dirittifondamentali.it

La Corte di Giustizia si pronuncia in tema di conservazione generalizzata e indifferenziata dei dati relativi al traffico per finalità di lotta alla criminalità
(CGUE, Grande Sezione, sentenza 5 aprile 2022, C-140/20)

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 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta a misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Il predetto articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, non osta, invece, a misure legislative che prevedano, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica,

– la 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;

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

– la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta 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 dispongono tali fornitori di servizi, se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi.

L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificato dalla direttiva 2009/136, letto alla luce degli articoli 7, 8, 11 e dell'articolo 52, paragrafo l, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta a una normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento

di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale.

Il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce della Carta dei diritti fondamentali. L'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività

***

SENTENZA DELLA CORTE (Grande Sezione)
5 aprile 2022 (*)

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Riservatezza delle comunicazioni – Forniture di servizi di comunicazione elettronica – Conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Accesso ai dati conservati – Controllo giurisdizionale a posteriori – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11 e articolo 52, paragrafo 1 – Possibilità per un giudice nazionale di limitare gli effetti nel tempo di una declaratoria di invalidità di una normativa nazionale incompatibile con il diritto dell'Unione – Esclusione»

Nella causa C-140/20,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla Supreme Court (Corte suprema, Irlanda), con decisione del 25 marzo 2020, pervenuta in cancelleria in pari data, nel procedimento

G.D.

contro

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis e N. Jääskinen, presidenti di sezione, T. von Danwitz (relatore), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi e A. Kumin, giudici,

avvocato generale: M. Campos Sánchez-Bordona

cancelliere: D. Dittert, capo unità

vista la fase scritta del procedimento e in seguito all'udienza del 13 settembre 2021,

considerate le osservazioni presentate:

– per G.D., da J. Dunphy, solicitor, R. Kennedy, R. Farrell, SC, e K. McCormack, BL;

– per il Commissioner of An Garda Síochána, il Minister for Communications, Energy and Natural Resources e l'Attorney General, da M. Browne, S. Purcell, C. Stone, J. Quaney e A. Joyce, in qualità di agenti, assistiti da S. Guerin, P. Gallagher, SC, D. Fennelly e L. Dwyer, BL;

– per il governo belga, da P. Cottin e J.-C. Halleux, in qualità di agenti, assistiti da J. Vanpraet, advocaat;

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

– per il governo danese, inizialmente da J. Nymann-Lindegren, M. Jespersen e M. Wolff, poi da M. Wolff e V. Jørgensen, in qualità di agenti;

– per il governo estone, da A. Kalbus e M. Kriisa, in qualità di agenti;

– per il governo spagnolo, da L. Aguilera Ruiz, in qualità di agente;

– per il governo francese, da E. de Moustier, A. Daniel, D. Dubois, T. Stéhelin e J. Illouz, in qualità di agenti;

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

– per il governo dei Paesi Bassi, da C.S. Schillemans, K. Bulterman e A. Hanje, in qualità di agenti;

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

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

– per il governo finlandese, da M. Pere e A. Laine, in qualità di agenti;

– per il governo svedese, da O. Simonsson, J. Lundberg, H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson e H. Eklinder, in qualità di agenti;

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

– per il Garante europeo della protezione dei dati, da D. Nardi, N. Stolič, K. Ujazdowski e A. Buchta, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 18 novembre 2021,

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, 11 e 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 controversia che oppone G.D. al Commissioner of An Garda Síochána (capo della polizia nazionale, Irlanda), al Minister for Communications, Energy and Natural Risorse (Ministro delle comunicazioni, dell'energia e delle risorse naturali, Irlanda) e all'Attorney General (consulente giuridico del governo) in merito alla validità del Communications (Retention of Data) Act 2011 [legge del 2011 sulle comunicazioni (conservazione dei dati); in prosieguo: la «legge del 2011»].

Contesto normativo

Diritto dell'Unione

3 I considerando 2, 6, 7 e 11 della direttiva 2002/58 così recitano:

«(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].

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(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 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 dell['Unione europea].

2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva [95/46]. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del [Trattato FUE], 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».

5 Ai sensi dell'articolo 2 della direttiva 2002/58, intitolato «Definizioni»:

«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;

(...)».

6 L'articolo 3 della direttiva 2002/58, intitolato «Servizi interessati», prevede quanto segue:

«La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell['Unione], comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

7 Ai sensi dell'articolo 5 di tale direttiva, intitolato «Riservatezza delle comunicazioni»:

«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».

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

«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.

(...)».

9 L'articolo 9 della direttiva, 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. (...)».

10 L'articolo 15 della direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», così 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 irlandese

11 Come risulta dalla domanda di pronuncia pregiudiziale, la legge del 2011 è stata adottata al fine di recepire nell'ordinamento giuridico irlandese la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54).

12 L'articolo 1 della legge del 2011 definisce il termine «dati» come «i dati relativi al traffico o i dati relativi all'ubicazione nonché i dati connessi necessari per identificare l'abbonato o l'utente» e il termine «reato grave» come riguardante un reato punibile con una pena detentiva di durata pari o superiore a cinque anni o uno degli altri reati elencati all'allegato 1 di tale legge.

13 L'articolo 3, paragrafo 1, di detta legge impone a tutti i fornitori di servizi di comunicazione elettronica di conservare i dati di cui al suo allegato 2, parte 1, per un periodo di due anni nonché i dati di cui al suo allegato 2, parte 2, per un periodo di un anno.

14 L'allegato 2, parte 1, della medesima legge riguarda, tra l'altro, i dati relativi alla telefonia fissa e alla telefonia mobile che consentono di identificare la fonte e la destinazione di una comunicazione, di determinare la data e l'ora dell'inizio e della fine di una comunicazione, di determinare il tipo di comunicazione di cui trattasi nonché di individuare il tipo e l'ubicazione geografica del materiale di comunicazione utilizzato. In particolare, il punto 6 di tale allegato 2, parte 1, prevede la conservazione dei dati necessari per localizzare un mezzo di comunicazione elettronica mobile, dati che sono, da un lato, l'identificatore di cella e, dall'altro, i dati che permettono di stabilire l'ubicazione geografica delle celle, con riferimento alla loro identità di ubicazione (identificatore di cella), durante il periodo di conservazione dei dati di comunicazione.

15 L'allegato 2, parte 2, della legge del 2011 riguarda i dati relativi all'accesso a Internet, la posta elettronica e la telefonia via Internet e comprende, in particolare, i numeri identificativi e di telefono, gli indirizzi IP nonché la data e l'ora dell'inizio e della fine di una comunicazione. Il contenuto delle comunicazioni non rientra in questo tipo di dati.

16 In forza degli articoli 4 e 5 della legge del 2011, i fornitori di servizi di comunicazione elettronica devono adottare talune misure per garantire che i dati siano protetti dagli accessi non autorizzati.

17 L'articolo 6 di tale legge, che prevede le condizioni alle quali può essere presentata una domanda di accesso, al paragrafo 1 dispone quanto segue:

«Un funzionario della polizia nazionale di grado non inferiore a sovrintendente capo può chiedere a un prestatore di servizi di comunicargli i dati in suo possesso ai sensi dell'articolo 3, se ritiene che i dati in questione siano necessari:

a) alla prevenzione, all'accertamento, alle indagini o al perseguimento di un reato grave,

b) alla salvaguardia della sicurezza dello Stato,

c) alla protezione della vita umana».

18 L'articolo 7 di detta legge impone ai fornitori di servizi di comunicazione elettronica di accogliere le domande di cui all'articolo 6 della stessa.

19 Tra i meccanismi di controllo della decisione del funzionario di polizia nazionale di cui all'articolo 6 della legge del 2011 figurano la procedura di reclamo prevista dall'articolo 10 della legge e la procedura davanti al *designated judge* (giudice designato), ai sensi dell'articolo 12 della stessa, al quale è affidato il compito di esaminare l'applicazione delle disposizioni di detta legge.

Procedimento principale e questioni pregiudiziali

20 Nel marzo 2015 G.D. è stato condannato all'ergastolo per l'omicidio di una persona scomparsa nell'agosto 2012 e i cui resti sono stati scoperti solo nel settembre 2013. Nell'appello contro la sua condanna, l'interessato ha contestato, in particolare, al giudice di primo grado di avere erroneamente ammesso come prova i dati relativi al traffico e i dati relativi all'ubicazione afferenti a chiamate telefoniche, adducendo che la legge del 2011, che disciplinava la conservazione di tali dati e in base alla quale gli investigatori della polizia nazionale avevano avuto accesso agli stessi, violava i diritti conferitigli dal diritto dell'Unione. Tale appello è attualmente pendente.

