Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

20 settembre 2022 *

[Testo rettificato con ordinanza del 27 ottobre 2022]

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Riservatezza delle comunicazioni – Fornitori di servizi di comunicazione elettronica – Conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 6, 7, 8 e 11 nonché articolo 52, paragrafo 1 – Articolo 4, paragrafo 2, TUE»

Nelle cause riunite C-793/19 e C-794/19,

aventi ad oggetto le domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 TFUE, dal Bundesverwaltungsgericht (Corte amministrativa federale, Germania), con decisioni del 25 settembre 2019, pervenute in cancelleria il 29 ottobre 2019, nei procedimenti

Bundesrepublik Deutschland, rappresentata dalla Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

contro

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis e I. Ziemele, presidenti di sezione, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (relatore), 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,

* Lingua processuale: il tedesco.

considerate le osservazioni presentate:

– per la Bundesrepublik Deutschland, rappresentata dalla Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, da C. Mögelin, in qualità di agente;

– [Come rettificato con ordinanza del 27 ottobre 2022] per la SpaceNet AG, da M. Bäcker, Universitätsprofessor;

– per la Telekom Deutschland GmbH, da T. Mayen, Rechtsanwalt;

– per il governo tedesco, da J. Möller, F. Halibi, M. Hellmann, D. Klebs ed E. Lankenau, in qualità di agenti;

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

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

– per l'Irlanda, da A. Joyce e J. Quaney, in qualità di agenti, assistiti da D. Fennelly, BL, e P. Gallagher, SC;

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

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

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

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

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

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

– per il governo svedese, da H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson e H. Shev, in qualità di agenti;

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

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

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

ha pronunciato la seguente

Sentenza

1 Le domande di pronuncia pregiudiziale vertono 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 da 6 a 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») e dell'articolo 4, paragrafo 2, TUE.

2 Tali domande sono state presentate nell'ambito di controversie tra, da un lato, la Bundesrepublik Deutschland (Repubblica federale di Germania), rappresentata dalla Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agenzia federale delle reti per l'energia elettrica, il gas, le telecomunicazioni, la posta e le ferrovie, Germania), e, dall'altro, la SpaceNet AG (causa C-793/19) e la Telekom Deutschland GmbH (causa C-794/19), in merito all'obbligo imposto a queste ultime di conservare dati relativi al traffico e dati relativi all'ubicazione attinenti alle telecomunicazioni dei loro clienti.

Contesto normativo

Diritto dell'Unione

Direttiva 95/46/CE

3 La 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), è stata abrogata, con decorrenza dal 25 maggio 2018, dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1).

4 L'articolo 3, paragrafo 2, della direttiva 95/46 così disponeva:

«Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali:

– effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

– effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

Direttiva 2002/58

5 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 tale Carta.

(...)

(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], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza, la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, [firmata a Roma il 4 novembre 1950] come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali».

6 L'articolo 1 di tale direttiva, intitolato «Finalità e campo d'applicazione», così dispone:

«1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

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 UE] 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».

7 Ai sensi dell'articolo 2 della direttiva in questione, 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 sul 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;

(...)».

8 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 nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

9 Ai sensi dell'articolo 5 della stessa 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».

10 L'articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», stabilisce 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.

(...)».

11 L'articolo 9 di tale direttiva, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», al paragrafo 1 prevede 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. (...)».

12 L'articolo 15 della direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», al paragrafo 1 così recita:

«Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE]».

Diritto tedesco

Il TKG

13 L'articolo 113a, paragrafo 1, prima frase, del Telekommunikationsgesetz (legge in materia di telecomunicazioni), del 22 giugno 2004 (BGBl. 2004 I, pag. 1190), nella versione applicabile alle controversie principali (in prosieguo: il «TKG»), è del seguente tenore:

«Gli obblighi concernenti la conservazione, l'utilizzo e la sicurezza dei dati relativi al traffico definiti negli articoli da 113b a 113g riguardano gli operatori che forniscono agli utenti finali servizi di telecomunicazione accessibili al pubblico».

14 In forza dell'articolo 113b del TKG:

«(1) Gli operatori di cui all'articolo 113a, paragrafo 1, devono conservare i dati nel territorio nazionale nel modo seguente:

1. per dieci settimane nel caso dei dati di cui ai paragrafi 2 e 3,

2. per quattro settimane nel caso dei dati relativi all'ubicazione di cui al paragrafo 4.

(2) I fornitori di servizi di telefonia accessibili al pubblico conservano:

1. il numero di telefono o altro identificativo della linea chiamante e della linea chiamata, nonché di ogni altra linea utilizzata in caso di commutazione o trasferimento di chiamata,

2. la data e l'ora di inizio e fine del collegamento con indicazione del relativo fuso orario,

3. le indicazioni del servizio utilizzato, qualora possano essere utilizzati diversi servizi nell'ambito della telefonia,

4. nel caso della telefonia mobile, inoltre
   a) l'identificativo internazionale degli abbonati alla telefonia mobile per la linea chiamante e la linea chiamata,
   b) l'identificativo internazionale dell'apparecchiatura terminale chiamante e chiamata,
   c) la data e l'ora della prima attivazione del servizio con indicazione del relativo fuso orario, in caso di servizi prepagati,

5. nel caso di telefonia via Internet, anche gli indirizzi IP (protocollo Internet) della linea chiamante e della linea chiamata e gli identificativi di utente attribuiti.

Il primo comma si applica, mutatis mutandis,

1. in caso di comunicazione per SMS, messaggio multimediale o simile; in tal caso, le indicazioni di cui al primo comma, punto 2, sono sostituite dall'ora di invio e di ricezione del messaggio;

2. alle chiamate senza risposta o non riuscite per un intervento dell'operatore di rete (...).

(3) I fornitori di servizi di accesso a Internet accessibili al pubblico conservano

1. l'indirizzo IP assegnato all'abbonato ai fini dell'uso di Internet,

2. l'identificativo univoco della linea attraverso la quale ha luogo l'uso di Internet, nonché l'identificativo di utente attribuito,

3. la data e l'ora di inizio e fine dell'uso di Internet dall'indirizzo IP assegnato, con indicazione del relativo fuso orario.

(4) In caso di utilizzo di servizi di telefonia mobile deve essere conservata l'indicazione delle celle telefoniche utilizzate all'inizio del collegamento da chi effettua la chiamata e da chi la riceve. Per quanto riguarda i servizi di accesso a Internet accessibili al pubblico, deve essere conservata, in caso di uso mobile, l'indicazione delle celle telefoniche utilizzate all'inizio della connessione a Internet. Devono inoltre essere conservati i dati che permettano di conoscere la posizione geografica e le direzioni di radiazione massima delle antenne che servono la cella telefonica in questione.

(5) Non possono essere conservati ai sensi della presente disposizione il contenuto della comunicazione, i dati relativi ai siti Internet consultati e i dati dei servizi di posta elettronica.

