dirittifondamentali.it

La Corte di Giustizia si pronuncia in tema di vita privata e di perseguimento di reati gravi (CGUE, Grande Sezione, 30 aprile 2024, C-178/22)

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, dev'essere interpretato nel senso che: esso non osta a una disposizione nazionale che impone al giudice nazionale – allorché interviene in sede di controllo preventivo a seguito di una richiesta motivata di accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente di un mezzo di comunicazione elettronica, conservati dai fornitori di servizi di comunicazione elettronica, presentata da un'autorità nazionale competente nell'ambito di un'indagine penale – di autorizzare tale accesso qualora quest'ultimo sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni, purché sussistano sufficienti indizi di tali reati e detti dati siano rilevanti per l'accertamento dei fatti, a condizione, tuttavia, che tale giudice abbia la possibilità di negare detto accesso se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato.

***

SENTENZA DELLA CORTE (Grande Sezione)
30 aprile 2024 (*)

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Riservatezza delle comunicazioni – Fornitori di servizi di comunicazione elettronica – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea – Accesso a tali dati richiesto da un'autorità nazionale competente al fine di perseguire reati di furto aggravato – Definizione della nozione di "reato grave" il cui perseguimento può giustificare una grave ingerenza nei diritti fondamentali – Competenza degli Stati membri – Principio di proporzionalità – Portata del controllo preventivo del giudice sulle richieste di accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica»
Nella causa C-178/22,
avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Giudice delle indagini preliminari presso il Tribunale di Bolzano (Italia), con

ordinanza del 20 febbraio 2022, pervenuta in cancelleria l'8 marzo 2022, nei procedimenti penali a carico di

Ignoti,

con l'intervento di:

Procura della Repubblica presso il Tribunale di Bolzano,

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, L. Bay Larsen, vicepresidente, A. Arabadjiev, A. Prechal, K. Jürimäe, T. von Danwitz e Z. Csehi, presidenti di sezione, J.-C. Bonichot, S. Rodin, P.G. Xuereb (relatore), D. Gratsias, M.L. Arastey Sahún e M. Gavalec, giudici,

avvocato generale: A.M. Collins

cancelliere: C. Di Bella, amministratore

vista la fase scritta del procedimento e in seguito all'udienza del 21 marzo 2023,

considerate le osservazioni presentate:

– per la Procura della Repubblica presso il Tribunale di Bolzano, da F. Iovene, sostituto procuratore della Repubblica;

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

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

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

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

– per il governo francese, da A. Daniel, A.-L. Desjonquères, B. Fodda e J. Illouz, in qualità di agenti;

– per il governo cipriota, da E. Neophytou, in qualità di agente;

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

– per il governo dei Paesi Bassi, da M.K. Bulterman, A. Hanje e J. Langer, in qualità di agenti;

– per il governo austriaco, da A. Posch, J. Schmoll, C. Gabauer, K. Ibili e E. Samoilova, in qualità di agenti;

– per il governo polacco, da B. Majczyna, D. Lutostańska e J. Sawicka, in qualità di agenti;

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

sentite le conclusioni dell'avvocato generale, presentate all'udienza dell'8 giugno 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»), letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo l, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 Tale domanda è stata presentata nell'ambito di una richiesta della Procura della Repubblica presso il Tribunale di Bolzano (Italia) (in prosieguo: il «pubblico ministero») al Giudice delle

indagini preliminari presso il Tribunale di Bolzano (Italia), volta ad ottenere l'autorizzazione ad accedere a dati personali conservati da fornitori di servizi di comunicazione elettronica al fine di identificare gli autori di due furti aggravati di telefoni cellulari.

Contesto normativo

Diritto dell'Unione

Direttiva 2002/58

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 quest'ultima].

(...)

(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 comunitario. 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 di tale direttiva, intitolato «Definizioni», così 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 di detta direttiva, intitolato «Riservatezza delle comunicazioni», prevede quanto segue:

«1. 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.
(...)
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 stessa direttiva, intitolato «Dati sul traffico», così recita:

«1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica 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 della rete pubblica 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, intitolato «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 tale direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», 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], 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 italiano

Decreto legislativo n. 196/2003

9 L'articolo 132, comma 3, del decreto legislativo del 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (supplemento ordinario alla GURI n. 174 del 29 luglio 2003), nella versione applicabile al procedimento principale (in prosieguo: il «decreto legislativo n. 196/2003»), prevede quanto segue:

«Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private».