21 Per poter contestare l'ammissibilità di tali prove nel procedimento penale, G.D. ha intentato un'azione civile presso la High Court (Alta Corte, Irlanda) diretta a far dichiarare l'invalidità di talune disposizioni della legge del 2011. Con decisione del 6 dicembre 2018, tale giudice ha accolto l'argomento di G.D. e ha ritenuto che l'articolo 6, paragrafo 1, lettera a), di tale legge fosse incompatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta. L'Irlanda ha interposto appello avverso tale decisione dinanzi alla Supreme Court (Corte suprema, Irlanda), giudice del rinvio.

22 Il procedimento penale pendente dinanzi alla Court of Appeal (Corte d'appello, Irlanda) è stato sospeso fino alla pronuncia della decisione del giudice del rinvio nell'ambito del procedimento civile principale.

23 Dinanzi al giudice del rinvio, l'Irlanda ha sostenuto che, per determinare se l'ingerenza nel diritto al rispetto della vita privata sancito all'articolo 7 della Carta costituita dalla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione ai sensi della legge del 2011 sia proporzionata, occorre esaminare gli obiettivi del regime istituito da tale legge nel suo complesso. Inoltre, secondo tale Stato membro, detta legge ha istituito un quadro dettagliato che disciplina l'accesso ai dati conservati, in forza del quale l'unità incaricata, in seno alla polizia nazionale, dell'esame preliminare delle domande di accesso gode di un'indipendenza funzionale rispetto alla polizia nazionale nell'esercizio della sua missione e, di conseguenza, soddisfa il requisito di un previo controllo effettuato da un organo amministrativo indipendente. Tale sistema di controllo sarebbe integrato da un procedimento di reclamo e da un controllo giurisdizionale. Infine, detto Stato membro afferma che, se si dovesse ritenere, in definitiva, che la legge del 2011 sia contraria al diritto dell'Unione, qualsiasi constatazione che ne sarà dedotta dal giudice del rinvio dovrebbe unicamente valere, sotto il profilo dei suoi effetti nel tempo, per il futuro.

24 Da parte sua, G.D. ha sostenuto che il regime di conservazione generalizzata e indifferenziata dei dati istituito dalla legge del 2011 nonché il regime di accesso a tali dati previsto da tale legge sono incompatibili con il diritto dell'Unione, come interpretato in particolare dalla Corte al punto 120 della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970).

25 Il giudice del rinvio precisa, in via preliminare, di essere tenuto soltanto a valutare se la High Court (Alta Corte) abbia correttamente dichiarato che l'articolo 6, paragrafo 1, lettera a), della legge del 2011 è incompatibile con il diritto dell'Unione e che, per contro, la questione della ricevibilità delle prove dedotte nell'ambito del processo penale rientra nella competenza esclusiva della Court of Appeal (Corte d'appello), investita dell'appello proposto avverso la decisione di condanna.

26 In tale contesto, il giudice del rinvio si interroga, anzitutto, sui requisiti del diritto dell'Unione per quanto riguarda la conservazione dei dati a fini di lotta contro la criminalità grave. A tal riguardo, esso ritiene, in sostanza, che solo una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione consenta di lottare, in maniera efficace, contro

la criminalità grave, cosa che una conservazione mirata e una conservazione rapida (*quick freeze*) non consentirebbero di fare. Per quanto riguarda la conservazione mirata, il giudice del rinvio si interroga sulla possibilità di prendere in considerazione gruppi o zone geografiche determinati ai fini della lotta alla criminalità grave, in quanto taluni reati gravi raramente implicherebbero circostanze note alle autorità nazionali competenti e che consentono loro di sospettare la commissione di un reato prima che avvenga. Inoltre, una conservazione mirata potrebbe dar luogo a discriminazioni. Quanto alla conservazione rapida, il giudice del rinvio ritiene che essa sia utile solo in situazioni in cui esista una persona sospettata identificabile in una fase precoce dell'indagine.

27 Per quanto riguarda, poi, l'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, il giudice del rinvio sottolinea che la polizia nazionale ha istituito, al suo interno, un meccanismo di autocertificazione delle domande di accesso rivolte a tali fornitori. Infatti, dagli elementi prodotti dinanzi alla High Court (Alta Corte) risulterebbe che il capo della polizia nazionale ha deciso, quale misura interna, che le domande di accesso presentate ai sensi della legge del 2011 devono essere oggetto di un trattamento centralizzato da un solo agente della polizia nazionale, avente la qualità di sovrintendente capo, ossia il capo della sezione Sicurezza e Informazione. Quest'ultimo, se ritiene che i dati di cui trattasi siano necessari ai fini, in particolare, della prevenzione, dell'accertamento, della ricerca o del perseguimento di un reato grave, può presentare una domanda di accesso ai fornitori di servizi di comunicazione elettronica. Inoltre, il capo della polizia nazionale avrebbe istituito, all'interno di quest'ultima, un'unità autonoma denominata *Telecommunications Liage Unit* (Unità di collegamento in materia di telecomunicazioni; in prosieguo: la «TLU»), al fine di fornire un sostegno al capo della sezione Sicurezza e Informazione nell'esercizio delle sue funzioni e di fungere da punto di contatto unico con i prestatori di servizi.

28 Il giudice del rinvio aggiunge che, durante il periodo interessato dall'indagine penale avviata nei confronti di G.D., tutte le domande di accesso dovevano essere approvate in primo luogo da un commissario o da un ispettore facente funzioni di commissario, prima di essere inviate alla TLU per essere trattate, e che gli inquirenti erano invitati a corredare le loro domande di accesso di dettagli sufficienti affinché potesse essere adottata una decisione informata. Inoltre, la TLU e il capo della sezione Sicurezza e Informazione erano tenuti a esaminare la legittimità, la necessità e la proporzionalità delle domande di accesso, tenendo presente che tale capo poteva essere chiamato a rispondere della sua decisione dinanzi a un giudice designato dalla High Court (Alta Corte). Oltre a ciò, la TLU sarebbe subordinata al controllo del Data Protection Commissioner (garante per la protezione dei dati, Irlanda).

29 Infine, il giudice del rinvio si interroga sulla portata e sugli effetti nel tempo di un'eventuale dichiarazione di non conformità della legge del 2011 al diritto dell'Unione. A tal riguardo, esso precisa che una siffatta dichiarazione potrebbe valere solo per il futuro, in quanto i dati utilizzati come prove nel procedimento penale a carico di G.D. sono stati oggetto di conservazione e di accesso alla fine del 2013, vale a dire in un periodo in cui l'Irlanda era tenuta ad applicare le disposizioni della legge del 2011 di recepimento della direttiva 2006/24. Secondo l'Irlanda, una soluzione del genere sarebbe appropriata anche in quanto, altrimenti, la ricerca e il perseguimento dei reati gravi in Irlanda, nonché la situazione di persone già giudicate e condannate, potrebbero risultare seriamente compromessi.

30 In tali circostanze la Supreme Court (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se un regime generale o universale di conservazione dei dati, anche soggetto a rigorose restrizioni in materia di conservazione e accesso, sia di per sé contrario alle disposizioni dell'articolo 15 della direttiva [2002/58], per come interpretate alla luce della [Carta].

2) Se, nel valutare la concessione di una declaratoria di incompatibilità di una misura nazionale attuata ai sensi della direttiva [2006/24] e che prevede un regime generale di conservazione dei dati (soggetto ai necessari rigorosi controlli in materia di conservazione e/o di accesso) e, in particolare, nel valutare la proporzionalità di tale regime, un giudice nazionale possa tener conto della circostanza che i dati possono essere legalmente conservati da prestatori di servizi per fini commerciali propri e potrebbe essere richiesta una loro conservazione per motivi di sicurezza nazionale esclusi dalle disposizioni della direttiva [2002/58].

3) Nel valutare la compatibilità con il diritto dell'Unione e, in particolare, con i diritti della Carta, di una misura nazionale di accesso ai dati conservati, quali criteri dovrebbe applicare un giudice nazionale per stabilire se un siffatto regime di accesso preveda il necessario controllo preventivo indipendente, come stabilito dalla Corte di giustizia nella sua giurisprudenza. In tale contesto, se un giudice nazionale possa, nell'ambito di tale valutazione, tener conto dell'esistenza di un controllo ex post di natura giurisdizionale o indipendente.

4) In ogni caso, se un giudice nazionale sia tenuto a dichiarare l'incompatibilità di una misura nazionale con le disposizioni dell'articolo 15 della direttiva [2002/58], qualora tale misura nazionale preveda un regime generale di conservazione dei dati ai fini della lotta contro reati gravi e laddove il giudice nazionale abbia concluso, sulla base di tutti gli elementi di prova disponibili, che tale conservazione sia al contempo indispensabile e strettamente necessaria al raggiungimento dell'obiettivo della lotta contro reati gravi.

