Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

6 ottobre 2020*

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Fornitori di servizi di comunicazione elettronica – Trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Salvaguardia della sicurezza nazionale – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 1, paragrafo 3, e articolo 3 – Riservatezza delle comunicazioni elettroniche – Tutela – Articolo 5 e articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11 nonché articolo 52, paragrafo 1 – Articolo 4, paragrafo 2, TUE»

Nella causa C-623/17,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dall'Investigatory Powers Tribunal (Tribunale incaricato dei poteri di indagine, Regno Unito), con decisione del 18 ottobre 2017, pervenuta in cancelleria il 31 ottobre 2017, nel procedimento

Privacy International

contro

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

LA CORTE (Grande Sezione),

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

avvocato generale: M. Campos Sánchez-Bordona

cancelliere: C. Strömholm, amministratrice

vista la fase scritta del procedimento e in seguito all'udienza del 9 e 10 settembre 2019,

* Lingua processuale: l'inglese.

considerate le osservazioni presentate:

– per la Privacy International, da B. Jaffey e T. de la Mare, QC, D. Cashman, solicitor, e H. Roy, avocat;

– per il governo del Regno Unito, da Z. Lavery, D. Guðmundsdóttir e S. Brandon, in qualità di agenti, assistiti da G. Facenna e D. Beard, QC, e da C. Knight e R. Palmer, barristers;

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

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

– per il governo tedesco, inizialmente da M. Hellmann, R. Kanitz, D. Klebs e T. Henze, successivamente da J. Möller, M. Hellmann, R. Kanitz e D. Klebs, in qualità di agenti;

– per il governo estone, da A. Kalbus, in qualità di agente;

– per il governo irlandese, da M. Browne, G. Hodge e A. Joyce, in qualità di agenti, assistiti da D. Fennelly, barrister;

– per il governo spagnolo, inizialmente da L. Aguilera Ruiz e M.J. García-Valdecasas Dorrego, successivamente da L. Aguilera Ruiz, in qualità di agenti;

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

– per il governo cipriota, da E. Symeonidou ed E. Neofytou, in qualità di agenti;

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

– per il governo ungherese, inizialmente da G. Koós, M.Z. Fehér, G. Tornyai e Z. Wagner, successivamente da G. Koós e M.Z. Fehér, in qualità di agenti;

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

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

– per il governo portoghese, da L. Inez Fernandes, M. Figueiredo e F. Aragão Homem, in qualità di agenti;

– per il governo svedese, inizialmente da A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren e A. Alriksson, successivamente da H. Shev, C. Meyer-Seitz, L. Zettergren e A. Alriksson, in qualità di agenti;

– per il governo norvegese, da T.B. Leming, M. Emberland e J. Vangsnes, in qualità di agenti;

– per la Commissione europea, inizialmente da H. Kranenborg, M. Wasmeier, D. Nardi e P. Costa de Oliveira, successivamente da H. Kranenborg, M. Wasmeier e D. Nardi, in qualità di agenti;

– per il Garante europeo della protezione dei dati, da T. Zerdick e A. Buchta, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 15 gennaio 2020,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'articolo 1, paragrafo 3, e 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»), letti alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7 e 8 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 Tale domanda è stata proposta nell'ambito di una controversia che vede la Privacy International contrapposta al Secretary of State for Foreign and Commonwealth Affairs (Ministro degli Affari esteri e del Commonwealth, Regno Unito), al Secretary of State for the Home Departement (Ministro dell'Interno, Regno Unito), al Government Communications Headquarters (Quartier generale delle comunicazioni, Regno Unito) (in prosieguo: il «GCHQ»), al Security Service (Servizio di sicurezza, Regno Unito; in prosieguo: il «MI5») e al Secret Intelligence Service (servizio segreto di intelligence, Regno Unito; in prosieguo: il «MI6»), in ordine alla legittimità di una normativa che autorizza l'acquisizione e l'utilizzo da parte dei servizi di sicurezza e di intelligence di dati di comunicazione in massa *(bulk communications data)*.

Contesto normativo

Diritto dell'Unione

Direttiva 95/46

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 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/CE (GU 2016, L 119, pag. 1). L'articolo 3 di detta direttiva, dal titolo «Campo d'applicazione», era così formulato:

«1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. 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 [TUE] 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

4 I considerando 2, 6, 7, 11, 22, 26 e 30 della direttiva 2002/58 sono così formulati:

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

(...)

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

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

(...)

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

(...)

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione. Ove ciò sia necessario per rendere più efficiente l'inoltro di tutte le informazioni accessibili al pubblico ad altri destinatari del servizio su loro richiesta, la presente direttiva non osta a che tali informazioni possano essere ulteriormente

memorizzate, a condizione che esse siano in ogni caso accessibili al pubblico senza restrizioni e che tutti i dati che si riferiscono ai singoli abbonati o utenti che richiedono tali informazioni siano cancellati.

(...)

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati (...) può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione (...) dovrebbero inoltre essere cancellati o resi anonimi. (…)

(...)

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari. (...)».

5 L'articolo 1 della direttiva 2002/58, dal titolo «Finalità e campo d'applicazione», dispone:

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

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

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del [TFUE], quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale».

6 Ai sensi dell'articolo 2 di tale direttiva, intitolato «Definizioni»:

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

Si applicano inoltre le seguenti definizioni:

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

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

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

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

(...)».

7 L’articolo 3 di detta direttiva, dal titolo «Servizi interessati», prevede:

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

8 A termini dell’articolo 5 della direttiva 2002/58, 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».

9 L’articolo 6 della direttiva 2002/58, dal titolo «Dati sul traffico», recita:

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

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

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

(...)

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

10 L'articolo 9 di tale direttiva, dal titolo «Dati relativi all'ubicazione diversi dai dati relativi al traffico», prevede, al paragrafo 1:

«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. (...)».

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

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

Regolamento 2016/679

12 L'articolo 2 del regolamento 2016/679 dispone:

«1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; (...)

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

(...)».

13 L'articolo 4 di tale regolamento dispone:

«Ai fini del presente regolamento s'intende per:

(...)

2) "trattamento", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(...)».

14 Ai sensi dell'articolo 23, paragrafo 1, dello stesso regolamento:

«Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili».

15 A tenore dell'articolo 94, paragrafo 2, del regolamento 2016/679:

«I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva [95/46] si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento».