10 Il comma 3-*bis* di tale articolo così recita:

«Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato».

11 Infine, ai sensi del comma 3-*quater* di detto articolo: «[i] dati acquisiti in violazione delle disposizioni dei commi 3 e 3-bis non possono essere utilizzati».

Codice penale

12 L'articolo 624 del codice penale, intitolato «Furto», dispone quanto segue:

«Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 154 a euro 516.

(...)

Il delitto è punibile a querela della persona offesa, salvo che ricorra una o più delle circostanze di cui agli articoli 61, numero 7), e 625».

13 L'articolo 625, primo comma, del codice penale, rubricato «Circostanze aggravanti», prevede quanto segue:

«La pena per il fatto previsto dall'articolo 624 è della reclusione da due a sei anni e della multa da euro 927 a euro 1 500:

(...)

2) se il colpevole usa violenza sulle cose o si vale di un qualsiasi mezzo fraudolento;

3) se il colpevole porta indosso armi o narcotici, senza farne uso;

4) se il fatto è commesso con destrezza;

5) se il fatto è commesso da tre o più persone, ovvero anche da una sola, che sia travisata o simuli la qualità di pubblico ufficiale o d'incaricato di un pubblico servizio;

6) se il fatto è commesso sul bagaglio dei viaggiatori in ogni specie di veicoli, nelle stazioni, negli scali o banchine, negli alberghi o in altri esercizi ove si somministrano cibi o bevande

7) se il fatto è commesso su cose esistenti in uffici o stabilimenti pubblici, o sottoposte a sequestro o a pignoramento, o esposte per necessità o per consuetudine o per destinazione alla pubblica fede, o destinate a pubblico servizio o a pubblica utilità, difesa o reverenza;

7 *bis*) se il fatto è commesso su componenti metalliche o altro materiale sottratto ad infrastrutture destinate all'erogazione di energia, di servizi di trasporto, di telecomunicazioni o di altri servizi pubblici e gestite da soggetti pubblici o da privati in regime di concessione pubblica;

8) se il fatto è commesso su tre o più capi di bestiame raccolti in gregge o in mandria, ovvero su animali bovini o equini, anche non raccolti in mandria;

8 *bis*) se il fatto è commesso all'interno di mezzi di pubblico trasporto;

8 *ter*) se il fatto è commesso nei confronti di persona che si trovi nell'atto di fruire ovvero che abbia appena fruito dei servizi di istituti di credito, uffici postali o sportelli automatici adibiti al prelievo di denaro».

Codice di procedura penale

14 Ai sensi dell'articolo 4 del codice di procedura penale, intitolato «Regole per la determinazione della competenza»:

«Per determinare la competenza si ha riguardo alla pena stabilita dalla legge per ciascun reato consumato o tentato. Non si tiene conto della continuazione, della recidiva e delle circostanze del

reato, fatta eccezione delle circostanze aggravanti per le quali la legge stabilisce una pena di specie diversa da quella ordinaria del reato e di quelle ad effetto speciale».

15 L'articolo 269, comma 2, di detto codice prevede quanto segue:

«(...) le registrazioni sono conservate fino alla sentenza non più soggetta a impugnazione. Tuttavia gli interessati, quando la documentazione non è necessaria per il procedimento, possono chiederne la distruzione, a tutela della riservatezza, al giudice che ha autorizzato o convalidato l'intercettazione».

Procedimento principale e questione pregiudiziale

16 A seguito di due denunce sporte per reati di furto di telefono cellulare, commessi, rispettivamente, il 27 ottobre e il 20 novembre 2021, il pubblico ministero ha avviato, ai sensi degli articoli 624 e 625 del codice penale, due procedimenti penali a carico di ignoti per reati di furto aggravato.