5) Qualora un giudice nazionale sia tenuto a dichiarare l'incompatibilità di una misura nazionale rispetto alle disposizioni dell'articolo 15 della direttiva [2002/58], come interpretate alla luce della Carta, se tale giudice abbia il diritto di limitare gli effetti nel tempo di tale declaratoria, ove ritenga che, in caso contrario, ciò comporterebbe un "conseguente grave disordine e un danno all'interesse pubblico" [conformemente all'approccio adottato, ad esempio, nella sentenza R (National Council for Civil Liberties)/Secretary of State for Home Department e Secretary of State for Foreign Affairs [2018] EWHC 975, punto 46].

6) Se un giudice nazionale, chiamato a dichiarare l'incompatibilità della legislazione nazionale con l'articolo 15 della direttiva [2002/58], e/o a disapplicare tale legislazione e/o a dichiarare che l'applicazione di tale legislazione ha violato i diritti di un singolo, sia nell'ambito di un procedimento avviato al fine di agevolare un dibattito sull'ammissibilità delle prove nell'ambito di un procedimento penale che in altro ambito, possa essere autorizzato a rifiutare l'emissione di tale provvedimento in relazione ai dati conservati in applicazione della disposizione nazionale adottata nel rispetto dell'obbligo di cui all'articolo 288 TFUE di introdurre fedelmente nel diritto nazionale le disposizioni di una direttiva, o a limitare l'efficacia di tale declaratoria al periodo successivo alla dichiarazione di invalidità della direttiva [2006/24] [da parte della sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238)]».

Sulle questioni pregiudiziali

Sulla prima, la seconda e la quarta questione

31 Con le questioni prima, seconda e quarta, 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 l, della Carta, debba essere interpretato nel senso che esso osta a una normativa nazionale che preveda una conservazione generalizzata e

indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di lotta alla criminalità grave.

32 Occorre ricordare, in via preliminare, che, secondo costante giurisprudenza, al fine di interpretare una disposizione del diritto dell'Unione, occorre riferirsi non soltanto alla lettera della stessa, ma anche al suo contesto e agli scopi perseguiti dalla normativa di cui essa fa parte nonché prendere in considerazione, in particolare, la genesi di tale normativa (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 105 e giurisprudenza citata).

33 Dalla formulazione stessa dell'articolo 15, paragrafo 1, della direttiva 2002/58 risulta che le disposizioni legislative che in forza di essa gli Stati membri sono autorizzati ad adottare, alle condizioni da essa stabilite, possono mirare soltanto «a limitare la portata» dei diritti e degli obblighi previsti in particolare agli articoli 5, 6 e 9 della direttiva 2002/58.

34 Per quanto riguarda il sistema istituito da tale direttiva e nel quale si inserisce l'articolo 15, paragrafo 1, della stessa, occorre ricordare che, ai sensi dell'articolo 5, paragrafo 1, prima e seconda frase, di detta direttiva, gli Stati membri sono tenuti a garantire, mediante la loro legislazione nazionale, la riservatezza delle comunicazioni effettuate tramite una rete pubblica di comunicazione e di servizi di comunicazione elettronica accessibili al pubblico, nonché la riservatezza dei relativi dati sul traffico. In particolare, essi hanno l'obbligo di vietare a persone diverse dagli utenti di ascoltare, captare, memorizzare le comunicazioni e i relativi dati sul traffico o di sottoporle a qualsiasi altro mezzo di intercettazione o di sorveglianza, senza il consenso degli utenti interessati, salvo quando tale persona vi sia legalmente autorizzata, conformemente all'articolo 15, paragrafo 1, della medesima direttiva.

35 A tal riguardo, la Corte ha già dichiarato che l'articolo 5, paragrafo 1, della direttiva 2002/58 sancisce il principio di riservatezza sia delle comunicazioni elettroniche sia dei dati relativi al traffico a queste correlati e implica, in particolare, il divieto imposto, in linea di principio, a qualsiasi persona diversa dagli utenti di memorizzare senza il loro consenso tali comunicazioni e dati (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 107).

36 Tale disposizione riflette l'obiettivo perseguito dal legislatore dell'Unione al momento dell'adozione della direttiva 2002/58. Risulta, infatti, dall'esposizione dei motivi della proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [COM(2000) 385 def.], all'origine della direttiva 2002/58, che il legislatore dell'Unione ha inteso «assicurare un elevato livello di tutela dei dati personali e della vita privata per tutti i servizi di comunicazione elettronica, indipendentemente dalla tecnologia da essi usata». Detta direttiva ha quindi lo scopo, come risulta in particolare dai considerando 6 e 7, di tutelare gli utenti dei servizi di comunicazione elettronica dai pericoli per i loro dati personali e la loro vita privata derivanti dalle nuove tecnologie e, in particolare, dalla maggiore capacità di memorizzazione e di trattamento automatizzati di dati. In particolare, come enunciato dal considerando 2 della medesima direttiva, la volontà del legislatore dell'Unione è di garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 della Carta (v., in tal senso, sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, EU:C:2016:970, punto 83, 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 106).

37 Adottando la direttiva 2002/58, il legislatore dell'Unione ha pertanto concretizzato tali diritti, di modo che gli utenti dei mezzi di comunicazione elettronica hanno il diritto di attendersi, in linea di principio, che le loro comunicazioni e i dati a queste correlati, in mancanza del loro consenso,

rimangano anonimi e non possano essere registrati (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 109).

38 Per quanto riguarda il trattamento e la memorizzazione da parte dei fornitori di servizi di comunicazione elettronica dei dati sul traffico relativi agli abbonati e agli utenti, l'articolo 6 della direttiva 2002/58 prevede, al paragrafo 1, che tali dati debbano essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, e precisa, al paragrafo 2, che i dati sul traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. Quanto ai dati relativi all'ubicazione diversi dai dati relativi al traffico, l'articolo 9, paragrafo 1, di detta direttiva stabilisce che tali dati possano essere trattati soltanto a determinate condizioni e dopo essere stati resi anonimi o con il consenso degli utenti o degli abbonati.

39 Pertanto, la direttiva 2002/58 non si limita a disciplinare l'accesso a tali dati mediante garanzie dirette a prevenire gli abusi, ma sancisce altresì, in particolare, il principio del divieto della loro memorizzazione da parte di terzi.

40 Nei limiti in cui l'articolo 15, paragrafo 1, della direttiva 2002/58 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 di tale direttiva, come quelli derivanti dai principi di riservatezza delle comunicazioni e dal divieto di memorizzazione dei dati ad esse relativi, ricordati al punto 35 della presente sentenza, tale disposizione prevede un'eccezione alla regola generale dettata in particolare dagli articoli 5, 6 e 9 e deve pertanto, conformemente a una giurisprudenza costante, essere oggetto di un'interpretazione restrittiva. Una siffatta 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 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 (v., in tal senso, sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, EU:C:2016:970, punto 89, 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 111).

41 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 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 112 e giurisprudenza citata).

42 Inoltre, dall'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 risulta che le misure adottate dagli Stati membri ai sensi di tale disposizione devono essere conformi ai principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e assicurare il rispetto dei diritti fondamentali garantiti dalla Carta. A tal riguardo, la Corte ha già dichiarato che l'obbligo imposto da uno Stato membro ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale, di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7 e 8 della Carta, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali, ma anche dell'articolo 11 della Carta, relativo alla libertà di espressione (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 113 e giurisprudenza citata).

43 Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/85 deve tenere conto dell'importanza sia del diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto alla protezione dei dati personali, sancito dall'articolo 8 di quest'ultima, quale emerge dalla giurisprudenza della Corte, nonché del diritto alla libertà di espressione, dal momento che tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata (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 114 e giurisprudenza citata).

44 Occorre precisare, a tale proposito, che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce, di per sé, da un lato, una deroga al divieto, previsto dall'articolo 5, paragrafo 1, della direttiva 2002/58, per qualsiasi persona diversa dagli utenti di memorizzare tali dati e, dall'altro, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta, a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile, che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza o che i dati conservati siano o meno utilizzati successivamente (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, punti 115 e 116, e giurisprudenza citata).

45 Questa conclusione risulta tanto più giustificata in quanto i dati relativi al traffico e i dati relativi all'ubicazione possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati, comprese informazioni sensibili, quali l'orientamento sessuale, le opinioni politiche, le convinzioni religiose, filosofiche, sociali o di altro tipo nonché lo stato di salute, mentre tali dati beneficiano, peraltro, di una tutela particolare nel diritto dell'Unione. Presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla 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 dette persone e gli ambienti sociali da esse frequentati. In particolare, questi dati forniscono gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni (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 e giurisprudenza citata).