(6) Non possono essere conservati ai sensi della presente disposizione i dati alla base delle comunicazioni di cui all'articolo 99, paragrafo 2. Ciò vale, mutatis mutandis, per le

comunicazioni telefoniche provenienti dagli enti di cui all'articolo 99, paragrafo 2. Si applica, mutatis mutandis, l'articolo 99, paragrafo 2, frasi dalla seconda alla settima.

(...)».

15 Le comunicazioni di cui all'articolo 99, paragrafo 2, del TKG, cui l'articolo 113b, paragrafo 6, del TKG rinvia, sono comunicazioni con persone, autorità e organizzazioni di carattere sociale o religioso, che propongono unicamente o essenzialmente a chiamanti, che restano in linea di principio anonimi, servizi di assistenza telefonica in casi di situazione d'urgenza psicologica o sociale e che sono soggette a loro volta, o i cui collaboratori sono soggetti, a particolari obblighi di riservatezza al riguardo. La deroga prevista all'articolo 99, paragrafo 2, frasi seconda e quarta, del TKG è subordinata all'iscrizione dei chiamati, su loro richiesta, in un elenco redatto dall'Agenzia federale delle reti per l'energia elettrica, il gas, le telecomunicazioni, la posta e le ferrovie, dopo che i titolari dei numeri di telefono hanno comprovato la loro attività producendo l'attestazione di un'autorità, di un organismo, di un ente o di una fondazione di diritto pubblico.

16 Ai sensi dell'articolo 113c, paragrafi 1 e 2, del TKG:

«(1) I dati conservati a norma dell'articolo 113b possono

1. essere trasmessi a un'autorità di polizia quando questa ne richieda la trasmissione in forza di una disposizione di legge che la autorizzi a raccogliere i dati di cui all'articolo 113b ai fini della repressione di reati di particolare gravità;

2. essere trasmessi a un'autorità di polizia dei Land quando questa ne richieda la trasmissione in forza di una disposizione di legge che autorizzi la raccolta dei dati di cui all'articolo 113b a fini di prevenzione di un rischio concreto per l'integrità fisica, la vita o la libertà di una persona o per l'esistenza dello Stato federale o di un Land;

(...)

(2) I dati conservati a norma dell'articolo 113b non possono essere utilizzati da persone soggette agli obblighi stabiliti all'articolo 113a, paragrafo 1, per finalità diverse da quelle previste al paragrafo 1».

17 L'articolo 113d del TKG così recita:

«La persona soggetta all'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che i dati conservati conformemente all'articolo 113b, paragrafo 1, in base all'obbligo di conservazione siano protetti, con misure tecniche e organizzative conformi allo stato della tecnica, da controlli e usi non autorizzati. Tali misure comprendono in particolare:

1. l'utilizzo di una procedura di crittografia particolarmente sicura,

2. l'archiviazione in infrastrutture di archiviazione distinte, separate da quelle destinate alle normali funzioni operative,

3. l'archiviazione, con un livello elevato di protezione contro gli attacchi informatici, in sistemi informatici scollegati di trattamento dei dati,

4. la limitazione dell'accesso agli impianti utilizzati per il trattamento dei dati alle persone in possesso di un'autorizzazione speciale rilasciata dalla persona soggetta all'obbligo e

5. l'obbligo di far intervenire, durante l'accesso ai dati, almeno due persone in possesso di un'autorizzazione speciale rilasciata dalla persona soggetta all'obbligo».

18 L'articolo 113e del TKG è così formulato:

«(1) La persona soggetta all'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che, ai fini del controllo della protezione dei dati, sia registrato, in virtù dell'obbligo di conservazione, ogni accesso, e in particolare la lettura, la copiatura, la modifica, la cancellazione e il blocco, ai dati conservati conformemente all'articolo 113b, paragrafo 1. Devono essere registrati

1. l'ora dell'accesso,

2. le persone che accedono ai dati,

3. lo scopo e la natura dell'accesso.

(2) I dati registrati non possono essere utilizzati per finalità diverse dal controllo della protezione dei dati.

(3) La persona soggetta all'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che i dati registrati siano cancellati dopo un anno».

19 Al fine di garantire un livello di sicurezza e di qualità dei dati particolarmente elevato, l'Agenzia federale delle reti per l'energia elettrica, il gas, le telecomunicazioni, la posta e le ferrovie stabilisce, conformemente all'articolo 113f, paragrafo 1, del TKG, un insieme di requisiti che, in forza dell'articolo 113 f, paragrafo 2, dello stesso, deve essere costantemente valutato e all'occorrenza adeguato. L'articolo 113g del TKG impone che siano integrate misure di sicurezza specifiche nella relazione sulla politica in materia di sicurezza che deve essere presentata dalla persona soggetta all'obbligo.

La StPO

20 L'articolo 100 g, paragrafo 2, prima frase, della Strafprozessordnung (codice di procedura penale; in prosieguo: la «StPO») è del seguente tenore:

«Qualora determinate circostanze inducano a sospettare che una persona abbia commesso, come autore o complice, uno dei reati particolarmente gravi di cui alla seconda frase o, nei casi in cui sia punibile il tentativo di reato, abbia tentato di commetterlo e se il reato è particolarmente grave anche nel singolo caso, i dati relativi al traffico, conservati conformemente all'articolo 113b del [TKG], possono essere raccolti laddove l'indagine sui fatti o la localizzazione della persona indagata sarebbero eccessivamente difficili o impossibili con altri mezzi e la raccolta dei dati sia proporzionata all'importanza del caso».

21 L'articolo 101a, paragrafo 1, della StPO sottopone a un'autorizzazione giudiziaria la raccolta di dati relativi al traffico ai sensi dell'articolo 100g della medesima. In forza dell'articolo 101a, paragrafo 2, della StPO, la motivazione della decisione deve contenere le considerazioni

essenziali relative alla necessità e all'adeguatezza della misura nel caso specifico in questione. L'articolo 101a, paragrafo 6, della StPO prevede l'obbligo di informare i partecipanti alla telecomunicazione di cui trattasi.

Procedimenti principali e questione pregiudiziale

22 La SpaceNet e la Telekom Deutschland forniscono, in Germania, servizi di accesso a Internet accessibili al pubblico. La seconda fornisce, inoltre, sempre in Germania, servizi di telefonia accessibili al pubblico.

23 Tali fornitori di servizi hanno contestato dinanzi al Verwaltungsgericht Köln (Tribunale amministrativo di Colonia, Germania) l'obbligo ad essi prescritto dal combinato disposto dell'articolo 113a, paragrafo 1, e dell'articolo 113b del TKG di conservare dati relativi al traffico e dati relativi all'ubicazione attinenti alle telecomunicazioni dei loro clienti a decorrere dal 1º luglio 2017.