17 Al fine di identificare gli autori di tali furti, il pubblico ministero, ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003, ha chiesto, rispettivamente il 7 e il 30 dicembre 2021, al Giudice delle indagini preliminari presso il Tribunale di Bolzano, giudice del rinvio, l'autorizzazione ad acquisire presso tutte le compagnie telefoniche i tabulati telefonici dei telefoni rubati. Tali richieste riguardavano: «tutti i dati [in possesso delle compagnie telefoniche], con metodo di tracciamento e localizzazione (in particolare utenze ed eventualmente codici IMEI [relativi all'identificatore internazionale apparecchiature mobili dei dispositivi] chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione ed indicazione delle celle e/o ripetitori interessati, utenze ed IMEI [dei dispositivi] mittenti/destinatari degli SMS o MMS e, ove possibile, generalità dei relativi intestatari) delle conversazioni/comunicazioni telefoniche e connessioni effettuate, anche in *roaming*, in entrata e in uscita anche se chiamate prive di fatturazione (squilli) dalla data del furto fino alla data di elaborazione della richiesta».

18 Il giudice del rinvio nutre dubbi circa la compatibilità dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 con l'articolo 15, paragrafo 1, della direttiva 2002/58, così come interpretato dalla Corte nella sua sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152).

19 Esso ricorda che, ai sensi del punto 45 di tale sentenza, disposizioni nazionali che consentono l'accesso di autorità pubbliche ai tabulati telefonici, comprendenti un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente interessato, sono giustificabili – tenuto conto del principio di proporzionalità previsto all'articolo 52, paragrafo 1, della Carta e della gravità dell'ingerenza nei diritti fondamentali alla vita privata, alla protezione dei dati a carattere personale e alla libertà di espressione e d'informazione, quali garantiti, rispettivamente, dagli articoli 7, 8 e 11 della Carta – solamente quando sono destinate a perseguire reati gravi, quali gravi minacce alla sicurezza pubblica, intesa quale quella dello Stato, e altre gravi forme di criminalità.

20 A tal proposito, il giudice del rinvio indica che, nella sentenza n. 33116 del 7 settembre 2021, la Corte suprema di Cassazione (Italia) ha dichiarato che, alla luce della discrezionalità interpretativa relativa all'individuazione dei reati che costituiscono gravi minacce alla sicurezza nazionale o altre forme di grave criminalità ai sensi della giurisprudenza della Corte, tale giurisprudenza non presentava le caratteristiche richieste per essere applicata direttamente dai giudici nazionali. Di conseguenza, il legislatore italiano avrebbe modificato l'articolo 132, comma 3, del decreto legislativo n. 196/2003, al fine di qualificare come reati gravi, per i quali sono acquisibili i tabulati

telefonici, i reati che la legge punisce con la pena della reclusione «non inferiore nel massimo a tre anni».

21 Secondo il giudice del rinvio, questa soglia dei tre anni, a partire dalla quale la massima pena reclusiva con la quale è punito un reato giustifica che quest'ultimo possa dar luogo alla comunicazione di tabulati telefonici alle autorità pubbliche, è tale che detti tabulati potrebbero essere comunicati a queste ultime per perseguire reati che destano solo scarso allarme sociale e che sono puniti solo a querela di parte, in particolare i furti di scarso valore come i furti di telefono cellulare o di bicicletta.

22 La disposizione nazionale in questione violerebbe quindi il principio di proporzionalità di cui all'articolo 52, paragrafo 1, della Carta, il quale impone un bilanciamento tra la gravità del reato perseguito e i diritti fondamentali che si sacrificano per il suo perseguimento. Tale principio osterebbe infatti a che una lesione dei diritti fondamentali garantiti dagli articoli 7, 8 e 11 della Carta sia giustificata al fine di perseguire un reato quale il furto.

23 Il giudice del rinvio precisa che i giudici italiani dispongono di un margine di discrezionalità molto limitato per negare l'autorizzazione all'acquisizione dei tabulati telefonici, poiché, ai sensi della disposizione in questione, l'autorizzazione deve essere rilasciata in presenza di «sufficienti indizi di reati» e se i dati richiesti sono «rilevant[i] ai fini dell'accertamento del reato». I giudici italiani non disporrebbero dunque di alcun margine valutativo in ordine alla concreta gravità del reato oggetto dell'indagine. Tale valutazione sarebbe stata effettuata una volta per tutte dal legislatore italiano quando ha stabilito che l'autorizzazione all'acquisizione dei dati dovesse essere rilasciata, in particolare, per tutti i reati punibili con la pena della reclusione non inferiore nel massimo a tre anni.