46 Pertanto, da un lato, la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di polizia è idonea a ledere il diritto al rispetto delle comunicazioni, sancito dall'articolo 7 della Carta, e a comportare effetti dissuasivi sull'esercizio, da parte degli utenti dei mezzi di comunicazione elettronica, della loro libertà di espressione, garantita dall'articolo 11 della Carta, effetti che sono tanto più gravi quanto maggiori sono il numero e la varietà dei dati conservati. Dall'altro lato, tenuto conto della quantità rilevante di dati relativi al traffico e di dati relativi all'ubicazione che possono essere conservati continuativamente mediante una misura di conservazione generalizzata e indifferenziata nonché del carattere sensibile delle informazioni che tali dati possono fornire, la conservazione di questi da parte dei fornitori di servizi di comunicazione elettronica comporta di per sé rischi di abuso e di accesso illecito (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 118 e 119, nonché giurisprudenza citata).

47 A questo proposito, occorre sottolineare che la conservazione di tali dati e l'accesso ad essi costituiscono, come risulta dalla giurisprudenza richiamata al punto 44 della presente sentenza, ingerenze distinte nei diritti fondamentali garantiti agli articoli 7 e 11 della Carta, che richiedono

una giustificazione distinta, ai sensi dell'articolo 52, paragrafo 1, della stessa. Ne consegue che una normativa nazionale che garantisce il pieno rispetto delle condizioni risultanti dalla giurisprudenza che ha interpretato la direttiva 2002/58 in materia di accesso ai dati conservati non può, per sua natura, essere idonea né a limitare e neppure a rimediare all'ingerenza grave, che risulterebbe dalla conservazione generalizzata di tali dati prevista da tale normativa nazionale, nei diritti garantiti dagli articoli 5 e 6 di tale direttiva e dai diritti fondamentali di cui tali articoli costituiscono la concretizzazione.

48 Ciò premesso, consentendo agli Stati membri di limitare i diritti e gli obblighi di cui ai punti da 34 a 37 della presente sentenza, l'articolo 15, paragrafo 1, della direttiva 2002/58 riflette il fatto che i diritti sanciti agli articoli 7, 8 e 11 della Carta non appaiono prerogative assolute, ma vanno considerati alla luce della loro funzione sociale. Infatti, come risulta dall'articolo 52, paragrafo 1, della Carta, quest'ultima ammette limitazioni all'esercizio di tali diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale dei summenzionati diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 alla luce della Carta richiede che si tenga conto allo stesso modo dell'importanza dei diritti sanciti agli articoli 3, 4, 6 e 7 della Carta e di quella che rivestono gli obiettivi di salvaguardia della sicurezza nazionale e di lotta alle forme gravi di criminalità nel contribuire alla protezione dei diritti e delle libertà altrui (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 da 120 a 122 nonché giurisprudenza citata).

49 Quindi, per quanto riguarda, in particolare, la lotta effettiva contro i reati di cui sono vittime, segnatamente, i minori e le altre persone vulnerabili si deve tener conto del fatto che dall'articolo 7 della Carta possono derivare obblighi positivi a carico dei pubblici poteri ai fini dell'adozione di misure giuridiche dirette a tutelare la vita privata e familiare. Obblighi siffatti possono parimenti derivare da detto articolo 7 per quanto riguarda la protezione del domicilio e delle comunicazioni, nonché dagli articoli 3 e 4 relativamente alla tutela dell'integrità fisica e psichica delle persone e al divieto di tortura e di trattamenti inumani e degradanti (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 126 e giurisprudenza citata).

50 Di fronte a questi diversi obblighi positivi, occorre quindi procedere al contemperamento dei diversi interessi legittimi e diritti in gioco. Infatti, la Corte europea dei diritti dell'uomo ha dichiarato che gli obblighi positivi derivanti dagli articoli 3 e 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, le cui garanzie corrispondenti figurano agli articoli 4 e 7 della Carta, implicano, in particolare, l'adozione di disposizioni sostanziali e procedurali nonché di misure di natura pratica che consentano di contrastare efficacemente i reati contro le persone attraverso indagini e azioni penali efficaci, obbligo che risulta ancora più importante quando sia minacciato il benessere fisico e morale di un minore. Ciò detto, le misure che spetta alle autorità competenti adottare devono rispettare pienamente le regole del giusto procedimento e le altre garanzie idonee a limitare la portata dei poteri di indagine penale nonché gli altri diritti e libertà. In particolare, secondo tale giudice, occorre stabilire un quadro normativo che consenta di conciliare i diversi interessi legittimi e diritti da tutelare (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 127 e 128 e giurisprudenza citata).

51 In tale contesto, dalla formulazione stessa dell'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 discende che gli Stati membri possono adottare una misura che deroga al principio di riservatezza evocato al punto 35 della presente sentenza qualora tale misura sia «necessaria,

opportuna e proporzionata all'interno di una società democratica», alla luce degli obiettivi enunciati da detta disposizione, laddove il considerando 11 di detta direttiva precisa che una misura siffatta deve essere «strettamente» proporzionata allo scopo perseguito (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 129).

52 A tal riguardo, occorre ricordare che la tutela del diritto fondamentale al rispetto della vita privata esige, conformemente alla giurisprudenza costante della Corte, che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario. Inoltre, un obiettivo di interesse generale non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un contemperamento equilibrato tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi (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 e giurisprudenza citata).

53 Più in particolare, dalla giurisprudenza della Corte risulta che 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 e giurisprudenza citata).

54 Per soddisfare il requisito di proporzionalità, una normativa deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e fissino un minimo di requisiti, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso. Tale normativa deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato, in particolare quando esiste un rischio considerevole di accesso illecito ai dati stessi. Tali considerazioni valgono segnatamente quando è in gioco la protezione di quella categoria particolare di dati personali che sono i dati sensibili (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 132 e giurisprudenza citata).

55 Pertanto, una normativa che preveda una conservazione dei dati personali deve sempre rispondere a criteri oggettivi, che mettano in rapporto i dati da conservare con l'obiettivo perseguito. In particolare, per quanto riguarda la lotta alla criminalità grave, i dati che si prevede di conservare devono essere tali da contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi (v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 59, 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 133).

56 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, in particolare dalla 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), 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.

57 A questo proposito, la Corte ha statuito che 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 (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, punti 135 e 136).

58 È per questo motivo che la Corte ha affermato 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, non osta a misure legislative che consentano, a fini di salvaguardia della sicurezza nazionale, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica di procedere a una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, in situazioni nelle quali lo Stato membro interessato affronti una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, ove il provvedimento che prevede tale ingiunzione possa essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, diretto ad accertare l'esistenza di una di tali situazioni nonché il rispetto delle condizioni e delle garanzie che devono essere previste, e detta ingiunzione possa essere emessa solo per un periodo temporalmente limitato allo stretto necessario, ma sia rinnovabile in caso di persistenza di tale minaccia (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).

59 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 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 140 e giurisprudenza citata).

60 In udienza, la Commissione europea ha sostenuto che la criminalità particolarmente grave potrebbe essere assimilata ad una minaccia per la sicurezza nazionale.

61 Ebbene, la Corte ha già statuito che l'obiettivo di preservare la sicurezza nazionale corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società mediante la prevenzione e la repressione delle attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo (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, punto 135).

62 Occorre inoltre rilevare che, a differenza della criminalità, anche particolarmente grave, una minaccia per la sicurezza nazionale deve essere reale ed attuale o, quanto meno, prevedibile, il che

presuppone il verificarsi di circostanze sufficientemente concrete, da poter giustificare una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, per un periodo limitato. Una minaccia del genere si distingue quindi, per sua natura, per gravità e specificità delle circostanze che la costituiscono, dal rischio generale e permanente rappresentato dal verificarsi di tensioni o di perturbazioni, anche gravi, della pubblica sicurezza o da quello di reati gravi (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 136 e 137).

63 Pertanto, la criminalità, anche particolarmente grave, non può essere equiparata a una minaccia per la sicurezza nazionale. Infatti, come rilevato dall'avvocato generale ai paragrafi 49 e 50 delle sue conclusioni, una siffatta equiparazione equivarrebbe a introdurre una categoria intermedia tra la sicurezza nazionale e la sicurezza pubblica, per applicare alla seconda i requisiti inerenti alla prima.

64 Ne consegue anche che il fatto, menzionato nella seconda questione pregiudiziale, che i dati relativi al traffico e i dati relativi all'ubicazione siano stati legittimamente conservati per salvaguardare la sicurezza nazionale è irrilevante per la legittimità della loro conservazione ai fini della lotta contro la criminalità grave.

65 Per quanto riguarda l'obiettivo della lotta alle forme gravi di criminalità, la Corte ha statuito che una normativa nazionale che prevede, a tal fine, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione travalica i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica. Infatti, tenuto conto del carattere sensibile delle informazioni che i dati relativi al traffico e i dati relativi all'ubicazione possono fornire, la riservatezza di tali dati è essenziale per il diritto al rispetto della vita privata. Pertanto, e tenuto conto, da un lato, degli effetti dissuasivi sull'esercizio dei diritti fondamentali sanciti dagli articoli 7 e 11 della Carta, menzionati al punto 46 della presente sentenza, che la conservazione di tali dati può determinare e, dall'altro, della gravità dell'ingerenza che una siffatta conservazione comporta, occorre, in una società democratica, che detta ingerenza costituisca, come prevede il sistema istituito dalla direttiva 2002/58, l'eccezione e non la regola e che i dati in questione non possano essere oggetto di una conservazione sistematica e continuativa. Questa conclusione si impone anche con riguardo agli obiettivi di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica nonché all'importanza che occorre loro riconoscere (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 141 e 142 e giurisprudenza citata).