24 Con sentenze del 20 aprile 2018 il Verwaltungsgericht Köln (Tribunale amministrativo di Colonia) ha dichiarato che la SpaceNet e la Telekom Deutschland non erano tenute a conservare i dati relativi al traffico attinenti alle telecomunicazioni, di cui all'articolo 113b, paragrafo 3, del TKG, dei clienti ai quali esse forniscono un accesso a Internet e che la Telekom Deutschland non era, inoltre, tenuta a conservare i dati relativi al traffico attinenti alle telecomunicazioni, di cui all'articolo 113b, paragrafo 2, frasi prima e seconda, del TKG, dei clienti ai quali essa fornisce un accesso a servizi di telefonia accessibili al pubblico. Tale giudice ha infatti ritenuto, alla luce della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), che tale obbligo di conservazione fosse contrario al diritto dell'Unione.

25 Avverso tali sentenze la Repubblica federale di Germania ha proposto ricorsi per cassazione (*Revision*) dinanzi al Bundesverwaltungsgericht (Corte amministrativa federale, Germania), giudice del rinvio.

26 Quest'ultimo ritiene che stabilire se l'obbligo di conservazione prescritto dal combinato disposto dell'articolo 113a, paragrafo 1, e dell'articolo 113b del TKG sia contrario al diritto dell'Unione dipenda dall'interpretazione della direttiva 2002/58.

27 A tale riguardo, il giudice del rinvio rileva che la Corte ha già statuito in modo definitivo, nella sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15), che normative vertenti sulla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nonché sull'accesso a tali dati da parte delle autorità nazionali rientrano, in linea di principio, nell'ambito di applicazione della direttiva 2002/58.

28 Esso rileva altresì che l'obbligo di conservazione di cui ai procedimenti principali, in quanto limita i diritti derivanti dall'articolo 5, paragrafo 1, dall'articolo 6, paragrafo 1, e dall'articolo 9, paragrafo 1, della direttiva 2002/58, potrebbe essere giustificato solo sulla base dell'articolo 15, paragrafo 1, di tale direttiva.

29 A tale riguardo, esso ricorda che dalla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), risulta 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 una normativa nazionale la quale preveda, per

finalità di lotta contro la criminalità, una conservazione generalizzata e indiscriminata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica.

30 Orbene, secondo il giudice del rinvio, al pari delle normative nazionali in questione nelle cause che hanno dato origine alla sentenza succitata, la normativa nazionale oggetto dei procedimenti principali non richiede alcuna motivazione per la conservazione dei dati né un qualsivoglia collegamento tra i dati conservati e un reato o un rischio per la pubblica sicurezza. Tale normativa nazionale imporrebbe infatti la conservazione, senza alcuna motivazione, generalizzata e indiscriminata da un punto di vista personale, temporale e geografico, di gran parte dei dati relativi al traffico attinenti alle telecomunicazioni.

31 Il giudice del rinvio ritiene, tuttavia, che non sia escluso che l'obbligo di conservazione di cui ai procedimenti principali possa essere giustificato in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58.

32 In primo luogo, esso rileva che, contrariamente alle normative nazionali oggetto delle cause che hanno dato origine alla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), la normativa nazionale oggetto dei procedimenti principali non richiede la conservazione dell'insieme dei dati relativi al traffico attinenti alle telecomunicazioni di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica. Non solo sarebbe escluso dall'obbligo di conservazione il contenuto delle comunicazioni, ma anche i dati relativi ai siti Internet consultati, i dati dei servizi di posta elettronica e i dati inerenti alle comunicazioni a carattere sociale o religioso da o verso talune linee non potrebbero essere conservati, come risulta dall'articolo 113b, paragrafi 5 e 6, del TKG.

33 In secondo luogo, tale giudice riferisce che l'articolo 113b, paragrafo 1, del TKG prevede un periodo di conservazione di quattro settimane per i dati relativi all'ubicazione e di dieci settimane per i dati relativi al traffico, mentre 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), sulla quale erano basate le normative nazionali oggetto delle cause che hanno dato origine alla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), prevedeva un periodo di conservazione compreso tra i sei mesi e i due anni.

34 Orbene, secondo il giudice del rinvio, sebbene l'esclusione di determinati mezzi di comunicazione o di determinate categorie di dati e la limitazione del periodo di conservazione non siano sufficienti a eliminare qualsiasi rischio che venga tracciato un profilo completo degli interessati, tale rischio sarebbe quantomeno considerevolmente ridotto nell'ambito dell'attuazione della normativa nazionale di cui ai procedimenti principali.

35 In terzo luogo, tale normativa prevederebbe rigide limitazioni per quanto riguarda la protezione dei dati conservati e l'accesso agli stessi. Infatti, da un lato, essa garantirebbe una protezione efficace dei dati conservati dai rischi di abuso nonché da qualsiasi accesso illecito ai medesimi. Dall'altro, i dati conservati potrebbero essere utilizzati solo per finalità di contrasto dei reati gravi o di prevenzione di un rischio concreto per l'integrità fisica, la vita o la libertà di una persona oppure per l'esistenza dello Stato federale o di un Land.

36 In quarto luogo, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 nel senso di un'incompatibilità generale con il diritto dell'Unione di qualsiasi conservazione di dati che sia priva di motivazione potrebbe scontrarsi con l'obbligo di agire degli Stati membri, derivante dal diritto alla sicurezza sancito dall'articolo 6 della Carta.

37 In quinto luogo, il giudice del rinvio ritiene che un'interpretazione dell'articolo 15 della direttiva 2002/58 che precluda la conservazione generalizzata dei dati limiterebbe considerevolmente il margine di manovra del legislatore nazionale in un settore che interessa la repressione dei reati e la pubblica sicurezza, il quale resterebbe, conformemente all'articolo 4, paragrafo 2, TUE, di esclusiva competenza di ciascuno Stato membro.

38 In sesto luogo, il giudice del rinvio ritiene che si debba tener conto della giurisprudenza della Corte europea dei diritti dell'uomo e rileva che questa ha dichiarato che l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU») non osta a disposizioni nazionali che prevedano l'intercettazione massiccia dei flussi oltre frontiera di dati, in considerazione delle minacce cui attualmente fanno fronte numerosi Stati e degli strumenti tecnologici sui quali possono ormai contare i terroristi e i criminali per commettere atti perseguibili.