24 In tali circostanze, il Giudice delle indagini preliminari presso il Tribunale di Bolzano ha deciso di sospendere il procedimento e di sottoporre alla Corte la seguente questione pregiudiziale:

«Se l'articolo 15, comma 1 della direttiva [2002/58] osta alla normativa nazionale dell'articolo 132[, comma 3,] del decreto legislativo [n. 196/2003], (...) che (...) così stabilisce:

"3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private"».

Sulla ricevibilità della domanda di pronuncia pregiudiziale

25 Il governo italiano e l'Irlanda sostengono che la domanda di pronuncia pregiudiziale è parzialmente irricevibile. Essi rilevano che le richieste di accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica sono state presentate dal pubblico ministero, ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003, al fine di perseguire reati di furto aggravato di telefono cellulare. Orbene, con la sua questione pregiudiziale, il giudice del rinvio domanderebbe parimenti alla Corte se l'articolo 15, paragrafo 1, della direttiva 2002/58 osti a una disposizione nazionale che consente di ottenere l'accesso a dati conservati dai fornitori di servizi di comunicazione elettronica al fine di perseguire reati ricompresi nell'articolo 132, comma 3, del decreto legislativo n. 196/2003 diversi da quelli di cui trattasi nel procedimento principale, quali il

furto semplice o le molestie gravi a mezzo telefonico. Pertanto, nella misura in cui riguarda tali altri reati, la domanda di pronuncia pregiudiziale presenterebbe un carattere ipotetico.

26 A tal proposito, occorre ricordare che, secondo costante giurisprudenza, nell'ambito della cooperazione tra la Corte e i giudici nazionali istituita dall'articolo 267 TFUE spetta esclusivamente al giudice nazionale, cui è stata sottoposta la controversia e che deve assumere la responsabilità dell'emananda decisione giurisdizionale, valutare, alla luce delle particolari circostanze di ciascuna causa, sia la necessità di una pronuncia pregiudiziale per essere in grado di emettere la propria sentenza, sia la rilevanza delle questioni che sottopone alla Corte. Pertanto, allorché le questioni sollevate riguardano l'interpretazione del diritto dell'Unione, la Corte è, in via di principio, tenuta a statuire [sentenza del 21 marzo 2023, Mercedes-Benz Group (Responsabilità dei produttori di veicoli muniti di impianti di manipolazione), C-100/21, EU:C:2023:229, punto 52 e giurisprudenza citata].

27 Ne consegue che le questioni vertenti sul diritto dell'Unione godono di una presunzione di rilevanza. Il diniego della Corte di statuire su una questione pregiudiziale posta da un giudice nazionale è possibile solo qualora appaia manifestamente che l'interpretazione del diritto dell'Unione richiesta non ha alcuna relazione con la realtà effettiva o con l'oggetto del procedimento principale, qualora il problema sia di natura ipotetica oppure, ancora, qualora la Corte non disponga degli elementi di fatto o di diritto necessari per fornire una risposta utile alle questioni che le vengono sottoposte [sentenza del 21 marzo 2023, Mercedes-Benz Group (Responsabilità dei produttori di veicoli muniti di impianti di manipolazione), C-100/21, EU:C:2023:229, punto 53 e giurisprudenza citata].

28 Orbene, riproducendo integralmente l'articolo 132, comma 3, del decreto legislativo n. 196/2003, la questione pregiudiziale, anche se non distingue i tipi di reato ai quali tale disposizione si applica, ricomprende necessariamente i reati di furto aggravato per i quali sono state presentate le richieste di autorizzazione di accesso ai dati personali nel procedimento principale.

29 Pertanto, tale questione non presenta carattere ipotetico ed è quindi ricevibile.

Sulla questione pregiudiziale

30 Come rilevato dal governo francese nelle sue osservazioni scritte, la questione sollevata dal giudice del rinvio, così come formulata, invita la Corte a pronunciarsi sulla compatibilità dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 con l'articolo 15, paragrafo 1, della direttiva 2002/58.