66 Inoltre, la Corte ha sottolineato che una normativa che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione riguarda le comunicazioni elettroniche della quasi totalità della popolazione senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito. Una normativa siffatta riguarda in maniera globale l'insieme delle persone che si avvalgono di servizi di comunicazione elettronica, senza che tali persone si trovino, neanche indirettamente, in una situazione idonea a dar luogo ad azioni penali. Essa si applica quindi anche a persone per le quali non vi è alcun indizio che il loro comportamento possa avere un legame, anche indiretto o remoto, con l'obiettivo di combattere gli atti di criminalità grave e, in particolare, senza che sia stabilita una correlazione tra i dati di cui è prevista la conservazione e una minaccia per la sicurezza pubblica. In particolare, come già dichiarato dalla Corte, una normativa siffatta non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui

dati, per altri motivi, potrebbe contribuire alla lotta contro la criminalità grave (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 143 e 144 e giurisprudenza citata).

67 Per contro, al punto 168 della 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), la Corte ha precisato che l'articolo 15, paragrafo 1, della direttiva 2002/58, 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 alle forme gravi di criminalità e della prevenzione delle minacce gravi alla sicurezza pubblica

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

– una conservazione generalizzata e indifferenziata dei dati relativi all'identità civile 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 (*quick freeze*) dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono,

se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi.

68 Nella presente domanda di pronuncia pregiudiziale, che è pervenuta alla Corte prima della pronuncia delle sentenze del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), e del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152), il giudice del rinvio ha tuttavia ritenuto che solo una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione consenta di combattere efficacemente le forme gravi di criminalità. All'udienza del 13 settembre 2021 è stato sostenuto, in particolare dall'Irlanda e dal governo francese, che una tale affermazione non era invalidata dal fatto che gli Stati membri possano ricorrere alle misure menzionate al punto precedente.

69 A tal riguardo, occorre rilevare, in primo luogo, che l'efficacia delle azioni penali dipende in genere non da un solo strumento di indagine, bensì da tutti gli strumenti di indagine di cui dispongono le autorità nazionali competenti a tal fine.

70 In secondo luogo, occorre sottolineare 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, come interpretato dalla giurisprudenza ricordata al punto 67 della presente sentenza, consente agli Stati membri di adottare, ai fini della lotta alle forme gravi di criminalità e della prevenzione di minacce gravi alla sicurezza pubblica, non solo misure che istituiscono una conservazione mirata e una conservazione rapida, ma anche misure che prevedano una conservazione generalizzata e indifferenziata, da un lato, dei dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica e, dall'altro, degli indirizzi IP attribuiti alla fonte di una connessione.

71 A tale riguardo, è pacifico che la conservazione dei dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica può contribuire alla lotta alle forme gravi di criminalità,

purché tali dati consentano di identificare le persone che hanno utilizzato simili mezzi nell'ambito della preparazione o della commissione di un atto rientrante nelle forme gravi di criminalità.

72 Ebbene, come risulta dalla giurisprudenza sintetizzata al punto 67 della presente sentenza, la direttiva 2002/58 non osta, ai fini della lotta alla criminalità in generale, alla conservazione generalizzata dei dati relativi all'identità civile. Ciò considerato, occorre precisare che né tale direttiva né alcun altro atto del diritto dell'Unione ostano a una normativa nazionale, avente ad oggetto la lotta alla criminalità grave, ai sensi della quale l'acquisizione di un mezzo di comunicazione elettronica, quale una carta SIM prepagata, è subordinata alla verifica di documenti ufficiali che provino l'identità dell'acquirente e alla registrazione, da parte del venditore, delle informazioni che ne derivano, essendo il venditore eventualmente tenuto a consentire l'accesso a tali informazioni alle autorità nazionali competenti.

73 Inoltre, occorre ricordare che la conservazione generalizzata degli indirizzi IP della fonte della connessione costituisce un'ingerenza grave nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, dal momento che tali indirizzi IP possono consentire di trarre conclusioni precise sulla vita privata dell'utente dal mezzo di comunicazione elettronica interessato e può avere effetti dissuasivi sull'esercizio della libertà di espressione garantita dall'articolo 11 della stessa. Tuttavia, per quanto riguarda siffatta conservazione, la Corte ha affermato che, ai fini del necessario contemperamento dei diritti e degli interessi legittimi in gioco richiesto dalla giurisprudenza di cui ai punti da 50 a 53 della presente sentenza, occorre tener conto del fatto che, nel caso di un reato commesso online e, in particolare, nel caso dell'acquisto, della diffusione, della trasmissione o della messa a disposizione online di materiale pedopornografico, ai sensi dell'articolo 2, lettera c), della direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU 2011, L 335, pag. 1) l'indirizzo IP può costituire l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione di detto reato (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 153 e 154).

74 Pertanto, la Corte ha statuito che una siffatta conservazione generalizzata e indifferenziata dei soli indirizzi IP attribuiti alla fonte di una connessione non risulta, in linea di principio, contraria all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta, purché tale possibilità sia subordinata al rigoroso rispetto delle condizioni sostanziali e procedurali che devono disciplinare l'utilizzo di tali dati di cui ai punti 155 e 156 della 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).

75 In terzo luogo, per quanto riguarda le misure legislative che prevedono una conservazione mirata e una conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione, dalle indicazioni contenute nella domanda di pronuncia pregiudiziale emerge una comprensione più restrittiva della portata di tali misure rispetto a quella accolta dalla giurisprudenza richiamata al punto 67 della presente sentenza. Infatti, sebbene, conformemente a quanto ricordato al punto 40 della presente sentenza, tali misure di conservazione debbano avere natura derogatoria nel sistema istituito dalla direttiva 2002/58, quest'ultima, letta alla luce dei diritti fondamentali sanciti agli articoli 7, 8 e 11 nonché all'articolo 52, paragrafo 1, della Carta, non subordina la possibilità di emettere un'ingiunzione che impone una conservazione mirata alla condizione che siano conosciuti, in anticipo, i luoghi che possono essere la scena di un atto di criminalità grave né le persone sospettate di essere implicate in un atto del genere. Del pari, detta direttiva non richiede che

l'ingiunzione che impone una conservazione rapida sia limitata a persone sospette identificate prima di una siffatta ingiunzione.

76 Per quanto riguarda, sotto un primo profilo, la conservazione mirata, la Corte ha dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58 non osta a una normativa nazionale fondata su elementi oggettivi che permettano di prendere in considerazione, da un lato, le persone i cui dati relativi al traffico e all'ubicazione sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave o a prevenire un grave rischio per la sicurezza pubblica o, ancora, un rischio per la sicurezza nazionale (sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15,EU:C:2016:970, punto 111, 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 148).

77 La Corte ha precisato al riguardo che, anche se tali elementi oggettivi possono variare a seconda delle misure adottate per la prevenzione, la ricerca, l'accertamento e il perseguimento di atti di criminalità grave, le persone in tal modo considerate possono essere, in particolare, quelle precedentemente identificate, nell'ambito delle procedure nazionali applicabili e sulla base di elementi oggettivi e non discriminatori, come soggetti che costituiscono una minaccia per la sicurezza pubblica o la sicurezza nazionale dello Stato membro interessato (v., in tal senso, sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15,EU:C:2016:970, punto 110, 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 149).

78 Gli Stati membri hanno quindi, in particolare, la facoltà di adottare misure di conservazione nei confronti di persone che, nell'ambito di tale identificazione, sono sottoposte ad indagine o ad altre misure di sorveglianza in corso o sono iscritte nel casellario giudiziario nazionale ove è menzionata una condanna precedente per atti di criminalità grave che possono comportare un elevato rischio di recidiva. Orbene, quando una siffatta identificazione è fondata su elementi oggettivi e non discriminatori, definiti dal diritto nazionale, la conservazione mirata riguardante persone così identificate è giustificata.

79 Dall'altro lato, una misura di conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione può, a seconda della scelta del legislatore nazionale e nel rigoroso rispetto del principio di proporzionalità, essere fondata anche su un criterio geografico qualora le autorità nazionali competenti ritengano, sulla base di elementi oggettivi e non discriminatori, che sussista, in una o più zone geografiche, una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave. Tali zone possono essere, in particolare, luoghi caratterizzati da un numero elevato di atti di criminalità grave, luoghi particolarmente esposti alla commissione di atti di criminalità grave, quali luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone, o ancora luoghi strategici, quali aeroporti, stazioni o aree di pedaggio (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 150 nonché giurisprudenza citata).