Diritto del Regno Unito

16 L'articolo 94 del Telecommunications Act 1984, nella versione applicabile ai fatti del procedimento principale (in prosieguo: la «legge del 1984»), dal titolo «Istruzioni nell'interesse della sicurezza nazionale ecc.», dispone:

«(1) Il Ministro può, previa consultazione di una persona cui si applica il presente articolo, ingiungere a tale persona ordini di carattere generale, nei limiti di quanto necessario, secondo il Ministro, nell'interesse della sicurezza nazionale o delle relazioni intrattenute con il governo di un paese o territorio situato fuori dal Regno Unito.

(2) Ove appaia necessario al Ministro procedere in tal senso nell'interesse della sicurezza nazionale o delle relazioni intrattenute con il governo di un paese o territorio situato fuori dal Regno Unito, esso può, previa consultazione di una persona cui si applica il presente articolo, ingiungere ordini a tale persona chiedendole (a seconda delle circostanze del caso di specie) di eseguire o di non eseguire un'azione particolare specificata negli ordini.

(2A) Il Ministro può ingiungere ordini ai sensi del paragrafo (1) o (2) solo se ritenga che il comportamento imposto da questi ultimi sia proporzionato all'obiettivo da conseguire attraverso tale comportamento.

(3) La persona a cui si applica il presente articolo deve eseguire tutti gli ordini che le vengono impartiti dal Ministro ai sensi del presente articolo, malgrado ogni altro obbligo ad essa incombente in forza della parte 1 o della parte 2, capo 1, del Communications Act 2003 [legge del 2003 sulle comunicazioni] e, nel caso di ordini impartiti al gestore di una rete pubblica di comunicazioni elettroniche, anche se detti ordini gli si applicano in base ad una qualità diversa da quella di fornitore di accesso ad una rete del genere.

(4) Il Ministro deposita presso ciascuna delle Camere del Parlamento copia di tutti gli ordini impartiti ai sensi del presente articolo, a meno che non ritenga che la divulgazione di detti ordini sia in contrasto con gli interessi della sicurezza nazionale o delle relazioni intrattenute con il governo di un paese o territorio situato fuori dal Regno Unito, o con gli interessi commerciali di una persona.

(5) Una persona non deve divulgare, o non può essere tenuta a divulgare, in forza di una legge o altro, informazioni di qualunque genere riguardanti misure adottate ai sensi del presente articolo ove il Ministro le abbia comunicato di essere del parere che la divulgazione di tali informazioni sia in contrasto con gli interessi della sicurezza nazionale o delle relazioni intrattenute con il governo di un paese o territorio situato fuori dal Regno Unito, o con agli interessi commerciali di un'altra persona.

(...)

(8) Il presente articolo si applica all'[Office of communications (OFCOM)] e a fornitori di reti pubbliche di comunicazione elettronica».

17 L'articolo 21, paragrafi 4 e 6, del Regulation of Investigatory Powers Act 2000 (legge del 2010 recante disciplina dei poteri d'indagine; in prosieguo: la «RIPA»), dispone:

«(4) [L]'espressione "dati relativi a comunicazioni" può avere uno dei significati che seguono:

(a) i dati sul traffico riportati in una comunicazione o allegati ad essa (dal mittente o altrimenti) per le finalità di qualsiasi sevizio postale o di qualsiasi sistema di telecomunicazione tramite il quale la comunicazione sia trasmessa o possa essere trasmessa;

(b) le informazioni che non ricomprendono nessuno dei contenuti di una comunicazione [ad eccezione delle informazioni di cui alla lettera a)], relative all'utilizzo effettuato da qualsiasi persona:
(i) di qualsiasi servizio postale o servizio di telecomunicazione; o
(ii) in relazione alla fornitura o all'utilizzo da parte di qualsiasi persona di qualsivoglia servizio di telecomunicazioni, di qualsiasi parte di un sistema di telecomunicazioni;

(c) le informazioni che non rientrano nelle lettere (a) o (b), conservate o acquisite, in relazione ai destinatari del servizio, da una persona che presta un sevizio postale o un servizio di telecomunicazioni.

(...)

(6) [L]'espressione "dati sul traffico", in relazione a qualsiasi comunicazione, si riferisce a:

(a) qualsiasi dato che individui o sia idoneo a individuare la persona, l'apparecchio o l'ubicazione verso cui o da cui viene trasmessa o può essere trasmessa una comunicazione,

(b) qualsiasi dato che individui o selezioni oppure sia idoneo a individuare o selezionare l'apparecchio con cui viene trasmessa o può essere trasmessa la comunicazione,

(c) qualsiasi dato che includa segnali per l'attivazione dell'apparecchio utilizzato in un sistema di comunicazione ai fini della trasmissione di qualsiasi comunicazione, e

(d) qualsiasi dato che identifichi i dati riportati in una specifica comunicazione o allegati ad essa o altri dati come dati riportati in una specifica comunicazione o allegati ad essa.

(...)».

18 Gli articoli da 65 a 69 della RIPA fissano le norme relative al funzionamento e alle competenze dell'Investigatory Powers Tribunal (Tribunale incaricato dei poteri d'indagine, Regno Unito). Conformemente all'articolo 65 di tale legge, possono essere presentate denunce presso tale tribunale se vi è motivo di ritenere che taluni dati siano stati ottenuti in maniera inappropriata.

Procedimento principale e questioni pregiudiziali

19 All'inizio dell'anno 2015, l'esistenza di pratiche di raccolta e di utilizzo di dati relativi a comunicazioni in massa da parte dei vari servizi di sicurezza e di intelligence del Regno Unito, e cioè il GCHQ, il MI5 e il MI6, è stata resa pubblica, in particolare in un rapporto dell'Intelligence and Security Committee of Parliament (commissione intelligence e sicurezza del Parlamento, Regno Unito). Il 5 giugno 2015, la Privacy International, organizzazione non governativa, ha sottoposto all'Investigatory Powers Tribunal (Tribunale incaricato dei poteri d'indagine, Regno Unito) un ricorso contro il Ministro degli Affari esteri e del Commonwealth, il Ministro dell'Interno nonché detti servizi di sicurezza e di intelligence, contestando la legittimità di tali pratiche.