39 Ciò considerato, il Bundesverwaltungsgericht (Corte amministrativa federale) ha deciso di sospendere i procedimenti e di sottoporre alla Corte la seguente questione pregiudiziale:

«Se l'articolo 15 della direttiva [2002/58], alla luce degli articoli 7, 8 e 11, nonché 52, paragrafo 1, della [Carta], da un lato, e dell'articolo 6 della Carta medesima, nonché dell'articolo 4 [TUE], dall'altro, debba essere interpretato nel senso che esso osti ad una normativa nazionale, la quale obblighi i fornitori di servizi di comunicazione elettronica accessibili al pubblico a conservare i dati relativi al traffico e all'ubicazione degli utenti finali di detti servizi, laddove

1) tale obbligo non presupponga alcun motivo specifico di ordine locale, temporale o geografico,

2) costituiscano oggetto dell'obbligo di archiviazione, nella fornitura di servizi telefonici accessibili al pubblico – inclusa la trasmissione di messaggi di testo (SMS), multimediali (MMS) o simili, nonché le chiamate senza risposta oppure non riuscite – i seguenti dati:
   a) il numero di telefono o altro identificativo della linea chiamante e della linea chiamata, nonché di ogni altra linea utilizzata in caso di commutazione o trasferimento di chiamata,
   b) la data e l'ora di inizio e fine del collegamento o – nel caso di trasmissione di un messaggio di testo (SMS), multimediale (MMS) o simile – il momento della spedizione e della ricezione del messaggio con indicazione del relativo fuso orario,
   c) indicazione del servizio utilizzato, qualora possano essere utilizzati diversi servizi nell'ambito della telefonia,
   d) nel caso della telefonia mobile, inoltre
      i) l'identificativo internazionale degli abbonati alla telefonia mobile per la linea chiamante e la linea chiamata,
      ii) l'identificativo internazionale dell'apparecchiatura terminale chiamante e chiamata,
      iii) data e ora della prima attivazione del servizio con indicazione del relativo fuso orario, in caso di servizi prepagati,
      iv) l'indicazione delle celle telefoniche utilizzate dalla linea chiamante e dalla linea chiamata all'inizio del collegamento,
   e) nel caso di telefonia via Internet, anche gli indirizzi di protocollo Internet della linea chiamante e della linea chiamata e gli identificativi di utente attribuiti,

3) costituiscano oggetto dell'obbligo di archiviazione, nella fornitura di servizi di accesso a Internet accessibili al pubblico, i seguenti dati:
   a) l'indirizzo di protocollo Internet assegnato all'abbonato ai fini dell'uso di Internet,
   b) l'identificativo univoco della linea attraverso la quale ha luogo l'uso di Internet, nonché l'identificativo di utente attribuito,
   c) data e ora di inizio e fine dell'uso di Internet con l'indirizzo di protocollo Internet assegnato con indicazione del relativo fuso orario,
   d) in caso di uso mobile, l'indicazione della cella telefonica utilizzata all'inizio del collegamento a Internet,

4) i seguenti dati non possano essere memorizzati:
   a) il contenuto della comunicazione,
   b) dati relativi alla pagina Internet visitata,
   c) dati dei servizi di posta elettronica,
   d) dati relativi ai collegamenti in uscita o in entrata da determinate linee di persone, autorità e organizzazioni in ambito sociale o religioso,

5) la durata della conservazione di dati relativi all'ubicazione, vale a dire l'indicazione della cella telefonica utilizzata, sia pari a quattro settimane e, per gli altri dati, a dieci settimane,

6) sia assicurata un'efficace protezione dei dati conservati contro i rischi di abuso e di accesso non autorizzato, e

7) i dati conservati possano essere utilizzati solo ai fini del perseguimento di reati particolarmente gravi o della prevenzione di un pericolo concreto per la vita, l'integrità fisica o la libertà di una persona ovvero ai fini della salvaguardia dello Stato o di un Land, ad eccezione degli indirizzi di protocollo Internet assegnati all'abbonato per l'uso di Internet, il cui utilizzo sia consentito nell'ambito di un accesso ai dati archiviati finalizzato al perseguimento di eventuali reati, al mantenimento dell'ordine e della sicurezza pubblici, nonché all'assolvimento dei compiti dei servizi di informazione».

Procedimento dinanzi alla Corte

40 Con decisione del presidente della Corte del 3 dicembre 2019, le cause C-793/19 e C-794/19 sono state riunite ai fini delle fasi scritta e orale del procedimento nonché della sentenza.

41 Con decisione del presidente della Corte del 14 luglio 2020, il procedimento nelle cause riunite C-793/19 e C-794/19 è stato sospeso a norma dell'articolo 55, paragrafo 1, lettera b), del regolamento di procedura della Corte, fino alla pronuncia della sentenza nella causa La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18).

42 Avendo la Corte pronunciato, il 6 ottobre 2020, la sua sentenza nella causa La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), il presidente della Corte ha disposto, l' 8 ottobre 2020, la riassunzione del procedimento nelle cause riunite C-793/19 e C-794/19.

43 Il giudice del rinvio, al quale la cancelleria aveva comunicato tale sentenza, ha dichiarato di confermare la propria domanda di pronuncia pregiudiziale.

44 A tale riguardo, detto giudice del rinvio ha, anzitutto, osservato che l'obbligo di conservazione previsto dalla normativa di cui ai procedimenti principali riguarda un numero di dati inferiore e un periodo di conservazione meno lungo rispetto a quanto prevedevano le normative nazionali, oggetto delle cause che hanno dato origine alla 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). Tali particolari circostanze ridurrebbero la probabilità che i dati conservati possano consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati.

45 Esso ha poi ribadito che la normativa nazionale di cui ai procedimenti principali garantisce una protezione efficace dei dati conservati dai rischi di abuso e di accesso illecito.

46 Infine, esso ha sottolineato che sussistono incertezze quanto alla questione della compatibilità con il diritto dell'Unione della conservazione degli indirizzi IP, prevista dalla normativa nazionale di cui ai procedimenti principali, per via di un'incoerenza tra i punti 155 e 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). In tal senso, secondo il giudice del rinvio, tale sentenza non chiarirebbe se la Corte richieda, per la conservazione degli indirizzi IP, una motivazione per la conservazione connessa all'obiettivo di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità o di prevenzione delle minacce gravi alla pubblica sicurezza, come risulterebbe dal punto 168 della sentenza succitata, oppure se la conservazione degli indirizzi IP sia consentita anche in assenza di una motivazione concreta, atteso che solo l'utilizzazione dei dati conservati è limitata da detti obiettivi, come risulterebbe dal punto 155 della stessa sentenza.

Sulla questione pregiudiziale

47 Con la sua questione pregiudiziale, il giudice del rinvio chiede, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli da 6 a 8 e 11 nonché dell'articolo 52, paragrafo l, della Carta e dell'articolo 4, paragrafo 2, TUE, debba essere interpretato nel senso che esso osta a una misura legislativa nazionale che, salvo talune eccezioni, impone ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ai fini elencati all'articolo 15, paragrafo 1, di tale direttiva, e in particolare ai fini del perseguimento dei reati gravi o della prevenzione di un rischio concreto per la sicurezza nazionale, la conservazione generalizzata e indiscriminata di gran parte dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti finali di tali servizi, prevedendo un periodo di conservazione di varie settimane nonché norme volte a garantire un'efficace protezione dei dati conservati dai rischi di abuso e da qualsiasi accesso illecito a tali dati.

