, che le operazioni di indagine penale effettuate nel caso di specie erano legittime e che le informazioni raccolte conformemente alle disposizioni della legge sull'intelligence criminale erano state utilizzate legalmente per valutare l'esistenza di un'eventuale condotta illecita del ricorrente nel procedimento principale.

22 Il ricorrente nel procedimento principale ha adito in appello il Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema di Lituania), giudice del rinvio, sostenendo che l'accesso da parte degli organi di indagine, nell'ambito di un'operazione di indagine penale, ai dati relativi al traffico e al contenuto stesso delle comunicazioni elettroniche costituiva una violazione dei

diritti fondamentali di gravità tale per cui, tenuto conto delle disposizioni della direttiva 2002/58 e della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), detto accesso poteva essere concesso solo ai fini della lotta contro reati gravi. Orbene, l'articolo 19, paragrafo 3, della legge sull'intelligence criminale prevedrebbe che tali dati possano essere utilizzati per indagare non solo su reati gravi, ma anche su illeciti disciplinari o condotte illecite di natura corruttiva.

23 Secondo il giudice del rinvio, le questioni sollevate dal ricorrente nel procedimento principale vertono su due elementi, vale a dire, da un lato, l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica a fini diversi dalla lotta contro i reati gravi e dalla prevenzione delle minacce gravi alla sicurezza pubblica e, dall'altro, una volta ottenuto tale accesso, l'utilizzo di tali dati per indagare su condotte illecite di natura corruttiva.

24 Tale giudice ricorda che, dalla giurisprudenza della Corte, segnatamente dalla sentenza del 6 ottobre 2020, Privacy International (C-623/17, EU:C:2020:790, punto 39) risulta, da un lato, che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto in combinato disposto con l'articolo 3 di quest'ultima, deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale direttiva non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa che imponga loro di accordare alle autorità nazionali competenti l'accesso a tali dati. Dall'altro lato, da tale giurisprudenza, segnatamente dalla sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152, punti 33 e 35) deriverebbe che, per quanto riguarda l'obiettivo 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.

25 Tuttavia, la Corte non si sarebbe ancora pronunciata sull'incidenza dell'uso successivo dei dati in questione sull'ingerenza nei diritti fondamentali. In tali circostanze, il giudice del rinvio si chiede se un siffatto uso successivo debba parimenti essere considerato come un'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta di gravità tale da poter essere giustificata solo dalla lotta alla criminalità grave e dalla prevenzione delle minacce gravi alla sicurezza pubblica, il che escluderebbe la possibilità di utilizzare detti dati in indagini per condotta illecita di natura corruttiva.

26 In tali circostanze, il Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema di Lituania) ha deciso di sospendere il procedimento e di sottoporre alla Corte la seguente questione pregiudiziale:

«Se l’articolo 15, paragrafo 1, della direttiva [2002/58], in combinato disposto con gli articoli 7, 8, 11 e 52, paragrafo 1, della [Carta], debba essere interpretato nel senso che esso vieti alle autorità pubbliche competenti di utilizzare, nell’ambito di indagini per condotta illecita di natura corruttiva nell’esercizio di funzioni pubbliche, i dati conservati dai fornitori di servizi di comunicazione elettronica che possono fornire informazioni sui dati di un utente di un mezzo di comunicazione elettronica e sulle comunicazioni da questi effettuate, indipendentemente dal fatto che l’accesso a tali dati sia stato concesso, nel caso concreto, ai fini del contrasto di reati gravi e di prevenzione di gravi minacce alla sicurezza pubblica».

Sulla questione pregiudiziale

27 Con la sua questione, 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 che dati personali relativi a comunicazioni elettroniche che sono stati conservati, in applicazione di una misura legislativa adottata ai sensi di tale disposizione, dai fornitori di servizi di comunicazione elettronica e che sono stati successivamente messi a disposizione, in applicazione della medesima misura, delle autorità competenti a fini di lotta alla criminalità grave possano essere utilizzati nell’ambito di indagini per condotte illecite di natura corruttiva.

28 In via preliminare, occorre rilevare che dalla decisione di rinvio risulta che, sebbene il fascicolo amministrativo relativo al procedimento conclusosi con i decreti di cui al procedimento principale richiamati al punto 19 della presente sentenza comprendesse anche informazioni raccolte dalle autorità competenti grazie all’intercettazione e alla registrazione di comunicazioni elettroniche che erano state autorizzate, ai fini dell’azione penale, da due ordinanze giudiziarie, ciò non toglie che il giudice del rinvio si interroghi non tanto sull’uso di dati personali ottenuti senza l’intervento dei fornitori di servizi di comunicazione elettronica, quanto sull’uso successivo di dati personali che sono stati conservati da tali fornitori sulla base di una misura legislativa dello Stato membro che impone loro un siffatto obbligo di conservazione, ai sensi dell’articolo 15, paragrafo 1, della direttiva 2002/58.