20 Il giudice del rinvio ha esaminato la questione della legittimità di dette pratiche alla luce, innanzitutto, del diritto interno e delle disposizioni della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 (in prosieguo: la «CEDU»), e poi del diritto dell'Unione. In una sentenza del 17 ottobre 2016, tale giudice ha affermato che i convenuti nel procedimento principale avevano riconosciuto che detti servizi di sicurezza e di intelligence raccoglievano e utilizzavano, nell'ambito delle loro attività, aggregati di dati riguardanti privati e rientranti in varie categorie *(bulk personal data)*, come dati biografici o relativi a viaggi, informazioni di natura finanziaria o commerciale, dati in relazione a comunicazioni e atti a contenere informazioni sensibili, coperte da segreto professionale, o ancora materiale giornalistico. Tali dati, ottenuti per vie diverse, anche segrete, sarebbero analizzati mediante controlli incrociati nonché mediante trattamenti automatizzati, potrebbero essere divulgati ad altre persone e autorità, e condivisi con controparti estere. In tale contesto, i servizi di sicurezza e di intelligence utilizzerebbero altresì dati relativi a comunicazioni in massa, raccolti presso gestori di reti pubbliche di comunicazione elettronica in forza, in particolare, di ordini ministeriali adottati sul fondamento dell'articolo 94 della legge del 1984. Il GCHQ e il MI5 procederebbero in tal modo rispettivamente a partire dagli anni 2001 e 2005.

21 Detto giudice ha ritenuto che tali misure di raccolta e di utilizzo di dati fossero conformi al diritto interno e, a partire dall'anno 2015, fatte salve le questioni, non ancora esaminate, relative alla proporzionalità di dette misure e ai trasferimenti di dati a terzi, all'articolo 8 della CEDU. A quest'ultimo proposito, ha precisato che dinanzi ad esso erano state prodotte prove vertenti sulle garanzie applicabili, in particolare per quanto riguarda le procedure di accesso e di divulgazione al di fuori dei servizi di sicurezza e di intelligence, le modalità di conservazione dei dati e l'esistenza di controlli indipendenti.

22 Per quanto riguarda la legittimità delle misure di raccolta e di utilizzo controverse nel procedimento principale alla luce del diritto dell'Unione, il giudice del rinvio ha esaminato, in una sentenza dell'8 settembre 2017, la questione se tali misure rientrassero nell'ambito di applicazione di tale diritto e, in caso affermativo, se esse fossero compatibili con tale diritto. Tale giudice ha affermato, per quanto riguarda i dati relativi alle comunicazioni in massa, che i gestori di reti di comunicazione elettronica erano tenuti, in forza dell'articolo 94 della legge del 1984, in caso di ordini in questo senso provenienti da un ministro, a fornire i dati raccolti nell'ambito della loro attività economica rientrante nel diritto dell'Unione ai servizi di sicurezza e di intelligence. Per contro, ciò non valeva per la raccolta degli altri dati, ottenuti da tali servizi senza ricorrere a siffatti poteri d'imperio. Sulla base di tale constatazione, detto giudice ha ritenuto necessario interpellare la Corte al fine di determinare se un regime come quello derivante da tale articolo 94 rientri nell'ambito di applicazione del diritto

dell'Unione e, in caso affermativo, se e in che modo le prescrizioni imposte dalla giurisprudenza derivante dalla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15; in prosieguo: la «sentenza Tele2», EU:C:2016:970), si applichino a tale regime.

23 Al riguardo, nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio afferma che, ai sensi di detto articolo 94, un ministro può dare ai fornitori di servizi di comunicazione elettronica gli ordini generali o specifici che gli appaiono necessari nell'interesse della sicurezza nazionale o delle relazioni con un governo estero. Rinviando alle definizioni contenute all'articolo 21, paragrafi 4 e 6, della RIPA, tale giudice precisa che i dati interessati comprendono i dati relativi al traffico nonché le informazioni sui servizi utilizzati, ai sensi di quest'ultima disposizione, con la sola esclusione del contenuto delle comunicazioni. Tali dati e tali informazioni permetterebbero, in particolare, di conoscere il «chi, dove, quando e come» di una comunicazione. Detti dati sarebbero trasmessi ai servizi di sicurezza e di intelligence e conservati da questi ultimi ai fini delle loro attività.

24 Secondo detto giudice, il regime controverso nel procedimento principale si distingue da quello risultante dal Data Retention and Investigatory Powers Act 2014 (legge del 2014 sulla conservazione dei dati e sui poteri d'indagine), controverso nella causa che ha dato luogo alla sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), poiché quest'ultimo regime prevedeva la conservazione dei dati da parte dei fornitori di servizi di comunicazione elettronica e la loro messa a disposizione, nell'interesse della sicurezza nazionale, non soltanto dei servizi di sicurezza e di intelligence, ma anche di altre autorità pubbliche, in relazione alle loro esigenze. Tale sentenza avrebbe peraltro riguardato un'indagine penale e non la sicurezza nazionale.

25 Il giudice del rinvio aggiunge che le banche dati costituite dai servizi di sicurezza e di intelligence formano oggetto di un'elaborazione di massa e automatizzata, non specifica, diretta a rivelare l'esistenza di eventuali minacce ignote. A tal fine, tale giudice afferma che gli aggregati di metadati così costituiti dovrebbero essere il più possibile completi, al fine di poter disporre di un «pagliaio» per trovare l'«ago» che vi si cela. Riguardo all'utilità della raccolta di dati in massa da parte di detti servizi e delle tecniche di consultazione di tali dati, detto giudice fa riferimento in particolare alle conclusioni del rapporto redatto il 19 agosto 2016 dal sig. David Anderson, QC, all'epoca United Kingdom Independent Reviewer of Terrorism Legislation (controllore indipendente del Regno Unito della legislazione relativa al terrorismo), e che si sarebbe fondato, per redigere tale rapporto, su un esame effettuato da un gruppo di specialisti dell'intelligence e sulla testimonianza di agenti dei servizi di sicurezza e di intelligence.

26 Il giudice del rinvio precisa altresì che, secondo la Privacy International, il regime controverso nel procedimento principale è illegittimo alla luce del diritto dell'Unione, mentre i convenuti nel procedimento principale ritengono che l'obbligo di trasmissione dei dati previsto da tale regime, l'accesso a tali dati nonché il loro utilizzo non rientrino nelle competenze dell'Unione, conformemente, in particolare, all'articolo 4, paragrafo 2, TUE, ai sensi del quale la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro.