Sull'applicabilità della direttiva 2002/58

48 Per quanto riguarda l'argomentazione dell'Irlanda nonché dei governi francese, dei Paesi Bassi, polacco e svedese secondo cui la normativa nazionale di cui ai procedimenti principali, in quanto adottata segnatamente ai fini della salvaguardia della sicurezza nazionale, non rientrerebbe nell'ambito di applicazione della direttiva 2002/58, è sufficiente ricordare che una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di conservare dati relativi al traffico e dati relativi all'ubicazione a fini, in particolare, di salvaguardia della sicurezza nazionale e di lotta alla criminalità, quale la normativa di cui trattasi nei procedimenti principali, rientra nell'ambito di applicazione della direttiva 2002/58 (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 104).

Sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58

Richiamo dei principi derivanti dalla giurisprudenza della Corte

49 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 32 e giurisprudenza ivi citata).

50 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» i diritti e gli obblighi previsti in particolare agli articoli 5, 6 e 9 della direttiva 2002/58 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 33).

51 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, frasi prima e seconda, di detta direttiva, gli Stati membri sono tenuti ad assicurare, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate attraverso la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare, essi hanno l'obbligo di vietare l'ascolto, la captazione, l'archiviazione 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 ciò sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1, della medesima direttiva (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 34).

52 A tale 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 archiviare tali comunicazioni e dati senza il loro consenso (sentenze del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:20, punto 107, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 35).

53 Tale disposizione riflette l'obiettivo perseguito dal legislatore dell'Unione al momento dell'adozione della direttiva 2002/58. Risulta, infatti, dalla motivazione 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 definitivo], 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 archiviazione 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, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 36 e giurisprudenza ivi citata).

54 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 (sentenze del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:20, punto 109, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 37).

55 Per quanto riguarda il trattamento e l'archiviazione 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 relativi al 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.

56 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 archiviazione da parte di terzi (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 39).

57 Nei limiti in cui l'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di adottare misure legislative volte 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 archiviazione dei dati ad esse relativi, ricordati al punto 52 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 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 archiviare tali dati, previsto all'articolo 5 di detta direttiva, divenga la regola, salvo privare quest'ultima norma di gran parte della sua portata (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 40 e giurisprudenza ivi citata).

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

59 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 tale 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, ma anche dell'articolo 11 della Carta, relativo alla libertà di espressione, libertà questa che costituisce uno dei fondamenti essenziali di una società democratica e pluralista e che fa parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione europea è fondata (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punti 42 e 43 e giurisprudenza ivi citata).

60 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 archiviare 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 delicato, che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza o che i dati conservati siano o meno utilizzati successivamente (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 44 e giurisprudenza ivi citata).

61 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 delicate, 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 di 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 degli interessati, informazione tanto delicata, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 45 e giurisprudenza ivi citata).

62 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 indiscriminata, nonché del carattere delicato delle informazioni che tali dati possono fornire, la conservazione di questi dati da parte dei fornitori di servizi di comunicazione elettronica comporta di per sé rischi di abuso e di accesso illecito (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 46 e giurisprudenza ivi citata).

63 Ciò premesso, consentendo agli Stati membri di limitare i diritti e gli obblighi di cui ai punti da 51 a 54 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 come 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 48 e giurisprudenza ivi citata).

64 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 concreti 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 49 e giurisprudenza ivi citata).

65 A fronte di questi diversi obblighi positivi, occorre quindi procedere al contemperamento dei diversi interessi legittimi e diritti in gioco e stabilire un quadro normativo che consenta tale contemperamento (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 50 e giurisprudenza ivi citata).

66 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 deroghi al principio di riservatezza evocato al punto 52 della presente sentenza qualora una tale misura sia «necessaria, opportuna e proporzionata all'interno di una società democratica», mentre il considerando 11 della stessa direttiva precisa al riguardo che una simile misura deve essere «strettamente» proporzionata allo scopo perseguito.

67 A tale 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 52 e giurisprudenza ivi citata).

68 Più in particolare, dalla giurisprudenza della Corte risulta che la facoltà 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 53 e giurisprudenza ivi citata).

69 Per soddisfare il requisito di proporzionalità, una normativa nazionale 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 siano 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 delicati (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 54 e giurisprudenza ivi citata).

70 Pertanto, una normativa nazionale 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 55 e giurisprudenza ivi citata).

71 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 56).

72 In tal senso, per quanto riguarda la salvaguardia della sicurezza nazionale, la cui importanza è maggiore rispetto a quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, la Corte ha constatato che tale disposizione, letta 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 indiscriminata 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 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 58 e giurisprudenza ivi citata).

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

74 Per quanto riguarda l'obiettivo della lotta ai reati gravi, la Corte ha statuito che una normativa nazionale che prevede, a tal fine, la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione viola i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica. Infatti, tenuto conto del carattere delicato 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 62 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 riguardo agli obiettivi di lotta ai reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza nonché all'importanza che occorre loro riconoscere (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 65 e giurisprudenza ivi citata).

75 Per contro, 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 ai reati gravi e della prevenzione delle minacce gravi alla pubblica sicurezza

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

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

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

– il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida (*quick freeze*) dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono,

quando tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi è subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongano di garanzie effettive contro il rischio di abusi (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 168, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 67).

Su una misura che prevede, per un periodo di varie settimane, una conservazione generalizzata e indiscriminata della maggior parte dei dati relativi al traffico e dei dati relativi all'ubicazione

76 È alla luce delle considerazioni di principio suesposte che occorre esaminare le caratteristiche della normativa nazionale oggetto dei procedimenti principali, evidenziate dal giudice del rinvio.

77 In primo luogo, per quanto attiene all'ampiezza dei dati conservati, dalla decisione di rinvio risulta che, nell'ambito della fornitura di servizi di telefonia, l'obbligo di conservazione prescritto da tale normativa riguarda, in particolare, i dati necessari per individuare l'origine e la destinazione di una comunicazione, la data e l'ora di inizio e fine della comunicazione o – in caso di comunicazione per SMS, messaggio multimediale o simile – il momento dell'invio e della ricezione del messaggio nonché, in caso di utilizzo di servizi di telefonia mobile, l'indicazione delle celle telefoniche utilizzate all'inizio della comunicazione da chi effettua la chiamata e da chi la riceve. Nell'ambito della fornitura di servizi di accesso a Internet, l'obbligo di conservazione riguarda, tra l'altro, l'indirizzo IP assegnato all'abbonato, la data e l'ora di inizio e fine dell'utilizzo di Internet a partire dall'indirizzo IP assegnato e, in caso di utilizzo di servizi di telefonia mobile, l'indicazione delle celle telefoniche utilizzate all'inizio del collegamento a Internet. Devono altresì essere conservati i dati che permettano di conoscere la posizione geografica e le direzioni di radiazione massima delle antenne che servono la cella telefonica in questione.