29 A tale riguardo, dalle indicazioni contenute nella domanda di pronuncia pregiudiziale risulta che i dati oggetto della questione sollevata sono quelli conservati in forza dell’articolo 65, paragrafo 2, della legge sulle comunicazioni elettroniche, in combinato disposto con l’allegato 1 a tale legge, che impone ai fornitori di servizi di comunicazione elettronica un obbligo di conservare, in modo generalizzato e indifferenziato, i dati relativi al traffico e i dati relativi all’ubicazione relativi a siffatte comunicazioni ai fini della lotta alla criminalità grave.

30 Per quanto concerne le condizioni alle quali tali dati possono essere utilizzati in occasione di un procedimento amministrativo relativo a condotte illecite di natura corruttiva, occorre innanzitutto ricordare che l'accesso ai dati suddetti può essere concesso, in applicazione di una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, soltanto se e in quanto tali dati siano stati conservati da detti fornitori in un modo conforme a detta disposizione [v., in tal senso, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 29 e giurisprudenza ivi citata]. Inoltre, l'uso successivo di dati relativi al traffico e dei dati relativi all'ubicazione riguardanti siffatte comunicazioni ai fini della lotta alla criminalità grave è possibile soltanto a condizione, da un lato, che la conservazione di detti dati da parte dei fornitori di servizi di comunicazione elettronica sia avvenuta in modo conforme all'articolo 15, paragrafo 1, della direttiva 2002/58, come interpretata dalla giurisprudenza della Corte, e, dall'altro, che l'accesso a tali dati sia anch'esso stato concesso alle autorità competenti in modo conforme alla suddetta disposizione.

31 A questo proposito, la Corte ha già statuito 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 osta a misure legislative che prevedono, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla pubblica sicurezza, la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione (sentenza del 20 settembre 2022, SpaceNet e Telekom Deutschland, C-793/19 e C-794/19, EU:C:2022:702, punti 74 e 131 nonché giurisprudenza ivi citata). Per contro, essa ha precisato che l'articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, non osta a misure legislative che prevedano, ai fini della lotta ai reati gravi e della prevenzione delle minacce gravi alla pubblica sicurezza,

– una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;

– una conservazione generalizzata e indiscriminata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– una conservazione generalizzata e indiscriminata dei dati relativi all'identità anagrafica degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per

un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono,

quando tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi è subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongono di garanzie effettive contro il rischio di abusi (sentenza del 20 settembre 2022, SpaceNet e Telekom Deutschland, C-793/19 e C-794/19, EU:C:2022:702, punto 75 e giurisprudenza ivi citata).

32 Per quanto riguarda gli obiettivi idonei a giustificare l'utilizzo, da parte delle autorità pubbliche, dei dati conservati dai fornitori di servizi di comunicazione elettronica in applicazione di una misura conforme a tali disposizioni, occorre ricordare che l'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio, enunciato all'articolo 5, paragrafo 1, di tale direttiva, di garantire la riservatezza dei dati personali nonché ai corrispondenti obblighi, menzionati in particolare agli articoli 6 e 9 di detta direttiva, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa e 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 che prevedano la conservazione dei dati per un periodo di tempo limitato, qualora ciò sia giustificato da uno dei suddetti motivi (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, punto 110).

33 Orbene, l'articolo 15, paragrafo 1, della direttiva 2002/58 non può giustificare il fatto che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati e, in particolare, al divieto di memorizzare tali dati, espressamente previsto all'articolo 5 di detta direttiva, divenga la regola, salvo privare quest'ultima norma di gran parte della sua portata (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 40).

34 Quanto agli obiettivi idonei a giustificare una limitazione dei diritti e degli obblighi previsti, in particolare, dagli articoli 5, 6 e 9 della direttiva 2002/58, la Corte ha già dichiarato che l'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, prima frase, di tale direttiva ha carattere tassativo, di modo che una misura legislativa adottata ai sensi di detta disposizione deve rispondere in modo effettivo e rigoroso ad uno di questi obiettivi (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 41).

35 Per quanto attiene agli obiettivi d'interesse generale che possono giustificare una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, si evince dalla giurisprudenza della Corte che, secondo il principio di proporzionalità,

esiste una gerarchia tra tali obiettivi in funzione della loro rispettiva importanza e che l'importanza dell'obiettivo perseguito da una simile misura deve essere rapportata alla gravità dell'ingerenza che ne risulta (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 56).

36 A questo proposito, l'importanza dell'obiettivo della salvaguardia della sicurezza nazionale, letto alla luce dell'articolo 4, paragrafo 2, TUE, secondo il quale la salvaguardia della sicurezza nazionale rimane di competenza esclusiva di ciascuno Stato membro, supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, in particolare degli obiettivi di lotta alla criminalità in generale, anche grave, e di salvaguardia della sicurezza pubblica. Fatto salvo il rispetto degli altri requisiti previsti all'articolo 52, paragrafo 1, della Carta, l'obiettivo di salvaguardia della sicurezza nazionale è quindi idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare tali altri obiettivi (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 57 e giurisprudenza ivi citata).