27 A tal riguardo, il giudice del rinvio considera, sulla base della sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punti da 56 a 59), relativa al trasferimento dei dati PNR *(Passenger Name Record)* a fini di tutela della pubblica sicurezza, che le attività delle società commerciali nell'ambito del trattamento e del trasferimento di dati al fine di tutelare la sicurezza nazionale non sembrano rientrare nell'ambito di applicazione del diritto dell'Unione. Occorrerebbe verificare non se l'attività controversa costituisca un trattamento di dati, ma soltanto se, nella sua sostanza e nei suoi effetti, l'oggetto di tale attività sia quello di supportare una funzione essenziale dello Stato, ai sensi dell'articolo 4, paragrafo 2, TUE, nell'ambito di un quadro stabilito dai pubblici poteri in ordine alla pubblica sicurezza.

28 Nell'ipotesi in cui le misure controverse nel procedimento principale rientrassero tuttavia nell'ambito di applicazione del diritto dell'Unione, il giudice del rinvio ritiene che le prescrizioni di cui ai punti da 119 a 125 della sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970), appaiano inadeguate nel contesto della sicurezza nazionale e siano tali da ostacolare la capacità dei servizi di sicurezza e di intelligence di far fronte a talune minacce alla sicurezza nazionale.

29 Di conseguenza, l'Investigatory Powers Tribunal (Tribunale incaricato dei poteri d'indagine) ha deciso di sospendere il giudizio e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«In una fattispecie in cui:

a) le capacità [dei servizi di sicurezza e di intelligence] di usare [i dati di comunicazione in massa] di cui dispongono sono essenziali per la tutela della sicurezza nazionale del Regno Unito, anche ai fini di combattere il terrorismo, lo spionaggio e la proliferazione delle armi nucleari;

b) un aspetto fondamentale dell'utilizzo di [dati di comunicazione in massa] da parte [dei servizi di sicurezza e di intelligence] consiste nel rilevare minacce alla sicurezza nazionale precedentemente ignote, attraverso tecniche di raccolta non mirate che si basano sull'aggregazione di [dati di comunicazione in massa] in un unico luogo, la cui principale utilità consiste nell'individuazione e nell'elaborazione tempestiva di obiettivi, oltre a fornire una base d'azione a fronte di una minaccia imminente;

c) il fornitore di una rete di comunicazioni elettroniche non è successivamente tenuto a trattenere [i dati di comunicazione in massa] (oltre il periodo previsto per esigenze aziendali), che vengono quindi conservati unicamente dallo Stato (attraverso [i servizi di sicurezza e di intelligence]);

d) il giudice nazionale ha accertato (con talune riserve) che le garanzie relative all'uso di [dati di comunicazione in massa] da parte [dei servizi di sicurezza e di intelligence] sono conformi con i requisiti imposti dalla CEDU; e

e) il giudice nazionale ha accertato che l'imposizione delle prescrizioni specificate nei punti da 119 a 125 della sentenza [del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)], ove applicabili, vanificherebbe le misure adottate [dai servizi di sicurezza e di intelligence] per proteggere la sicurezza nazionale, mettendo perciò a rischio la sicurezza del Regno Unito;

1) Se, tenuto conto dell'articolo 4 TUE e dell'articolo 1, paragrafo 3, della direttiva [2002/58], la prescrizione contenuta in un ordine rivolto da un ministro a un gestore di reti di comunicazione elettronica di fornire dati di comunicazione in massa [ai servizi] di sicurezza e di intelligence di uno Stato membro rientri nell'ambito di applicazione del diritto dell'Unione e della direttiva [2002/58].

2) In caso di risposta affermativa alla prima questione, se al menzionato ordine ministeriale si applichi alcuna delle prescrizioni [applicabili ai dati relativi a comunicazioni conservate, specificati nei punti da 119 a 125 della sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970)] o qualsiasi altra prescrizione oltre a quelle imposte dalla CEDU. In caso affermativo, in qual misura ed entro quali limiti si applichino tali prescrizioni, tenuto conto dell'esigenza fondamentale [per i servizi di sicurezza e di intelligence] di utilizzare tecniche di acquisizione in massa e di trattamento automatizzato per proteggere la sicurezza nazionale, e altresì in qual misura le capacità di cui trattasi, qualora altrimenti conformi alla CEDU, possano essere seriamente ostacolate dall'imposizione di dette prescrizioni».

Sulle questioni pregiudiziali

Sulla prima questione

30 Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se l'articolo 1, paragrafo 3, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE, debba essere interpretato nel senso che rientra nell'ambito di applicazione di tale direttiva una normativa nazionale che consente ad un'autorità pubblica di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere ai servizi di sicurezza e di intelligence dati relativi al traffico e dati relativi all'ubicazione ai fini della salvaguardia della sicurezza nazionale.

31 A tal riguardo, la Privacy International sostiene, in sostanza, che, alla luce dei principi derivanti dalla giurisprudenza della Corte in ordine all'ambito di applicazione della direttiva 2002/58, tanto la raccolta dei dati da parte dei servizi di sicurezza e di intelligence presso tali fornitori, in forza dell'articolo 94 della legge del 1984, quanto il loro utilizzo da parte di detti servizi rientrano nell'ambito di applicazione di tale direttiva, sia che detti dati vengano raccolti mediante trasmissione effettuata in differita sia che essi lo siano in tempo reale. In particolare, il fatto che l'obiettivo di tutela della sicurezza nazionale sia espressamente elencato all'articolo 15, paragrafo 1, di detta direttiva non avrebbe come conseguenza l'inapplicabilità di quest'ultima a situazioni del genere, e l'articolo 4, paragrafo 2, TUE non inciderebbe su tale valutazione.

32 Per contro, i governi del Regno Unito, ceco ed estone, l'Irlanda nonché i governi francese, cipriota, ungherese, polacco e svedese sostengono sostanzialmente che la direttiva 2002/58 non trova applicazione nei confronti della normativa nazionale controversa nel procedimento principale, in quanto quest'ultima ha come finalità la salvaguardia della sicurezza nazionale. Le attività dei servizi di sicurezza e di intelligence rientrerebbero nelle funzioni essenziali degli Stati membri, attinenti al mantenimento dell'ordine pubblico nonché alla salvaguardia della sicurezza interna e dell'integrità territoriale e, di conseguenza, sarebbero di esclusiva competenza di questi ultimi, come testimonierebbe, in particolare, l'articolo 4, paragrafo 2, terza frase, TUE.