78 Se è vero che la normativa nazionale di cui ai procedimenti principali esclude dall'obbligo di conservazione il contenuto della comunicazione e i dati relativi ai siti Internet consultati, e impone la conservazione dell'identificatore di cella solo all'inizio della comunicazione, occorre tuttavia osservare che lo stesso valeva, in sostanza, per le normative nazionali di recepimento della direttiva 2006/24 in discussione nelle cause che hanno dato origine alla 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). Orbene, nonostante tali limitazioni, la Corte ha dichiarato, nella sentenza succitata, che le categorie di dati conservati in forza di detta direttiva e di tali normative nazionali potevano consentire di trarre conclusioni molto precise sulla vita privata degli interessati, quali le abitudini di vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati e di fornire, in particolare, gli strumenti per stabilire il profilo di tali persone.

79 Va oltretutto constatato che, sebbene la normativa oggetto dei procedimenti principali non riguardi i dati relativi ai siti Internet consultati, essa prevede nondimeno la conservazione degli indirizzi IP. Orbene, poiché tali indirizzi possono essere utilizzati per effettuare, in particolare, il tracciamento completo del percorso di navigazione di un utente di Internet e, di conseguenza, della sua attività online, tali dati consentono di stabilire il profilo dettagliato di quest'ultimo. Pertanto, la conservazione e l'analisi di detti indirizzi IP necessari per un siffatto tracciamento costituiscono ingerenze gravi nei diritti fondamentali dell'utente di Internet sanciti dagli articoli 7 e 8 della Carta (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 153).

80 Inoltre, e come rilevato dalla SpaceNet nelle sue osservazioni scritte, i dati relativi ai servizi di posta elettronica, pur non essendo soggetti all'obbligo di conservazione previsto dalla normativa di cui ai procedimenti principali, rappresentano solo una minima parte dei dati in questione.

81 Pertanto, come rilevato, in sostanza, dall'avvocato generale al paragrafo 60 delle sue conclusioni, l'obbligo di conservazione previsto dalla normativa nazionale di cui ai procedimenti principali si estende a un insieme molto ampio di dati relativi al traffico e di dati relativi all'ubicazione, che corrispondono, in sostanza, a quelli che hanno portato alla giurisprudenza costante richiamata al punto 78 della presente sentenza.

82 Per di più, in risposta a un quesito posto in udienza, il governo tedesco ha precisato che solo 1 300 enti erano inseriti nell'elenco delle persone, delle autorità o delle organizzazioni a carattere sociale o religioso i cui dati relativi alle comunicazioni elettroniche non sono conservati in forza dell'articolo 99, paragrafo 2, e dell'articolo 113 b, paragrafo 6, del TKG, il che rappresenta manifestamente una parte ridotta di tutti gli utenti dei servizi di telecomunicazione in Germania i cui dati rientrano nell'obbligo di conservazione previsto dalla normativa nazionale di cui ai procedimenti principali. Sono così conservati, in particolare, i dati di utenti soggetti al segreto professionale, quali avvocati, medici e giornalisti.

83 Dalla decisione di rinvio risulta quindi che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione prevista da tale normativa nazionale riguarda la quasi totalità delle persone che compongono la popolazione, senza che queste ultime si trovino, anche indirettamente, in una situazione tale da dar avvio a procedimenti penali. Analogamente, detta normativa impone la conservazione, senza alcuna motivazione, generalizzata e indiscriminata da un punto di vista personale, temporale e geografico, di gran parte dei dati relativi al traffico e dei dati relativi all'ubicazione la cui ampiezza corrisponde, in sostanza, a quella dei dati conservati di cui alle cause che hanno portato alla giurisprudenza menzionata al punto 78 della presente sentenza.

84 Pertanto, alla luce della giurisprudenza citata al punto 75 della presente sentenza, un obbligo di conservazione dei dati come quello di cui ai procedimenti principali non può essere considerato come una conservazione mirata dei dati, contrariamente a quanto sostiene il governo tedesco.

85 In secondo luogo, per quanto riguarda il periodo di conservazione dei dati, dall'articolo 15, paragrafo 1, seconda frase, della direttiva 2002/58 emerge che il periodo di conservazione previsto da una misura nazionale che impone un obbligo di conservazione generalizzata e indiscriminata è, certamente, un fattore rilevante, tra gli altri, al fine di stabilire se il diritto dell'Unione osti a una simile misura, atteso che detta frase richiede che tale periodo di tempo sia «limitato».

86 Orbene, nel caso di specie, vero è che tali periodi, i quali, ai sensi dell'articolo 113b, paragrafo 1, del TKG, ammontano a quattro settimane per i dati relativi all'ubicazione e a dieci settimane per gli altri dati, sono notevolmente più brevi di quelli previsti dalle normative nazionali che imponevano un obbligo di conservazione generalizzato e indifferenziato esaminate dalla Corte nelle sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, EU:C:2020:791), e del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258).

87 Tuttavia, come risulta dalla giurisprudenza citata al punto 61 della presente sentenza, la gravità dell'ingerenza deriva dal rischio, tenuto conto in particolare della loro quantità e della loro varietà, che i dati conservati, considerati nel loro insieme, consentano di trarre conclusioni molto

precise riguardo alla vita privata della persona o delle persone i cui dati sono stati conservati e, in particolare, forniscano i mezzi per stabilire il profilo della persona o delle persone interessate, che è un'informazione tanto delicata, alla luce del diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni.

88 Pertanto, la conservazione dei dati relativi al traffico o dei dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali dallo stesso utilizzate, presenta in ogni caso un carattere grave indipendentemente dalla durata del periodo di conservazione, dalla quantità o dalla natura dei dati conservati, qualora questo insieme di dati sia tale da permettere di trarre conclusioni molto precise sulla vita privata della persona o delle persone interessate [v., per quanto riguarda l'accesso a simili dati, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 39].

89 A tale riguardo, anche la conservazione di un quantitativo limitato di dati relativi al traffico o di dati relativi all'ubicazione, oppure la conservazione di tali dati per un breve periodo, sono idonee a fornire informazioni molto precise sulla vita privata di un utente di un mezzo di comunicazione elettronica. Inoltre, la quantità dei dati disponibili e le informazioni molto precise sulla vita privata dell'interessato che ne derivano possono essere valutate solo dopo la consultazione dei dati suddetti. Orbene, l'ingerenza risultante dalla conservazione di detti dati avviene necessariamente prima che i dati e le informazioni che ne derivano possano essere consultati. Pertanto, la valutazione della gravità dell'ingerenza costituita dalla conservazione si effettua necessariamente in funzione del rischio generalmente afferente alla categoria di dati conservati per la vita privata degli interessati, senza che risulti rilevante, per altro verso, sapere se le informazioni relative alla vita privata che ne derivano abbiano o no, concretamente, un carattere delicato [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 40].

90 Nel caso di specie, come risulta dal punto 77 della presente sentenza e come confermato in udienza, un insieme di dati relativi al traffico e di dati relativi all'ubicazione conservati, rispettivamente, per dieci settimane e per quattro settimane può consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono conservati, quali le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati, e, in particolare, di stabilire un profilo di dette persone.

91 In terzo luogo, per quanto riguarda le garanzie previste dalla normativa nazionale oggetto dei procedimenti principali, volte a proteggere i dati conservati dai rischi di abuso e da qualsiasi accesso illecito, occorre rilevare che la conservazione di tali dati e l'accesso ad essi costituiscono, come risulta dalla giurisprudenza richiamata al punto 60 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 garantisca 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 a limitare e neppure a rimediare all'ingerenza grave che risulterebbe dalla conservazione generalizzata di tali dati prevista da detta normativa nazionale, nei diritti garantiti dagli articoli 5 e 6 di tale direttiva e dai diritti fondamentali di cui i citati articoli costituiscono la concretizzazione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 47).

92 In quarto e ultimo luogo, per quanto riguarda l'argomento della Commissione europea secondo cui la criminalità particolarmente grave potrebbe essere equiparata a una minaccia per la sicurezza nazionale, 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 le attività di terrorismo (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 61 e giurisprudenza ivi citata).

93 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 indiscriminata 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 62 e giurisprudenza ivi citata).

94 Pertanto, la criminalità, anche particolarmente grave, non può essere equiparata a una minaccia per la sicurezza nazionale. Infatti, una siffatta equiparazione equivarrebbe a introdurre una categoria intermedia tra la sicurezza nazionale e la pubblica sicurezza, per applicare alla seconda i requisiti inerenti alla prima (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 63).

Sulle misure che prevedono una conservazione mirata, una conservazione rapida o una conservazione degli indirizzi IP

95 Diversi governi, tra i quali il governo francese, sottolineano che solo una conservazione generalizzata e indiscriminata consentirebbe la realizzazione efficace degli obiettivi perseguiti dalle misure di conservazione, mentre il governo tedesco precisa, in sostanza, che una simile conclusione non è inficiata dal fatto che gli Stati membri possano ricorrere alle misure di conservazione mirata e di conservazione rapida di cui al punto 75 della presente sentenza.

96 A tale riguardo occorre rilevare, in primo luogo, che l'efficacia delle azioni giudiziarie in materia penale 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 69).

97 In secondo luogo, 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 75 della presente sentenza, consente agli Stati membri di adottare, ai fini della lotta ai reati gravi e della prevenzione di minacce gravi alla pubblica sicurezza, non solo misure che istituiscono una conservazione mirata e una conservazione rapida, ma anche misure che prevedano una conservazione generalizzata e indiscriminata, da un lato, dei dati relativi all'identità anagrafica degli utenti dei mezzi di comunicazione elettronica e, dall'altro, degli indirizzi IP attribuiti alla fonte di una connessione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 70).

98 A tale riguardo, è pacifico che la conservazione dei dati relativi all'identità anagrafica degli utenti dei mezzi di comunicazione elettronica può contribuire alla lotta ai reati gravi, purché tali dati consentano di identificare le persone che hanno utilizzato simili mezzi nell'ambito della preparazione o della commissione di un atto rientrante nei reati gravi (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 71).

99 Ebbene, la direttiva 2002/58 non osta, ai fini della lotta alla criminalità in generale, alla conservazione generalizzata dei dati relativi all'identità anagrafica. 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, mentre il venditore è eventualmente tenuto a consentire l'accesso a tali informazioni alle autorità nazionali competenti (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 72).

100 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 constatato che, ai fini del necessario contemperamento dei diritti e degli interessi legittimi in gioco richiesto dalla giurisprudenza di cui ai punti da 65 a 68 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, e rettifica in GU 2012, L 18, pag. 7), 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 73).

101 Ciò posto, se è pur vero che una misura legislativa che preveda la conservazione degli indirizzi IP di tutte le persone fisiche proprietarie di un'apparecchiatura terminale a partire dalla quale può essere effettuato un accesso a Internet potrebbe riguardare persone che, a prima vista, non presentino un collegamento, ai sensi della giurisprudenza citata al punto 70 della presente sentenza, con gli obiettivi perseguiti, e che gli utenti di Internet dispongono, conformemente a quanto osservato al precedente punto 54, del diritto di attendersi, in forza degli articoli 7 e 8 della Carta, che la loro identità, in linea di principio, non sia rivelata, una misura legislativa che preveda la conservazione generalizzata e indiscriminata dei soli indirizzi IP attribuiti all'origine 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 e dell'articolo 52, paragrafo 1, della Carta, purché tale facoltà sia subordinata al rigoroso rispetto delle condizioni sostanziali e procedurali che devono disciplinare l'utilizzo dei dati in questione (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 155).

102 Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta che tale conservazione comporta, solo la lotta ai reati gravi e la prevenzione delle minacce gravi alla pubblica sicurezza sono idonee, al pari della salvaguardia della sicurezza nazionale, a giustificare siffatta ingerenza. Inoltre, la durata della conservazione non può eccedere quella strettamente necessaria alla luce dell'obiettivo perseguito. Infine, una misura di questa natura deve prevedere condizioni e garanzie rigorose riguardo all'utilizzo di tali dati, segnatamente mediante tracciamento, in relazione alle comunicazioni ed attività effettuate online dagli interessati (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 156).

103 Pertanto, contrariamente a quanto sottolineato dal giudice del rinvio, non esiste alcuna tensione tra i punti 155 e 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). Infatti, come rilevato in sostanza dall'avvocato generale ai paragrafi 81 e 82 delle sue conclusioni, da detto punto 155, letto in combinato disposto con il punto 156 e con il punto 168 di tale sentenza, risulta chiaramente che solo la lotta ai reati gravi e la prevenzione di minacce gravi alla pubblica sicurezza sono idonee, al pari della salvaguardia della sicurezza nazionale, a giustificare la conservazione generalizzata degli indirizzi IP attribuiti alla fonte di una connessione, indipendentemente dal fatto che gli interessati possano presentare un nesso, quanto meno indiretto, con gli obiettivi perseguiti.

104 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, da talune considerazioni esposte da alcuni Stati membri in ordine a simili misure emerge una comprensione più restrittiva della portata di tali misure rispetto a quella accolta dalla giurisprudenza citata al punto 75 della presente sentenza. Infatti, sebbene, conformemente a quanto ricordato al punto 57 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 imponga 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 imponga una conservazione rapida sia limitata a persone sospette identificate prima di una siffatta ingiunzione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 75).

105 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, di contribuire alla lotta contro la criminalità grave o di prevenire un grave rischio per la pubblica sicurezza o, ancora, un rischio per la sicurezza nazionale (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 76 e giurisprudenza ivi citata).

106 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 prese in considerazione 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 pubblica sicurezza o la sicurezza nazionale dello Stato membro interessato (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 77).

107 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 78).

108 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, porti marittimi o aree di pedaggio (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 79 e giurisprudenza ivi citata).

109 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 80).

110 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 aree 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, mediante 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 81).

111 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 i reati gravi. Infatti, la Corte ha già dichiarato che la durata delle misure di conservazione mirata descritte ai punti da 105 a 110 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 (sentenze del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:20, punto 151, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 82).

112 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 indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 83).

113 In ogni caso, come rilevato dall'avvocato generale al paragrafo 50 delle sue conclusioni, 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 indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 84).

114 Per quanto riguarda, sotto un secondo profilo, la conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione trattati e archiviati 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 avvenire, conformemente alle disposizioni nazionali che recepiscono detta direttiva, il loro trattamento e la loro archiviazione. Tuttavia, la Corte ha stabilito che, durante il trattamento o l'archiviazione, possono presentarsi situazioni nelle quali si ponga 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 rilevanti (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 85).

115 In una situazione del genere, tenuto conto del necessario contemperamento dei diritti e degli interessi legittimi di cui ai punti da 65 a 68 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 (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 163, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 86).

116 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 illustrato 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) (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 87).

117 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 pubblica sicurezza 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 70 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 (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 165, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 88).

118 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 pubblica sicurezza o alla commissione di un atto di criminalità grave, una vittima sia stata in contatto utilizzando i suoi mezzi di comunicazione elettronica (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 89).

119 Una siffatta conservazione rapida può, secondo la giurisprudenza della Corte ricordata al punto 117 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, vittima potenziale di un atto di criminalità grave, sia 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) (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 90).

120 Per altro verso, 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 pubblica sicurezza 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 91).

121 Per quanto riguarda ancora la diversità di misure di conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione di cui al punto 75 della presente sentenza, occorre precisare che tali differenti 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 92).

122 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 necessità, ma anche di quello relativo al carattere proporzionato di tali misure rispetto all'obiettivo perseguito (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 93).

123 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 pubblica sicurezza e la sua efficacia possa dipendere in larga misura dall'uso delle moderne tecniche di indagine, un simile obiettivo di interesse generale, per quanto fondamentale, non può di per sé giustificare il fatto che una misura di conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, come quella introdotta dalla direttiva 2006/24, sia considerata necessaria (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 94).

124 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 64 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, la quale 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, quanto meno indiretta, con l'obiettivo perseguito (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 95).

125 Per altro verso, le sentenze della Corte EDU del 25 maggio 2021, Big Brother Watch e a. c. Regno Unito (CE:ECHR:2021:0525JUD 005817013), e del 25 maggio 2021, Centrum för Rättvisa c. Svezia (CE:ECHR:2021:0525JUD 003525208), invocate da taluni governi in udienza per sostenere che la CEDU non osterebbe a normative nazionali che prevedano, in sostanza, una conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, non possono rimettere in discussione l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 derivante dalle considerazioni che precedono. Infatti, tali sentenze riguardavano intercettazioni di massa di dati relative a comunicazioni internazionali. Pertanto, e come rilevato dalla Commissione in udienza, la Corte europea dei diritti dell'uomo non si è pronunciata, in dette sentenze, sulla conformità alla CEDU di una conservazione generalizzata e indiscriminata di dati relativi al traffico e di dati relativi all'ubicazione nel territorio nazionale né tantomeno di un'intercettazione di ampia portata di tali dati ai fini della prevenzione, dell'accertamento e della ricerca di reati gravi. In ogni caso, occorre ricordare che l'articolo 52, paragrafo 3, della Carta mira a garantire la necessaria coerenza tra i diritti contenuti in quest'ultima e i diritti corrispondenti garantiti dalla CEDU, senza pregiudicare l'autonomia del diritto dell'Unione e della Corte di giustizia dell'Unione europea, sicché occorre tenere conto dei diritti corrispondenti della CEDU ai fini dell'interpretazione della Carta solo quale soglia di protezione minima (sentenza del 17 dicembre 2020, Centraal Israëlitisch Consistorie van België e a., C-336/19, EU:C:2020:1031, punto 56).

Sull'accesso ai dati che sono stati conservati in modo generalizzato e indiscriminato

126 In 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 indiscriminato, 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.

127 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 indiscriminato 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, laddove, 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 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 97).

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

129 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 68, 71, 72 e 73 della presente sentenza (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 99).

130 Inoltre e soprattutto, conformemente alla giurisprudenza ricordata al punto 74 della presente sentenza, i dati relativi al traffico e i dati relativi all'ubicazione non possono essere oggetto di una conservazione generalizzata e indiscriminata 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 indiscriminata a fini di salvaguardia della sicurezza nazionale da una minaccia che si riveli reale e attuale o prevedibile, alle condizioni indicate al punto 71 della presente sentenza, le autorità nazionali competenti in materia di indagini penali non possono accedere a detti dati nell'ambito di procedimenti penali, salvo privare di ogni efficacia pratica il divieto di procedere a una siffatta conservazione ai fini della lotta alla criminalità grave, richiamato al citato punto 74 (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 100).

131 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle questione pregiudiziale dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta a misure legislative nazionali che prevedono, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla pubblica sicurezza, la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione. Il predetto articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso non osta, viceversa, a misure legislative nazionali:

– che consentono, 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 indiscriminata 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, e 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;

– che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta ai reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza, una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;

– che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta ai reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza, la conservazione generalizzata e indiscriminata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della pubblica sicurezza, una conservazione generalizzata e indiscriminata dei dati relativi all'identità anagrafica degli utenti di mezzi di comunicazione elettronica, e

– che consentono, a fini di lotta ai reati gravi e, a fortiori, di salvaguardia della sicurezza nazionale, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono,

quando tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi è subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongono di garanzie effettive contro il rischio di abusi.

Sulle spese

132 Nei confronti delle parti nei procedimenti principali le presenti cause costituiscono un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

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

L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo l, della Carta dei diritti fondamentali dell'Unione europea,

deve essere interpretato nel senso che esso:

osta a misure legislative nazionali che prevedono, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla pubblica sicurezza, la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione;

non osta a misure legislative nazionali:

– **che consentono, 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 indiscriminata 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, e 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;

– **che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta ai reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza, una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;**

– **che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta ai reati gravi e di prevenzione delle minacce gravi alla pubblica sicurezza, la conservazione generalizzata e indiscriminata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;**

– **che prevedono, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della pubblica sicurezza, una conservazione generalizzata e indiscriminata dei dati relativi all'identità anagrafica degli utenti di mezzi di comunicazione elettronica, e**

– **che consentono, a fini di lotta ai reati gravi e, a fortiori, di salvaguardia della sicurezza nazionale, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono,**

quando tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi è subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongono di garanzie effettive contro il rischio di abusi.

Firme