80 Occorre sottolineare che, secondo tale giurisprudenza, le autorità nazionali competenti possono adottare, per le zone di cui al punto precedente, una misura di conservazione mirata basata su un criterio geografico, come in particolare il tasso medio di criminalità in una zona geografica, senza che esse dispongano necessariamente di indizi concreti relativi alla preparazione o alla commissione, nelle zone interessate, di atti di criminalità grave. Poiché una conservazione mirata basata su un simile criterio può interessare, in funzione dei reati gravi considerati e della situazione propria dei rispettivi Stati membri, sia luoghi caratterizzati da un elevato numero di atti di criminalità grave sia luoghi particolarmente esposti alla commissione di atti del genere, essa non è,

in linea di principio, idonea a dar maggiormente luogo a discriminazioni, dato che il criterio relativo al tasso medio di criminalità grave non presenta, di per sé, alcun nesso con elementi potenzialmente discriminatori.

81 Inoltre e soprattutto, una misura di conservazione mirata riguardante luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone o luoghi strategici, quali aeroporti, stazioni, porti marittimi o zone di pedaggio, consente alle autorità competenti di raccogliere dati relativi al traffico e, in particolare, dati relativi all'ubicazione di tutte le persone che utilizzano, in un determinato momento, un mezzo di comunicazione elettronica in uno di tali luoghi. Pertanto, una siffatta misura di conservazione mirata può consentire a dette autorità di ottenere, tramite l'accesso ai dati così conservati, informazioni sulla presenza di tali persone nei luoghi o nelle zone geografiche interessati da tale misura nonché sui loro spostamenti tra o all'interno di questi ultimi e di trarne, ai fini della lotta alla criminalità grave, conclusioni sulla loro presenza e sulla loro attività in tali luoghi o zone geografiche in un determinato momento durante il periodo di conservazione.

82 Occorre poi rilevare che le zone geografiche interessate da siffatta conservazione mirata possono e, se del caso, devono essere modificate in funzione dell'evoluzione delle condizioni che ne hanno giustificato la selezione, consentendo così in particolare di reagire alle evoluzioni della lotta contro le forme gravi di criminalità. Infatti, la Corte ha già dichiarato che la durata delle misure di conservazione mirata descritte ai punti da 76 a 81 della presente sentenza non può eccedere quella strettamente necessaria alla luce dell'obiettivo perseguito e delle circostanze che le giustificano, fatto salvo un eventuale rinnovo a motivo della persistenza della necessità di procedere a una siffatta conservazione (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 151).

83 Per quanto riguarda la possibilità di prevedere criteri distintivi diversi da un criterio personale o geografico per attuare una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, non si può escludere che altri criteri, oggettivi e non discriminatori, possano essere presi in considerazione per garantire che la portata di una conservazione mirata sia limitata allo stretto necessario e per stabilire un nesso, almeno indiretto, tra gli atti di criminalità grave e le persone i cui dati sono conservati. Ciò premesso, poiché l'articolo 15, paragrafo 1, della direttiva 2002/58 riguarda misure legislative degli Stati membri, è a questi ultimi e non alla Corte che spetta identificare siffatti criteri, fermo restando che non può trattarsi di reintrodurre, in tal modo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

84 In ogni caso, come rilevato dall'avvocato generale Campos Sánchez-Bordona al paragrafo 50 delle sue conclusioni nelle cause riunite SpaceNet e Telekom Deutschland (C-793/19 e C-794/19, EU:C:2021:939), l'eventuale esistenza di difficoltà nel definire con precisione le ipotesi e le condizioni in cui può essere effettuata una conservazione mirata non può giustificare il fatto che alcuni Stati membri, facendo dell'eccezione una regola, prevedano una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

85 Per quanto riguarda, sotto un secondo profilo, la conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione trattati e memorizzati dai fornitori di servizi di comunicazione elettronica sulla base degli articoli 5, 6 e 9 della direttiva 2002/58 o su quella di misure legislative adottate in forza dell'articolo 15, paragrafo 1, di tale direttiva, occorre ricordare che simili dati devono, in linea di principio, essere cancellati o resi anonimi, a seconda dei casi, alla scadenza dei termini legali entro i quali devono intervenire, conformemente alle disposizioni nazionali che recepiscono detta direttiva, il loro trattamento e la loro memorizzazione. Tuttavia, la Corte ha

stabilito che, durante il trattamento o la memorizzazione, possono presentarsi situazioni nelle quali si pone la necessità di conservare tali dati oltre i suddetti termini al fine di indagare su reati gravi o attentati alla sicurezza nazionale, e ciò sia quando tali reati o attentati abbiano già potuto essere accertati, sia quando la loro esistenza possa essere ragionevolmente sospettata in esito ad un esame obiettivo di tutte le circostanze pertinenti (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 160 e 161).

86 In una situazione del genere, tenuto conto del necessario contemperamento dei diritti e degli interessi legittimi di cui ai punti da 50 a 53 della presente sentenza, gli Stati membri possono prevedere, in una normativa adottata sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58, la possibilità di ordinare ai fornitori 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 dei quali dispongono (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 163).

87 Dato che la finalità di una siffatta conservazione rapida non corrisponde più a quelle per le quali i dati sono stati raccolti e conservati inizialmente e poiché qualsiasi trattamento di dati deve, ai sensi dell'articolo 8, paragrafo 2, della Carta, rispondere a finalità determinate, gli Stati membri devono precisare, nella loro legislazione, il fine per il quale può aver luogo la conservazione rapida dei dati. Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta che una siffatta conservazione può comportare, solo la lotta alle forme gravi di criminalità e, a fortiori, la salvaguardia della sicurezza nazionale sono idonee a giustificare tale ingerenza, purché tale misura e l'accesso ai dati così conservati rispettino i limiti dello stretto necessario, come indicato ai punti da 164 a 167 della 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).

88 La Corte ha precisato che una misura di conservazione di questo tipo non deve essere limitata ai dati di persone precedentemente identificate come una minaccia per la sicurezza pubblica o la sicurezza nazionale dello Stato membro interessato o delle persone concretamente sospettate di avere commesso un atto grave di criminalità o un attentato alla sicurezza nazionale. Infatti, secondo la Corte, pur rispettando il quadro delineato dall'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, e tenuto conto delle considerazioni esposte al punto 55 della presente sentenza, una misura del genere può, a scelta del legislatore e nel rispetto dei limiti dello stretto necessario, essere estesa ai dati relativi al traffico e ai dati relativi all'ubicazione afferenti a persone diverse da quelle sospettate di avere progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati possano contribuire, sulla base di elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale, quali i dati della vittima o del suo ambiente sociale o professionale (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 165).

89 Pertanto, una misura legislativa può autorizzare il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione, in particolare, delle persone con le quali, anteriormente al verificarsi di una minaccia grave per la sicurezza pubblica o alla commissione di un atto di criminalità grave, una vittima è stata in contatto utilizzando i suoi mezzi di comunicazione elettronica.

90 Una siffatta conservazione rapida può, secondo la giurisprudenza della Corte ricordata al punto 88 della presente sentenza e alle stesse condizioni previste in tale punto, essere estesa anche a zone geografiche determinate, quali i luoghi della commissione e della preparazione del reato o dell'attentato alla sicurezza nazionale di cui trattasi. Occorre precisare che possono essere ancora oggetto di una siffatta misura i dati relativi al traffico e i dati relativi all'ubicazione del luogo in cui una persona, potenzialmente vittima di un atto di criminalità grave, è scomparsa, a condizione che tale misura nonché l'accesso ai dati in tal modo conservati rispettino i limiti dello stretto necessario ai fini della lotta alla criminalità grave o della salvaguardia della sicurezza nazionale, quali enunciati ai punti da 164 a 167 della 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).

91 Inoltre, occorre precisare che l'articolo 15, paragrafo 1, della direttiva 2002/58 non osta a che le autorità nazionali competenti dispongano una misura di conservazione rapida fin dalla prima fase dell'indagine relativa a una minaccia grave per la sicurezza pubblica o a un eventuale atto di criminalità grave, ossia dal momento in cui tali autorità, secondo le pertinenti disposizioni del diritto nazionale, possono avviare una siffatta indagine.

92 Per quanto riguarda la varietà delle misure di conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione di cui al punto 67 della presente sentenza, occorre precisare che tali diverse misure possono, a scelta del legislatore nazionale e nel rispetto dei limiti dello stretto necessario, essere applicate congiuntamente. Ciò premesso, 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, come interpretato dalla giurisprudenza risultante dalla 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), non osta a una combinazione di tali misure.