31 A tal riguardo, occorre ricordare che, nell'ambito del procedimento istituito dall'articolo 267 TFUE, la Corte non può pronunciarsi sull'interpretazione di disposizioni di legge o di regolamenti nazionali né sulla conformità di tali disposizioni al diritto dell'Unione. Infatti, secondo costante giurisprudenza, nell'ambito di un rinvio pregiudiziale ai sensi dell'articolo 267 TFUE, la Corte può unicamente interpretare il diritto dell'Unione nei limiti delle competenze che sono attribuite all'Unione stessa [sentenza del 14 dicembre 2023, Getin Noble Bank (Termine di prescrizione delle azioni di restituzione), C-28/22, EU:C:2023:992, punto 53 e giurisprudenza ivi citata].

32 Orbene, secondo costante giurisprudenza, in caso di questioni formulate in modo improprio o che eccedano l'ambito delle funzioni attribuitele dall'articolo 267 TFUE, la Corte deve ricavare dal complesso degli elementi forniti dal giudice nazionale, in particolare dalla motivazione della decisione di rinvio, gli elementi di diritto dell'Unione che richiedono un'interpretazione tenuto conto dell'oggetto della controversia. In tale ottica, la Corte deve, se necessario, riformulare le questioni che le vengono sottoposte (sentenza del 14 dicembre 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, punto 20 e giurisprudenza ivi citata).

33 Inoltre, la Corte può dover prendere in considerazione norme del diritto dell'Unione alle quali il giudice nazionale non ha fatto riferimento nella formulazione della sua questione (sentenza del 17 novembre 2022, Harman International Industries, C-175/21, EU:C:2022:895, punto 31 e giurisprudenza ivi citata).

34 Alla luce di quanto precede, si deve ritenere che, con la sua questione, il giudice del rinvio chieda, 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 disposizione nazionale che impone al giudice nazionale – allorché interviene in sede di controllo preventivo a seguito di una richiesta motivata di accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata di un utente di un mezzo di comunicazione elettronica, conservati dai fornitori di servizi di comunicazione elettronica, presentata da un'autorità nazionale competente nell'ambito di un'indagine penale – di autorizzare tale accesso qualora quest'ultimo sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni, purché sussistano sufficienti indizi di tali reati e detti dati siano rilevanti per l'accertamento dei fatti.

35 In via preliminare, occorre ricordare che, 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 comunicazione elettronica può, a fini di prevenzione, ricerca, accertamento e perseguimento dei reati, essere concesso ad autorità pubbliche, in applicazione di una misura legislativa adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, la Corte ha statuito che un tale accesso può essere concesso soltanto se e in quanto tali dati siano stati conservati da detti fornitori conformemente a direttiva [v., in tal senso, sentenza odierna, La Quadrature du Net e a. (Dati personali e lotta alla contraffazione), C-470/21, punto 65 nonché giurisprudenza ivi citata]. Essa ha altresì statuito che tale 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 [sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 30, e giurisprudenza ivi citata].

36 Occorre altresì ricordare la giurisprudenza della Corte secondo la quale soltanto gli obiettivi di lotta contro le forme gravi di criminalità o di prevenzione di gravi minacce alla sicurezza pubblica sono atti a giustificare la grave ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta derivante dall'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, 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 rendere l'obiettivo di prevenzione, ricerca, accertamento e generale perseguimento di reati idoneo a giustificare tale accesso [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 35 e giurisprudenza ivi citata].

37 Con la sua questione pregiudiziale, il giudice del rinvio chiede, in sostanza, se una tale grave ingerenza possa essere autorizzata per reati quali quelli previsti dalla normativa nazionale di cui trattasi nel procedimento principale.

38 Per quanto riguarda, anzitutto, la questione se gli accessi, come quelli di cui trattasi, possano essere qualificati come grave ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta, occorre rilevare che, al fine di individuare gli autori dei presunti furti che sono all'origine di tale controversia, il pubblico ministero, per ciascuno dei telefoni cellulari di cui trattasi, ha chiesto al giudice del rinvio, ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003, l'autorizzazione ad acquisire tutti i dati in possesso delle compagnie telefoniche, ottenuti con metodo di tracciamento e localizzazione delle conversazioni e comunicazioni telefoniche e delle connessioni effettuate con tali telefoni. Tali richieste riguardavano, più in particolare, le utenze e i codici IMEI dei dispositivi chiamati o chiamanti, i siti visitati e raggiunti, l'orario e la durata delle chiamate e delle connessioni, l'indicazione delle celle o dei ripetitori interessati nonché le utenze e i codici IMEI dei dispositivi mittenti e destinatari degli SMS o MMS.