37 Per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, la Corte ha rilevato che, conformemente al principio di proporzionalità, solo la lotta alle forme gravi di criminalità e la prevenzione di minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, come quelle che comporta la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione. Pertanto, solo le ingerenze in tali diritti fondamentali che non presentano un carattere grave possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 59 e giurisprudenza ivi citata).

38 Da tale giurisprudenza risulta che, sebbene la lotta alla criminalità grave e la prevenzione delle minacce gravi alla sicurezza pubblica siano di importanza minore, nella gerarchia degli obiettivi di interesse generale, rispetto alla salvaguardia della sicurezza nazionale (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 99), la loro importanza supera talvolta quella della lotta contro la criminalità in generale e della prevenzione della minacce non gravi alla sicurezza pubblica.

39 In tale contesto, occorre tuttavia ricordare che, come risulta altresì dal punto 31 della presente sentenza, la possibilità per gli Stati membri di giustificare una limitazione dei diritti e degli obblighi previsti, segnatamente, agli articoli 5, 6 e 9 della direttiva 2002/58 deve essere valutata misurando la gravità dell'ingerenza che una restrizione siffatta comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito da tale limitazione sia adeguata a detta gravità (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).

40 Inoltre, la Corte ha già dichiarato che l'accesso a dati relativi al traffico e a dati relativi all'ubicazione conservati da fornitori in applicazione di una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, che deve avvenire nel pieno rispetto delle condizioni risultanti dalla giurisprudenza che ha interpretato tale direttiva, può in linea di principio essere giustificato solo dall'obiettivo di interesse generale per il quale tale conservazione è stata imposta a tali fornitori. La situazione è diversa solo se l'importanza dell'obiettivo perseguito dall'accesso supera quella dell'obiettivo che ha giustificato la conservazione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 98 e giurisprudenza ivi citata).

41 Orbene, tali considerazioni si applicano mutatis mutandis a un uso successivo dei dati relativi al traffico e a dati relativi all'ubicazione conservati da fornitori di servizi di comunicazione elettronica in applicazione di una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 ai fini della lotta alla criminalità grave. In effetti, tali dati non possono, dopo essere stati conservati e messi a disposizione delle autorità competenti ai fini della lotta alla criminalità grave, essere trasmessi ad altre autorità e utilizzati al fine di realizzare obiettivi, quali, come nel caso di specie, la lotta a una condotta illecita di natura corruttiva, che sono di importanza minore, nella gerarchia degli obiettivi di interesse generale, rispetto a quello della lotta alla criminalità grave e della prevenzione delle minacce gravi alla sicurezza pubblica. Infatti, autorizzare, in una situazione del genere, l'accesso ai dati conservati sarebbe contrario a tale gerarchia degli obiettivi di interesse generale richiamata ai punti 33, da 35 a 37 e 40 della presente sentenza (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 99).

42 Per quanto riguarda l'argomento sollevato dal governo ceco e dall'Irlanda nelle loro osservazioni scritte, secondo cui un procedimento disciplinare relativo a una condotta illecita di natura corruttiva potrebbe essere collegato alla salvaguardia della sicurezza pubblica, è sufficiente rilevare che, nella sua decisione di rinvio, il giudice del rinvio non ha menzionato una minaccia grave alla sicurezza pubblica.

43 Peraltro, se è vero che le indagini amministrative vertenti su illeciti disciplinari o condotte illecite di natura corruttiva possono svolgere un ruolo importante nella lotta contro tali atti, una misura legislativa che prevede siffatte indagini non risponde in modo effettivo e rigoroso all'obiettivo del perseguimento e della sanzione dei reati, di cui all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58, il quale riguarda solo azioni penali.

44 Alla luce di quanto precede occorre rispondere alla questione sollevata 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 a che dati personali relativi a comunicazioni elettroniche che sono stati conservati, in applicazione di una misura legislativa adottata ai sensi di tale disposizione, dai fornitori di servizi di comunicazione

elettronica e che sono stati successivamente messi a disposizione, in applicazione della medesima misura, delle autorità competenti a fini di lotta alla criminalità grave possano essere utilizzati nell'ambito di indagini per condotte illecite di natura corruttiva.

Sulle spese

45 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 (Prima Sezione) dichiara:

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 a che dati personali relativi a comunicazioni elettroniche che sono stati conservati, in applicazione di una misura legislativa adottata ai sensi di tale disposizione, dai fornitori di servizi di comunicazione elettronica e che sono stati successivamente messi a disposizione, in applicazione della medesima misura, delle autorità competenti a fini di lotta alla criminalità grave possano essere utilizzati nell'ambito di indagini per condotte illecite di natura corruttiva.

Firme