93 In quarto e ultimo luogo, occorre sottolineare che la proporzionalità delle misure adottate in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58 richiede, secondo la giurisprudenza costante della Corte quale ricapitolata nella 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), il rispetto non solo dei requisiti di idoneità e di necessità, ma anche di quello relativo al carattere proporzionato di tali misure rispetto all'obiettivo perseguito.

94 In tale contesto, occorre ricordare che, al punto 51 della sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238), la Corte ha statuito che, sebbene la lotta contro le forme gravi di criminalità sia di capitale importanza per garantire la sicurezza pubblica e la sua efficacia possa dipendere in larga misura dall'uso delle moderne tecniche di indagine, simile obiettivo di interesse generale, per quanto fondamentale, non può di per sé giustificare il fatto che una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, come quella introdotta dalla direttiva 2006/24, sia considerata necessaria.

95 Nello stesso ordine di idee, la Corte ha precisato, al punto 145 della 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), che anche gli obblighi positivi degli Stati membri che possono derivare, a seconda dei casi, dagli articoli 3, 4 e 7 della Carta e che riguardano, come è stato rilevato al punto 49 della presente sentenza, l'istituzione di norme che consentano una lotta effettiva contro i reati non possono avere l'effetto di giustificare ingerenze tanto gravi quanto quelle che comporta una normativa che prevede una conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta della quasi totalità della popolazione senza che i dati degli interessati siano idonei a rivelare una connessione, almeno indiretta, con l'obiettivo perseguito.

96 All'udienza, il governo danese ha sostenuto che le autorità nazionali competenti dovrebbero poter accedere, ai fini della lotta alla criminalità grave, ai dati relativi al traffico e ai dati relativi all'ubicazione che sono stati conservati in modo generalizzato e indifferenziato, conformemente alla giurisprudenza risultante dalla 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 da 135 a 139), per fronteggiare una grave minaccia per la sicurezza nazionale che si riveli reale e attuale o prevedibile.

97 Occorre anzitutto rilevare che il fatto di autorizzare l'accesso, ai fini della lotta alla criminalità grave, a dati relativi al traffico e a dati relativi all'ubicazione che sono stati conservati in modo generalizzato e indifferenziato farebbe dipendere tale accesso da circostanze estranee a tale obiettivo, a seconda dell'esistenza o meno, nello Stato membro interessato, di una minaccia grave per la sicurezza nazionale, come quella di cui al punto precedente, mentre, alla luce del solo obiettivo di lotta alle forme gravi di criminalità che dovrebbe giustificare la conservazione e l'accesso a tali dati, nulla giustificherebbe una differenza di trattamento, in particolare tra gli Stati membri.

98 Come già dichiarato dalla Corte, 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 la direttiva 2002/58, 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 (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 165 e 166).

99 Orbene, l'argomento del governo danese riguarda una situazione in cui l'obiettivo della domanda di accesso di cui trattasi, vale a dire la lotta alla criminalità grave, è di importanza minore, nella gerarchia degli obiettivi di interesse generale, rispetto a quello che ha giustificato la conservazione, vale a dire la salvaguardia della sicurezza nazionale. Autorizzare, in una situazione del genere, l'accesso ai dati conservati sarebbe contrario a tale gerarchia degli obiettivi di interesse generale richiamata al punto precedente nonché ai punti 53, 56, 57 e 59 della presente sentenza.

100 Inoltre e soprattutto, conformemente alla giurisprudenza ricordata al punto 65 della presente sentenza, i dati relativi al traffico e i dati relativi all'ubicazione non possono essere oggetto di una conservazione generalizzata e indifferenziata ai fini della lotta alla criminalità grave e, pertanto, l'accesso a tali dati non può essere giustificato a questi stessi fini. Orbene, qualora tali dati siano stati eccezionalmente conservati in maniera generalizzata e indifferenziata a fini di salvaguardia della sicurezza nazionale da una minaccia che si riveli reale e attuale o prevedibile, alle condizioni indicate al punto 58 della presente sentenza, le autorità nazionali competenti in materia di indagini penali non possono accedere a detti dati nell'ambito di azioni penali, salvo privare di ogni effetto utile il divieto di procedere a una siffatta conservazione ai fini della lotta alla criminalità grave, richiamato al citato punto 65.

101 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle questioni prima, seconda e quarta 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 misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Il predetto articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta,

non osta, invece, a misure legislative che prevedano, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica,

– la 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;

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

– la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta 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 dispongono tali fornitori di servizi,

se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi.

Sulla terza questione

102 Con la terza 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, 11 e dell'articolo 52, paragrafo l, della Carta, debba essere interpretato nel senso che esso osta a una normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale.

103 In via preliminare, occorre ricordare che, se è vero che spetta al diritto nazionale determinare le condizioni alle quali i fornitori di servizi di comunicazione elettronica devono concedere alle autorità nazionali competenti l'accesso ai dati in loro possesso, la normativa nazionale deve prevedere, per soddisfare il requisito di proporzionalità, come ricordato al punto 54 della presente sentenza, norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e impongano requisiti minimi, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati dai rischi di abuso [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 48 e giurisprudenza citata].

104 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 [sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati delle comunicazioni elettroniche), C-746/18, EU:C:2021:152, paragrafo 49 e giurisprudenza citata].

105 Pertanto, poiché un accesso generale a tutti i dati conservati, indipendentemente da qualsiasi collegamento, almeno indiretto, con la finalità perseguita, non può considerarsi limitato allo stretto necessario, la normativa nazionale interessata 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 di cui trattasi. A questo proposito, un accesso siffatto può, in linea di principio, essere consentito, in relazione all'obiettivo della lotta alla criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un reato 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 può 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 [sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 50 e giurisprudenza citata].

106 Al fine di garantire, nella pratica, il 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 organo amministrativo indipendente e che la decisione di tale giudice o di tale organo intervenga a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di azione penale [sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati delle comunicazioni elettroniche), C-746/18, UE:C:2021:152, paragrafo 51 e giurisprudenza citata].

107 Tale controllo preventivo richiede segnatamente che il giudice o l'organo amministrativo indipendente incaricato di effettuarlo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per assicurare un contemperamento dei vari interessi legittimi e diritti in gioco. Per quanto riguarda, più in particolare, l'indagine penale, simile controllo richiede che tale giudice o tale organo sia in grado di garantire un giusto equilibrio tra, da un lato, gli interessi legittimi relativi 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 del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati delle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 52].

108 Qualora tale controllo venga effettuato non da un giudice, bensì da un organo amministrativo indipendente, quest'ultimo deve godere di uno status che gli 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. Pertanto, il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, così da essere in grado di esercitare tale controllo in modo obiettivo e imparziale, al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale [v. in tal senso, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati delle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punti 53 e 54].

109 In tal senso, la Corte ha considerato, in particolare, che ad un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale non può essere riconosciuto lo status di terzo rispetto agli interessi legittimi in gioco, dal momento che esso ha il compito non di dirimere in piena indipendenza una controversia, bensì di sottoporla, se del caso, al giudice competente, in quanto parte nel processo che esercita l'azione penale. Ne consegue che un simile pubblico ministero non è in grado di effettuare il controllo preventivo delle domande di accesso ai

dati conservati [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 55 e 57].

110 Infine, il controllo indipendente richiesto ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 deve intervenire prima di qualsiasi accesso ai dati interessati, salvo in caso di urgenza debitamente giustificata, nel qual caso il controllo deve avvenire in tempi brevi. Infatti, un controllo successivo non consentirebbe di rispondere all'obiettivo del controllo preventivo, che consiste nell'impedire che venga autorizzato un accesso ai dati in questione eccedente i limiti dello stretto necessario [v., in tal senso, sentenze 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, nonché del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 58].

111 Nel caso di specie, risulta anzitutto dalla domanda di pronuncia pregiudiziale che la legge del 2011 attribuisce a un funzionario di polizia, il cui rango non sia inferiore a quello di sovrintendente capo, la competenza ad esercitare il controllo preventivo delle domande di accesso ai dati provenienti dai servizi di indagine di polizia e a chiedere ai fornitori di servizi di comunicazione elettronica di fornirgli i dati che essi conservano. Poiché tale funzionario non riveste la qualità di terzo rispetto a tali servizi, egli non soddisfa i requisiti di indipendenza e di imparzialità ricordati al punto 108 della presente sentenza, nonostante sia assistito in tale missione da un'unità della polizia, nella fattispecie la TLU, che gode di una certa autonomia nell'esercizio della sua missione.

112 Se è vero, poi, che la legge del 2011 prevede meccanismi di controllo a posteriori della decisione del funzionario di polizia competente sotto forma di un procedimento di reclamo e di un procedimento dinanzi a un giudice incaricato di verificare l'applicazione delle disposizioni di detta legge, dalla giurisprudenza richiamata al punto 110 della presente sentenza risulta che un controllo esercitato a posteriori non può sostituirsi all'esigenza, ricordata al punto 106 della presente sentenza, di un controllo indipendente e, salvo casi di urgenza debitamente giustificata, preventivo.