39 L'accesso a un simile insieme di dati relativi al traffico o di dati relativi all'ubicazione sembra tale da permettere di trarre precise conclusioni sulla vita privata delle persone i cui dati sono stati conservati, come le abitudini di 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 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 36 e giurisprudenza ivi citata]. L'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta causata dall'accesso a tali dati appare quindi qualificabile come grave.

40 Come risulta dal punto 39 della sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152), tale valutazione non può essere smentita dal solo fatto che le due richieste di accesso ai dati relativi al traffico o ai dati relativi all'ubicazione in questione riguardavano soltanto brevi periodi, di meno di due mesi, che andavano dalla data dei presunti furti dei telefoni cellulari alla data in cui tali richieste sono state redatte, dal momento che dette richieste riguardavano un insieme di tali dati idoneo a fornire informazioni precise sulla vita privata delle persone che utilizzavano i telefoni cellulari di cui trattasi.

41 Parimenti, è irrilevante, ai fini della valutazione dell'esistenza di una grave ingerenza nei diritti garantiti dagli articoli 7 e 8 della Carta, la circostanza che i dati cui il pubblico ministero ha chiesto di poter accedere non siano quelli dei proprietari dei telefoni cellulari in questione, bensì quelli delle persone che hanno comunicato tra loro utilizzando tali telefoni dopo i presunti furti. Infatti, emerge dall'articolo 5, paragrafo 1, della direttiva 2002/58 che l'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche effettuate mediante una rete pubblica di comunicazione e servizi di comunicazione elettronica accessibili al pubblico, nonché la riservatezza dei dati relativi al traffico a queste correlati, riguarda le comunicazioni effettuate dagli utenti di tale rete. Orbene, l'articolo 2, lettera a), di tale direttiva definisce la nozione di «utente» come qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

42 Di conseguenza, considerata la giurisprudenza citata al punto 36 della presente sentenza, poiché le ingerenze nei diritti fondamentali causate dall'accesso ai dati, quali quelle di cui trattasi nel procedimento principale, possono essere considerate gravi, esse possono essere giustificate solo dagli obiettivi di lotta contro le forme gravi di criminalità o di prevenzione di gravi minacce alla sicurezza pubblica.

43 Inoltre, sebbene spetti al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazione elettronica devono concedere alle autorità nazionali competenti l'accesso ai dati di cui essi dispongono, una tale normativa deve tuttavia prevedere regole chiare e precise che disciplinino la portata e le condizioni di applicazione di un tale accesso. Quest'ultimo può, in linea di principio, essere concesso, in relazione all'obiettivo di lotta contro la criminalità, soltanto per i dati di persone sospettate di essere implicate in un reato grave. Al fine di garantire concretamente il pieno rispetto di tali condizioni, le quali assicurino che l'ingerenza sia limitata allo stretto necessario, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato, salvo in caso di urgenza debitamente giustificata, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente [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, punti da 48 a 51].

44 Per quanto riguarda, infine, la definizione della nozione di «reato grave», dalla giurisprudenza risulta che, purché l'Unione non abbia legiferato in materia, la normativa penale e le norme di procedura penale rientrano nella competenza degli Stati membri. Questi ultimi devono tuttavia esercitare tale competenza nel rispetto del diritto dell'Unione (v., in tal senso, sentenza del 26 febbraio 2019, Rimšēvičs e BCE/Lettonia, C-202/18 e C-238/18, EU:C:2019:139, punto 57 nonché giurisprudenza ivi citata).

45 A tal proposito, occorre osservare che la definizione dei reati, delle circostanze attenuanti e aggravanti e delle sanzioni riflette tanto le realtà sociali quanto le tradizioni giuridiche, che variano non solo tra gli Stati membri, ma anche nel tempo. Orbene, tali realtà e tradizioni rivestono un'indubbia importanza nella determinazione dei reati considerati gravi.