33 Secondo tali governi, la direttiva 2002/58 non potrebbe quindi essere interpretata nel senso che misure nazionali dirette alla salvaguardia della sicurezza nazionale rientrino nel suo ambito di applicazione. L'articolo 1, paragrafo 3, di tale direttiva delimiterebbe tale ambito di applicazione e ne escluderebbe, così come prevedeva già l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, le attività riguardanti la pubblica sicurezza, la difesa e la sicurezza dello Stato. Tali disposizioni rispecchierebbero la ripartizione delle competenze previste all'articolo 4, paragrafo 2, TUE e sarebbero private di effetto utile se misure rientranti nel settore della sicurezza nazionale dovessero rispettare le prescrizioni della direttiva 2002/58. Inoltre, la giurisprudenza della Corte risultante dalla sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346), che verte sull'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, sarebbe trasponibile all'articolo 1, paragrafo 3, della direttiva 2002/58.

34 A questo proposito, si deve rilevare che, ai sensi del suo articolo 1, paragrafo 1, la direttiva 2002/58 prevede, in particolare, 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, per quanto riguarda il trattamento dei dati personali nel settore delle comunicazioni elettroniche.

35 L'articolo 1, paragrafo 3, di tale direttiva esclude dall'ambito di applicazione di quest'ultima le «attività dello Stato» nei settori ivi indicati, tra le quali figurano le attività nel settore del diritto penale nonché quelle riguardanti la sicurezza pubblica, la difesa e la sicurezza dello Stato, compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato. Le attività

così menzionate a titolo esemplificativo sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 32 e giurisprudenza citata).

36 Inoltre, l'articolo 3 della direttiva 2002/58 enuncia che detta direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell'Unione, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati (in prosieguo: i «servizi di comunicazione elettronica»). Pertanto, la citata direttiva deve essere considerata come disciplinante le attività dei fornitori di tali servizi (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 33 e giurisprudenza citata).

37 In tale contesto, l'articolo 15, paragrafo 1, della direttiva 2002/58 autorizza gli Stati membri ad adottare, nel rispetto delle condizioni da esso previste, «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 [citata] direttiva» (sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 71).

38 Orbene, l'articolo 15, paragrafo 1, della direttiva 2002/58 presuppone necessariamente che le misure legislative nazionali ivi indicate rientrino nell'ambito di applicazione della suddetta direttiva, poiché quest'ultima autorizza espressamente gli Stati membri ad adottarle solamente nel rispetto delle condizioni che essa prevede. Inoltre, tali misure disciplinano, per le finalità menzionate in tale disposizione, l'attività dei fornitori di servizi di comunicazione elettronica (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 34 e giurisprudenza citata).

39 È in particolare alla luce di queste considerazioni che la Corte ha dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto in combinato disposto con l'articolo 3 di quest'ultima, deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale direttiva non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa che imponga loro di accordare alle autorità nazionali competenti l'accesso a tali dati. Infatti, misure legislative del genere implicano necessariamente un trattamento, da parte dei fornitori suddetti, di questi dati e, nei limiti in cui disciplinano le attività degli stessi fornitori, non possono essere equiparate ad attività proprie degli Stati, di cui all'articolo 1, paragrafo 3, di detta direttiva (v., in questo senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 35 e 37 nonché giurisprudenza citata).

40 Per quanto riguarda una misura legislativa come l'articolo 94 della legge del 1984, sul fondamento del quale l'autorità competente può dare ai fornitori di servizi di comunicazione elettronica l'ordine di comunicare mediante trasmissione dati in massa ai servizi di sicurezza e di intelligence, si deve rilevare che, in forza della definizione figurante all'articolo 4, punto 2, del regolamento 2016/679, la quale è applicabile conformemente all'articolo 2 della direttiva 2002/58, letto in combinato disposto con l'articolo 94, paragrafo 2, di detto regolamento, la nozione di «trattamento dei dati personali» designa «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, (...), la conservazione, (...), la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione (...)».

41 Ne consegue che una comunicazione di dati personali mediante trasmissione, così come una conservazione di dati o qualsiasi altra forma di messa a disposizione, configura un trattamento, ai sensi dell'articolo 3 della direttiva 2002/58, e, di conseguenza, rientra nell'ambito di applicazione di tale direttiva (v., in questo senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 45).

42 Inoltre, tenuto conto delle considerazioni di cui al punto 38 della presente sentenza e dell'economia generale della direttiva 2002/58, un'interpretazione di tale direttiva secondo la quale le misure legislative contemplate dall'articolo 15, paragrafo 1, sarebbero escluse dall'ambito di applicazione di detta direttiva in quanto le finalità che tali misure devono soddisfare coincidono sostanzialmente con le finalità perseguite dalle attività contemplate dall'articolo 1, paragrafo 3, della medesima direttiva, priverebbe tale articolo 15, paragrafo 1, di qualsiasi effetto utile (v., in questo senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 72 e 73).

43 La nozione di «attività» contenuta all'articolo 1, paragrafo 3, della direttiva 2002/58 non può quindi essere interpretata, come ha sostanzialmente rilevato l'avvocato generale al paragrafo 75 delle sue conclusioni nelle cause riunite La Quadrature du Net e a. (C-511/18 e C-512/18, EU:C:2020:6), alle quali egli rinvia al paragrafo 24 delle sue conclusioni nella presente causa, nel senso che ricomprende le misure legislative di cui all'articolo 15, paragrafo 1, di tale direttiva.

44 Le disposizioni dell'articolo 4, paragrafo 2, TUE, alle quali hanno fatto riferimento i governi menzionati al punto 32 della presente sentenza, non possono infirmare questa conclusione. Infatti, conformemente alla costante giurisprudenza della Corte, sebbene spetti agli Stati membri definire i loro interessi essenziali in materia di sicurezza e decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una misura nazionale sia stata adottata ai fini della tutela della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto [v., in questo senso, sentenze del 4 giugno 2013, ZZ, C-300/11, EU:C:2013:363, punto 38 e giurisprudenza citata; del 20 marzo 2018, Commissione/Austria (Tipografia di Stato), C-187/16, EU:C:2018:194, punti 75 e 76, nonché del 2 aprile 2020, Commissione/Polonia, Ungheria e Repubblica ceca (Meccanismo temporaneo di ricollocazione di richiedenti protezione internazionale), C-715/17, C-718/17 e C-719/17, EU:C:2020:257, punti 143 e 170].

45 Vero è che, nella sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punti da 56 a 59), la Corte ha dichiarato che il trasferimento di dati personali da parte di compagnie aeree ad autorità pubbliche di uno Stato terzo a fini di prevenzione nonché di lotta contro il terrorismo ed altri reati gravi esulava, in forza dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, dall'ambito di applicazione di tale direttiva, poiché un siffatto trasferimento rientrava in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza.

46 Tuttavia, alla luce delle considerazioni contenute ai punti 36, 38 e 39 della presente sentenza, tale giurisprudenza non è trasponibile all'interpretazione dell'articolo 1, paragrafo 3, della direttiva 2002/58. Infatti, come ha sostanzialmente rilevato l'avvocato generale ai paragrafi da 70 a 72 delle sue conclusioni nelle cause riunite La Quadrature du Net e a. (C-511/18 e C-512/18, EU:C:2020:6), l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, al quale si riferisce detta giurisprudenza, escludeva dall'ambito di applicazione di quest'ultima direttiva, in maniera generale, i «trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato», senza operare alcuna distinzione in relazione all'autore del trattamento di dati interessato. Per contro, nel contesto dell'interpretazione dell'articolo 1, paragrafo 3, della direttiva 2002/58, una siffatta distinzione si rivela necessaria. Infatti, come risulta dai punti da 37 a 39 e 42 della presente sentenza, l'insieme dei trattamenti di dati personali effettuati dai fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione di detta direttiva, ivi compresi i trattamenti derivanti da obblighi loro imposti dai pubblici poteri, mentre questi ultimi trattamenti potevano, eventualmente, rientrare nell'ambito di applicazione dell'eccezione prevista all'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, tenuto conto della formulazione più ampia di tale disposizione, riguardante l'insieme dei trattamenti, a prescindere dal loro autore, aventi ad oggetto la pubblica sicurezza, la difesa o la sicurezza dello Stato.

47 Inoltre, si deve rilevare che la direttiva 95/46, controversa nella causa che ha dato luogo alla sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346), è stata, in forza dell'articolo 94, paragrafo 1, del regolamento 2016/679, abrogata e sostituita da quest'ultimo, a decorrere dal 25 maggio 2018. Orbene, se è vero che detto regolamento precisa, all'articolo 2, paragrafo 2, lettera d), che esso non si applica ai trattamenti effettuati «dalle autorità competenti» a fini, in particolare, di prevenzione e di accertamento di reati, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, risulta dall'articolo 23, paragrafo 1, lettere d) e h), dello stesso regolamento che i trattamenti di dati personali effettuati a questi stessi fini da privati rientrano nell'ambito di applicazione di quest'ultimo. Ne consegue che l'interpretazione dell'articolo 1, paragrafo 3, dell'articolo 3 e dell'articolo 15, paragrafo 1, della direttiva 2002/58 che precede è coerente con la delimitazione dell'ambito di applicazione del regolamento 2016/679 che tale direttiva completa e precisa.

48 Invece, quando gli Stati membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di servizi di tali comunicazioni, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della direttiva 2002/58 ma in quello del solo diritto nazionale, fatta salva l'applicazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89), cosicché le misure di cui trattasi debbono rispettare in particolare il diritto nazionale di rango costituzionale e le disposizioni della CEDU.

49 Alla luce delle considerazioni che precedono, occorre rispondere alla prima questione dichiarando che l'articolo 1, paragrafo 3, l'articolo 3 e l'articolo 15, paragrafo 1, della direttiva 2002/58, letti alla luce dell'articolo 4, paragrafo 2, TUE, devono essere interpretati nel senso che rientra nell'ambito di applicazione di tale direttiva una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere ai servizi di sicurezza e di intelligence dati relativi al traffico e dati relativi all'ubicazione ai fini della salvaguardia della sicurezza nazionale.

Sulla seconda questione

50 Con la sua seconda questione, il giudice del rinvio mira, in sostanza, a stabilire se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che osta ad una normativa nazionale che consente ad un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence.

51 In via preliminare, occorre ricordare che, secondo le informazioni contenute nella domanda di pronuncia pregiudiziale, l'articolo 94 della legge del 1984 autorizza il ministro ad imporre ai fornitori di servizi di comunicazione elettronica, mediante ordini, qualora lo ritenga necessario nell'interesse della sicurezza nazionale o delle relazioni con un governo estero, di trasmettere ai servizi di sicurezza e di intelligence i dati relativi alle comunicazioni in massa, compresi i dati relativi al traffico e i dati relativi all'ubicazione, nonché informazioni sui servizi utilizzati, ai sensi dell'articolo 21, paragrafi 4 e 6, della RIPA. Quest'ultima disposizione riguarda, tra l'altro, i dati necessari per identificare la fonte di una comunicazione e la destinazione di quest'ultima, per determinare la data, l'ora, la durata e il tipo della comunicazione, per identificare il materiale utilizzato nonché localizzare le apparecchiature terminali e le comunicazioni, dati tra i quali figurano, in particolare, il nominativo e l'indirizzo dell'utente, il numero di telefono di chi chiama e il numero chiamato, gli indirizzi IP della fonte e del destinatario della comunicazione nonché gli indirizzi dei siti Internet visitati.

52 Una siffatta comunicazione mediante trasmissione dei dati riguarda l'insieme degli utenti dei mezzi di comunicazione elettronica, senza che sia precisato se tale trasmissione debba intervenire in tempo reale o in differita. Una volta trasmessi, tali dati, secondo le informazioni contenute nella domanda di pronuncia pregiudiziale, sono conservati dai servizi di sicurezza e di intelligence e rimangono a disposizione di questi ultimi ai fini delle loro attività, così come le altre banche dati detenute da tali servizi. In particolare, i dati così raccolti, che sono sottoposti a trattamenti e ad analisi di massa e automatizzati, possono essere incrociati con altre banche dati contenenti varie categorie di dati personali in massa o essere divulgati all'esterno di tali servizi e a Stati terzi. Infine, tali operazioni non sono subordinate alla previa autorizzazione di un giudice o di un'autorità amministrativa indipendente e non danno luogo ad alcuna informativa nei confronti delle persone interessate.

53 La direttiva 2002/58 ha come finalità, come risulta segnatamente dai suoi considerando 6 e 7, di tutelare gli utenti dei servizi di comunicazione elettronica contro i pericoli per i loro dati personali e la loro vita privata derivanti dalle nuove tecnologie e, in particolare, dall'accresciuta capacità di memorizzazione e di trattamento automatizzati di dati. In particolare, detta direttiva mira, come enunciato al suo considerando 2, a garantire il pieno rispetto dei diritti sanciti dagli articoli 7 e 8 della Carta. A tale proposito, risulta dalla relazione della proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [COM (2000) 385 def.], all'origine della direttiva 2002/58, che il legislatore dell'Unione ha inteso «assicurare un elevato livello di tutela dei dati personali e della vita privata per tutti i servizi di comunicazione elettronica, indipendentemente dalla tecnologia da essi usata».