113 Infine, la legge del 2011 non prevede criteri oggettivi che definiscano con precisione le condizioni e le circostanze in cui deve essere concesso alle autorità nazionali l'accesso ai dati, dato che il funzionario di polizia incaricato del trattamento delle domande di accesso ai dati conservati è il solo competente, come confermato dall'Irlanda in udienza, a valutare i sospetti gravanti sulle persone interessate e la necessità di un accesso ai dati relativi a queste ultime.

114 Di conseguenza, occorre rispondere alla terza questione dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e dell'articolo 52, paragrafo l, della Carta, deve essere interpretato nel senso che esso osta a una normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale.

Sulla quinta e la sesta questione

115 Con le questioni quinta e sesta, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se il diritto dell'Unione debba essere interpretato nel senso che un giudice nazionale può limitare nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta.

116 Dalle informazioni fornite dal giudice del rinvio risulta che la normativa nazionale controversa nel procedimento principale, ossia la legge del 2011, è stata adottata al fine di recepire nel diritto nazionale la direttiva 2006/24, che è stata poi dichiarata invalida dalla Corte nella sua sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238).

117 Inoltre, il giudice del rinvio rileva che, anche se l'esame della ricevibilità degli elementi di prova fondati su dati conservati in forza della legge del 2011 e invocati nei confronti di G.D. nell'ambito del procedimento penale è di competenza del giudice penale, spetta tuttavia al giudice del rinvio stesso, nell'ambito del procedimento civile, statuire sulla validità delle disposizioni controverse di tale legge e sugli effetti nel tempo di una loro dichiarazione di invalidità. Pertanto, sebbene l'unica questione che si pone dinanzi al giudice del rinvio sia quella della validità delle disposizioni della legge del 2011, detto giudice ritiene tuttavia necessario interrogare la Corte in merito all'incidenza di un'eventuale declaratoria di invalidità sull'ammissibilità degli elementi di prova ottenuti mediante la conservazione generalizzata e indifferenziata dei dati che tale legge ha consentito.

118 In via preliminare, occorre ricordare che il principio del primato del diritto dell'Unione sancisce la preminenza del diritto dell'Unione sul diritto degli Stati membri. Tale principio impone pertanto a tutte le istituzioni degli Stati membri di dare pieno effetto alle varie disposizioni del diritto dell'Unione, dato che il diritto degli Stati membri non può sminuire l'efficacia riconosciuta a tali disposizioni nel territorio dei suddetti Stati. In forza di tale principio, ove non sia possibile procedere a un'interpretazione della normativa nazionale conforme alle prescrizioni del diritto dell'Unione, il giudice nazionale incaricato di applicare, nell'ambito della propria competenza, le disposizioni di diritto dell'Unione ha l'obbligo di garantire la piena efficacia delle medesime, disapplicando all'occorrenza, di propria iniziativa, qualsiasi disposizione contrastante della legislazione nazionale, anche posteriore, senza doverne chiedere o attendere la previa rimozione in via legislativa o mediante qualsiasi altro procedimento costituzionale. [v., n tal senso, sentenze del 15 luglio 1964, Costa, 6/64, EU:C:1964:66, pagg. 1159 e 1160; del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema), C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punti 157, 158 e 160, 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, punti 214 e 215].

119 Solo la Corte può, eccezionalmente e per considerazioni imperative di certezza del diritto, concedere una sospensione provvisoria dell'effetto di disapplicazione esercitato da una norma di diritto dell'Unione rispetto a norme di diritto interno con essa in contrasto. Una siffatta limitazione nel tempo degli effetti dell'interpretazione data dalla Corte a tale diritto può essere concessa solo nella stessa sentenza che statuisce sull'interpretazione richiesta. Il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali, anche solo provvisoriamente, il primato rispetto al diritto dell'Unione al quale esse contravvengono (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 216 e 217 e giurisprudenza citata).

120 Vero è che la Corte ha considerato, in una causa riguardante la legittimità di misure adottate in violazione dell'obbligo sancito dal diritto dell'Unione di effettuare una valutazione preliminare dell'impatto di un progetto sull'ambiente e su un sito protetto, che un giudice nazionale può, se il diritto interno lo consente, eccezionalmente mantenere gli effetti di siffatte misure qualora tale mantenimento sia giustificato da considerazioni imperative connesse alla necessità di scongiurare una minaccia grave ed effettiva di interruzione dell'approvvigionamento di energia elettrica dello Stato membro interessato, cui non si potrebbe far fronte mediante altri mezzi e alternative, in

particolare nell'ambito del mercato interno, ma detto mantenimento può coprire soltanto il lasso di tempo strettamente necessario per porre rimedio a tale illegittimità (v., in tal senso, sentenza del 29 luglio 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punti 175, 176, 179 e 181).

121 Tuttavia, a differenza dell'omissione di un obbligo procedurale quale la valutazione preliminare dell'impatto di un progetto che s'inserisce nell'ambito specifico della tutela dell'ambiente, la violazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, non può essere oggetto di regolarizzazione mediante una procedura analoga a quella menzionata al punto precedente (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 219).

122 Infatti, il mantenimento degli effetti di una normativa nazionale come la legge del 2011 implicherebbe che detta normativa continui ad imporre ai fornitori di servizi di comunicazione elettronica obblighi che risultano contrari al diritto dell'Unione e comportano ingerenze gravi nei diritti fondamentali delle persone i cui dati sono stati conservati (v., per analogia, 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 219).

123 Pertanto, il giudice del rinvio non può limitare nel tempo gli effetti di una declaratoria di illegittimità ad esso spettante, in forza del diritto nazionale, della legislazione nazionale di cui trattasi nel procedimento principale (v., per analogia, 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 220).

124 A tal riguardo, come rilevato, in sostanza, dall'avvocato generale al paragrafo 75 delle sue conclusioni, la circostanza che tale normativa nazionale sia stata adottata al fine di recepire la direttiva 2006/24 nel diritto nazionale è irrilevante dal momento che, per effetto dell'invalidazione di tale direttiva da parte della Corte, invalidazione i cui effetti retroagiscono alla data della sua entrata in vigore (v., in tal senso, sentenza dell'8 febbraio 1996, FMC e a., C-212/94, EU:C:1996:40, punto 55), la validità di tale normativa nazionale deve essere valutata dal giudice del rinvio alla luce della direttiva 2002/58 e della Carta, quali interpretate dalla Corte.

125 Per quanto riguarda, in particolare, l'interpretazione della direttiva 2002/58 e della Carta accolta dalla Corte segnatamente nelle sue sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), e del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), occorre ricordare che, secondo giurisprudenza costante, l'interpretazione che la Corte dà di una norma di diritto dell'Unione, nell'esercizio della competenza attribuitale dall'articolo 267 TFUE, chiarisce e precisa il significato e la portata di tale norma, come deve o avrebbe dovuto essere intesa ed applicata dal momento della sua entrata in vigore. Ne deriva che la norma così interpretata può e deve essere applicata dal giudice anche a rapporti giuridici sorti e costituiti prima della pronuncia della sentenza che statuisce sulla domanda di interpretazione, purché sussistano, inoltre, i presupposti per sottoporre al giudice competente una controversia relativa all'applicazione di detta norma (sentenza del 16 settembre 2020, Romenergo e Aris Capital, C-339/19, EU:C:2020:709, punto 47 e giurisprudenza citata).

126 A tal riguardo, occorre anche precisare che nelle sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), e del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791) non è stata operata una limitazione nel tempo degli effetti dell'interpretazione adottata, cosicché, conformemente alla giurisprudenza richiamata al punto 119 della presente sentenza, essa non può intervenire in una sentenza della Corte ad esse successiva.

127 Infine, per quanto riguarda l'impatto della dichiarazione dell'eventuale incompatibilità della legge del 2011 con la direttiva 2002/58, letta alla luce della Carta, sull'ammissibilità delle prove dedotte contro G.D. nell'ambito del procedimento penale, è sufficiente fare riferimento alla pertinente giurisprudenza della Corte, in particolare ai principi richiamati ai punti da 41 a 44 della sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), (C-746/18, EU:C:2021:152), da cui discende che, conformemente al principio dell'autonomia procedurale degli Stati membri, tale ammissibilità rientra nel diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

128 Alla luce delle considerazioni che precedono, occorre rispondere alle questioni quinta e sesta dichiarando che il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta. L'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

Sulle spese

129 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 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta a misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Il predetto articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, non osta, invece, a misure legislative che prevedano, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica,

– la 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;

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

– la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta 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 dispongono tali fornitori di servizi,
se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi.

2) L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificato dalla direttiva 2009/136, letto alla luce degli articoli 7, 8, 11 e dell'articolo 52, paragrafo l, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta a una normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale.

3) Il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce della Carta dei diritti fondamentali. L'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

Firme