46 Pertanto, tenuto conto della ripartizione delle competenze tra l'Unione e gli Stati membri ai sensi del Trattato FUE e delle notevoli differenze esistenti tra gli ordinamenti giuridici degli Stati membri in materia penale, si deve ritenere che spetti agli Stati membri definire i «reati gravi» ai fini dell'applicazione dell'articolo 15, paragrafo 1, della direttiva 2002/58.

47 Tuttavia, la definizione dei «reati gravi» fornita dagli Stati membri deve rispettare i dettami di tale articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta.

48 A tal riguardo, si deve ricordare che, nella misura in cui consente agli Stati membri di adottare misure legislative intese a «limitare» i diritti e gli obblighi previsti in particolare agli articoli 5, 6 e 9 della direttiva 2002/58, come quelli derivanti dai principi di riservatezza delle comunicazioni e dal divieto di memorizzazione dei dati ad esse relativi, l'articolo 15, paragrafo 1, di tale direttiva prevede un'eccezione alla regola generale dettata in particolare da tali articoli 5, 6 e 9 e deve, pertanto, secondo costante giurisprudenza, essere oggetto di un'interpretazione restrittiva. Tale disposizione non può quindi giustificare il fatto che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati divenga la regola, salvo privare l'articolo 5 di detta direttiva di gran parte della sua portata (v. in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 40).

49 Inoltre, risulta dall'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 che le misure adottate dagli Stati membri ai sensi di tale disposizione devono essere conformi ai principi generali dell'Unione, tra i quali figura il principio di proporzionalità, e assicurare il rispetto dei diritti fondamentali garantiti dagli articoli 7, 8 e 11 della Carta (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 42).

50 Ne consegue che gli Stati membri non possono snaturare la nozione di «reato grave» e, per estensione, quella di «grave criminalità», includendovi, ai fini dell'applicazione di tale articolo 15, paragrafo 1, reati che manifestamente non sono gravi, alla luce delle condizioni sociali esistenti nello Stato membro interessato, sebbene il legislatore di tale Stato membro abbia previsto di punirli con la pena della reclusione non inferiore nel massimo a tre anni.

51 Al fine, segnatamente, di verificare l'assenza di un tale snaturamento, è essenziale che, qualora l'accesso da parte delle autorità nazionali competenti ai dati conservati comporti il rischio di una grave ingerenza nei diritti fondamentali della persona interessata, tale accesso sia subordinato a un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente [v., in tal senso, sentenza odierna, La Quadrature du Net e a. (Dati personali e lotta alla contraffazione), C-470/21, punti da 124 a 131].

52 Nel caso di specie, risulta dall'ordinanza di rinvio che l'articolo 132, comma 3, del decreto legislativo n. 196/2003 stabilisce le condizioni alle quali l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica può essere autorizzato da un giudice investito di una richiesta motivata di un'autorità pubblica. Tale disposizione definisce i reati per il cui perseguimento può essere autorizzato l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica con riferimento alla pena della reclusione non inferiore nel massimo a tre anni. Essa subordina tale accesso alla duplice condizione che sussistano «sufficienti indizi di reati» e che tali dati siano «rilevanti per l'accertamento dei fatti».

53 Il giudice del rinvio si chiede tuttavia se la definizione, quale risulta da detta disposizione, dei «reati gravi», per il cui perseguimento può essere autorizzato l'accesso ai dati, non sia troppo ampia, ricomprendendo reati che destano solo scarso allarme sociale.

54 A tal riguardo, occorre rilevare, in primo luogo, che una definizione, secondo la quale i «reati gravi», per il cui perseguimento può essere autorizzato l'accesso, sono quelli per i quali la pena reclusiva massima è almeno pari ad una durata determinata dalla legge, è fondata su un criterio oggettivo. Ciò è conforme all'esigenza che la normativa nazionale di cui trattasi si fondi su criteri oggettivi per definire le circostanze e le condizioni alle quali si deve concedere l'accesso ai dati in questione alle autorità nazionali competenti (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 105 nonché giurisprudenza ivi citata).

55 In secondo luogo, dalla giurisprudenza citata al punto 48 della presente sentenza emerge che la definizione data, nel diritto nazionale, dei «reati gravi» che possono permettere un accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, consentendo di trarre precise conclusioni sulla vita privata delle persone interessate, non deve essere talmente ampia da rendere l'accesso a tali dati la regola anziché l'eccezione. Pertanto essa non può ricomprendere la maggior parte dei reati, ciò che avverrebbe se la soglia oltre la quale la massima pena reclusiva prevista per un reato giustifica che quest'ultimo sia qualificato come reato grave fosse fissata ad un livello eccessivamente basso.