54 A tal fine, l'articolo 5, paragrafo 1, della direttiva 2002/58 dispone che «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». Nella stessa disposizione si sottolinea altresì che, «[i]n particolare, [gli Stati membri] 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», e si precisa che «[q]uesto paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza».

55 Pertanto, tale articolo 5, paragrafo 1, sancisce il principio di riservatezza sia delle comunicazioni elettroniche sia dei relativi dati sul traffico e implica, in particolare, il divieto imposto, in linea di principio, a qualunque soggetto diverso dagli utenti, di memorizzare, senza il consenso di questi ultimi, tali comunicazioni e tali dati. Alla luce del carattere generale della sua formulazione, tale disposizione si applica necessariamente a qualsiasi operazione che consenta a terzi di venire a conoscenza delle comunicazioni e dei dati ad esse relativi a fini diversi dalla trasmissione di una comunicazione.

56 Il divieto di intercettare le comunicazioni e i dati ad esse relativi, contenuto all'articolo 5, paragrafo 1, della direttiva 2002/58 ricomprende quindi qualsiasi forma di messa a disposizione, da parte dei fornitori di servizi di comunicazione elettronica, di dati relativi al traffico e di dati relativi all'ubicazione ad autorità pubbliche, come i servizi di sicurezza e di intelligence, nonché la conservazione di detti dati da parte di tali autorità, indipendentemente dal successivo utilizzo che ne venga fatto.

57 Pertanto, adottando tale direttiva, il legislatore dell'Unione ha concretizzato i diritti sanciti agli articoli 7 e 8 della Carta, in modo tale che gli utenti dei mezzi di comunicazione elettronica hanno diritto di attendersi, in linea di principio, che le loro comunicazioni e i relativi dati restino, senza il loro consenso, anonimi e non possano formare oggetto di registrazione (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 109).

58 Tuttavia, l'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio, sancito all'articolo 5, paragrafo 1, di tale direttiva, di garantire la riservatezza dei dati personali nonché agli obblighi corrispondenti, menzionati in particolare agli articoli 6 e 9 di detta direttiva, qualora una siffatta limitazione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica o per garantire la prevenzione, la ricerca, l'accertamento e il 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 qualora ciò sia giustificato da uno di tali motivi.

59 Stanti tali premesse, la facoltà di derogare ai diritti e agli obblighi previsti agli articoli 5, 6 e 9 della direttiva 2002/58 non può giustificare il fatto che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei relativi dati e, in particolare, al divieto di memorizzare tali dati, esplicitamente previsto all'articolo 5 di tale direttiva, diventi la regola (v., in questo senso, sentenze del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 89 e 104, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 111).

60 Inoltre, dall'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 risulta che gli Stati membri sono autorizzati ad adottare misure legislative dirette a limitare la portata dei diritti e degli obblighi contemplati agli articoli 5, 6 e 9 di tale direttiva solo nel rispetto dei principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e dei diritti fondamentali garantiti dalla Carta. Al riguardo, la Corte ha già dichiarato che l'obbligo imposto da uno Stato membro ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale, di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7 e 8 della Carta, relativi, rispettivamente, alla tutela della vita privata nonché alla tutela dei dati personali, ma anche dell'articolo 11 della Carta, relativo alla libertà di espressione (v., in questo senso, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 25 e 70, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 91 e 92 nonché giurisprudenza citata).

61 Le stesse questioni si pongono anche per gli altri tipi di trattamento di dati, come la loro trasmissione a soggetti diversi dagli utenti o l'accesso a tali dati ai fini del loro utilizzo [v., per analogia, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 122 e 123 e giurisprudenza citata].

62 Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 deve tener conto dell'importanza sia del diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto alla protezione dei dati personali, garantito dall'articolo 8 di quest'ultima, quale risulta dalla giurisprudenza della Corte, nonché del diritto alla libertà di espressione, dato che tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, e fa parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata (v., in questo senso, sentenze del 6 marzo 2001, Connolly/Commissione, C-274/99 P, EU:C:2001:127, punto 39, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 93 e giurisprudenza citata).

63 Tuttavia, 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 (v., in questo senso, sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 172 e giurisprudenza citata).

64 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 di detti diritti e, in ottemperanza al 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.

65 Occorre aggiungere che il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato (sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 175 e giurisprudenza citata).

66 Per quanto riguarda il rispetto del principio di proporzionalità, l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 dispone che gli Stati membri possono adottare una misura derogatoria al principio di riservatezza delle comunicazioni e dei dati relativi al traffico qualora una siffatta misura sia «necessaria, opportuna e proporzionata all'interno di una società democratica», alla luce degli obiettivi enunciati da tale disposizione. Il considerando 11 di tale direttiva precisa che una misura del genere dev'essere «strettamente» proporzionata allo scopo perseguito.

67 Al riguardo, occorre ricordare che la tutela del diritto fondamentale al rispetto della vita privata richiede, conformemente alla giurisprudenza costante della Corte, che le deroghe e le restrizioni alla tutela dei dati personali debbano operare 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 equilibrato contemperamento tra l'obiettivo e gli interessi e diritti in questione [v., in questo senso, sentenze del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, punto 56; del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punti 76, 77 e 86, nonché dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 52; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 140].

68 Per soddisfare al requisito di proporzionalità, una normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi. Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali 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 qualora i dati personali siano soggetti a trattamento automatico, in particolare qualora esista un rischio considerevole di accesso illecito ai dati stessi. Tali considerazioni valgono in particolare quando è in gioco la tutela della particolare categoria di dati personali costituita dai dati sensibili [v., in questo senso, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 54 e 55, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 117; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 141].

69 Per quanto riguarda la questione se una normativa nazionale, quale quella controversa nel procedimento principale, soddisfi i requisiti dell'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, occorre rilevare che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione a persone diverse dagli utenti, come i servizi di sicurezza e di intelligence, deroga al principio di riservatezza. Qualora tale operazione sia effettuata, come nel caso di specie, in maniera generalizzata e indifferenziata, essa ha l'effetto di trasformare in regola la deroga all'obbligo del principio di garantire la riservatezza dei dati, mentre il sistema istituito dalla direttiva 2002/58 richiede che tale deroga resti l'eccezione.

70 Inoltre, conformemente alla giurisprudenza costante della Corte, la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione ad un terzo costituisce un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, indipendentemente dal successivo utilizzo che venga fatto di tali dati. Al riguardo, poco importa che le informazioni relative alla vita privata interessate presentino o meno carattere sensibile o che gli interessati abbiano subito o meno eventuali inconvenienti a seguito di tale ingerenza [v., in questo senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126 nonché giurisprudenza citata, e sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punti 115 e 116].

71 L'ingerenza nel diritto fondamentale sancito dall'articolo 7 della Carta che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence comporta dev'essere considerata particolarmente grave, alla luce in particolare del carattere sensibile delle informazioni che possono fornire tali dati e, in particolare, della possibilità di stabilire, sulla base di questi ultimi, il profilo delle persone interessate, informazione, questa, tanto sensibile quanto il contenuto stesso delle comunicazioni. Inoltre, essa può ingenerare nelle persone interessate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua (v., per analogia, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 27 e 37, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 99 e 100).

72 Occorre rilevare altresì che una trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione ad autorità pubbliche a fini di sicurezza può, da sola, ledere il diritto al rispetto delle comunicazioni, sancito dall'articolo 7 della Carta, e comportare effetti dissuasivi sull'esercizio, da parte degli utenti dei mezzi di comunicazione elettronica, della loro libertà d'espressione, garantita dall'articolo 11 della Carta. Siffatti effetti dissuasivi possono incidere, in particolare, sulle persone le cui comunicazioni sono soggette, ai sensi delle norme nazionali, al segreto professionale nonché sugli informatori le cui attività sono tutelate dalla direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (GU 2019, L 305, pag. 17). Inoltre, tali effetti sono tanto più gravi in quanto il numero e la varietà dei dati conservati sono elevati (v., in questo senso, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 28; del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 101, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 118).

73 Infine, tenuto conto del rilevante quantitativo di dati relativi al traffico e di dati relativi all'ubicazione che possono essere conservati in maniera continua attraverso una misura di conservazione generalizzata nonché del carattere sensibile delle informazioni ricavabili da tali dati, la sola conservazione di detti dati da parte dei fornitori di servizi di comunicazione elettronica comporta rischi di abusi e di accesso illecito.

74 Quanto agli obiettivi che possono giustificare siffatte ingerenze, più in particolare quanto all'obiettivo di salvaguardia della sicurezza nazionale, controverso nel procedimento principale, si deve rilevare, anzitutto, che l'articolo 4, paragrafo 2, TUE stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Tale responsabilità corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprende la prevenzione e la repressione di attività che possono destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese e, in particolare, minacciare direttamente la società, la popolazione o lo Stato in quanto tale, come specialmente le attività terroristiche (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 135).

75 Orbene, l'importanza dell'obiettivo di salvaguardia della sicurezza nazionale, letto alla luce dell'articolo 4, paragrafo 2, TUE, supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, in particolare degli obiettivi di lotta alla criminalità in generale, anche grave, nonché di salvaguardia della pubblica sicurezza. Infatti, minacce come quelle considerate al punto

precedente si distinguono, per la loro natura e per la loro particolare gravità, dal rischio generale di insorgenza di tensioni o di problemi, anche gravi, per la pubblica sicurezza. Fatto salvo il rispetto delle altre condizioni previste dall'articolo 52, paragrafo 1, della Carta, l'obiettivo di salvaguardia della sicurezza nazionale è pertanto tale da giustificare misure comportanti ingerenze nei diritti fondamentali più gravi di quelle che potrebbero essere giustificate da tali altri obiettivi (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 136).

76 Tuttavia, per rispondere all'obbligo di proporzionalità ricordato al punto 67 della presente sentenza, secondo il quale le deroghe e le restrizioni alla tutela dei dati personali debbono operare nei limiti dello stretto necessario, una normativa nazionale comportante un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta deve rispettare gli obiettivi derivanti dalla giurisprudenza citata ai punti 65, 67 e 68 della presente sentenza.

77 In particolare, per quanto riguarda l'accesso di un'autorità a dati personali, una normativa non può limitarsi ad esigere che l'accesso ai dati da parte delle autorità risponda alla finalità perseguita da tale normativa, ma essa deve altresì prevedere le condizioni sostanziali e procedurali che disciplinano tale utilizzo [v., per analogia, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 192 e giurisprudenza citata].

78 Pertanto, dato che un accesso generale a tutti i dati conservati, in mancanza di qualunque nesso, anche indiretto, con la finalità perseguita, non può essere considerato limitato allo stretto necessario, una normativa nazionale che disciplina l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in cui dev'essere concesso alle autorità nazionali competenti l'accesso ai dati di cui trattasi (v., in questo senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 119 e giurisprudenza citata).

79 Tali requisiti si applicano, a fortiori, ad una misura legislativa, come quella controversa nel procedimento principale, sul fondamento della quale l'autorità nazionale competente può imporre ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence. Infatti, una siffatta trasmissione ha l'effetto di mettere tali dati a disposizione delle autorità pubbliche [v., per analogia, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 212].

80 Dato che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione avviene in maniera generalizzata e indifferenziata, essa riguarda in maniera globale l'insieme delle persone che fanno uso dei sistemi di comunicazione elettronica. Essa si applica quindi anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o remoto, con l'obiettivo di salvaguardia della sicurezza nazionale e, in particolare, senza che sia accertata una correlazione tra i dati di cui è prevista la trasmissione e una minaccia per la sicurezza nazionale (v., in questo senso, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 57 e 58, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 105). Tenuto conto del fatto che la trasmissione di tali dati alle autorità pubbliche equivale, conformemente a quanto è stato constatato al punto 79 della presente sentenza, ad un accesso, si deve ritenere che una normativa che consente una trasmissione generalizzata e indifferenziata dei dati alle autorità pubbliche implichi un accesso generale.

81 Ne consegue che una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence eccede i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come richiesto dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta.

82 Tenuto conto di tutte le considerazioni che precedono, occorre rispondere alla seconda questione dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, dev'essere interpretato nel senso che osta ad una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence.

Sulle spese

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

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

1) **L'articolo 1, paragrafo 3, l'articolo 3 e 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, letti alla luce dell'articolo 4, paragrafo 2, TUE, devono essere interpretati nel senso che rientra nell'ambito di applicazione di tale direttiva una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere ai servizi di sicurezza e di intelligence dati relativi al traffico e dati relativi all'ubicazione ai fini della salvaguardia della sicurezza nazionale.**

2) **L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, dev'essere interpretato nel senso che osta ad una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence.**

Firme