56 Orbene, una soglia fissata con riferimento alla pena della reclusione non inferiore nel massimo a tre anni non appare, al riguardo, eccessivamente bassa (v., in tal senso, sentenza del 21 giugno 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, punto 150).

57 Certamente, poiché la definizione dei «reati gravi», per i quali può essere richiesto l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, è stabilita con riferimento non a una pena minima applicabile, bensì ad una pena massima applicabile, non è escluso che un accesso a dati, costitutivo di una grave ingerenza nei diritti fondamentali, possa essere richiesto al fine di

perseguire reati che non rientrano, in realtà, nella criminalità grave (v., per analogia, sentenza del 21 giugno 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, punto 151).

58 Tuttavia, la fissazione di una soglia a partire dalla quale la massima pena reclusiva prevista per un reato giustifica che quest'ultimo sia qualificato come reato grave non è necessariamente contraria al principio di proporzionalità.

59 Da un lato, ciò pare essere il caso di una disposizione quale quella di cui trattasi nel procedimento principale, poiché, come risulta dall'ordinanza di rinvio, essa riguarda, in maniera generale, l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, senza precisare la natura di tali dati. Pertanto, tale disposizione pare ricomprendere segnatamente i casi in cui l'accesso non può essere qualificato come grave ingerenza, in quanto non riguarda un insieme di dati idonei a permettere di trarre precise conclusioni sulla vita privata delle persone interessate.

60 Dall'altro lato, il giudice o l'entità amministrativa indipendente, che interviene nell'ambito di un controllo preventivo effettuato a seguito di una richiesta motivata di accesso, deve poter negare o limitare tale accesso qualora constati che l'ingerenza nei diritti fondamentali che un tale accesso costituirebbe è grave, mentre risulta evidente che il reato in questione non rientra effettivamente nella criminalità grave (v., per analogia, sentenza del 21 giugno 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, punto 152).

61 Infatti, il giudice o l'entità incaricata del controllo deve essere in grado di garantire un giusto equilibrio tra, da un lato, gli interessi legittimi connessi alle esigenze dell'indagine nell'ambito della lotta alla 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 [sentenza odierna, La Quadrature du Net e a. (Dati personali e lotta alla contraffazione), C-470/21, punto 125 nonché giurisprudenza ivi citata].

62 In particolare, allorché esamina la proporzionalità dell'ingerenza nei diritti fondamentali della persona interessata causata dalla richiesta di accesso, tale giudice o tale entità deve essere in grado di escludere detto accesso qualora quest'ultimo sia richiesto nell'ambito di un'azione penale diretta a perseguire un reato manifestamente non grave, ai sensi del punto 50 della presente sentenza.

63 Da quanto precede risulta che occorre rispondere alla 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 non osta a una disposizione nazionale che impone al giudice nazionale – allorché interviene in sede di controllo preventivo a seguito di una richiesta motivata di accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente di un mezzo di comunicazione elettronica, conservati dai fornitori di servizi di comunicazione elettronica, presentata da un'autorità nazionale competente nell'ambito di un'indagine penale – di autorizzare tale accesso qualora quest'ultimo sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni, purché sussistano sufficienti indizi di tali reati e detti dati siano rilevanti per l'accertamento dei fatti, a condizione, tuttavia, che tale giudice abbia la possibilità di negare detto accesso se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato.

Sulle spese

64 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:

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,

dev'essere interpretato nel senso che:

esso non osta a una disposizione nazionale che impone al giudice nazionale – allorché interviene in sede di controllo preventivo a seguito di una richiesta motivata di accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente di un mezzo di comunicazione elettronica, conservati dai fornitori di servizi di comunicazione elettronica, presentata da un'autorità nazionale competente nell'ambito di un'indagine penale – di autorizzare tale accesso qualora quest'ultimo sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni, purché sussistano sufficienti indizi di tali reati e detti dati siano rilevanti per l'accertamento dei fatti, a condizione, tuttavia, che tale giudice abbia la possibilità di negare detto accesso se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato.