СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

SENTENZA DELLA CORTE (Grande Sezione)

21 dicembre 2016 *

«Rinvio pregiudiziale – Comunicazioni elettroniche – Trattamento dei dati personali – Riservatezza delle comunicazioni elettroniche – Tutela – Direttiva 2002/58/CE – Articoli 5, 6 e 9, nonché articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11, nonché articolo 52, paragrafo 1 – Normativa nazionale – Fornitori di servizi di comunicazione elettronica – Obbligo riguardante la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Autorità nazionali – Accesso ai dati – Assenza di controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente – Compatibilità con il diritto dell'Unione»

Nelle cause riunite C-203/15 e C-698/15,

aventi ad oggetto alcune domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 TFUE, dal Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile), Regno Unito], mediante decisioni in data, rispettivamente, 29 aprile 2015 e 9 dicembre 2015, pervenute in cancelleria il 4 maggio 2015 ed il 28 dicembre 2015, nei procedimenti

Tele2 Sverige AB (C-203/15)

contro

Post- och telestyrelsen,

* Lingue processuali: lo svedese e l'inglese.

IT

e

Secretary of State for the Home Department (C-698/15)

contro

Tom Watson,

Peter Brice,

Geoffrey Lewis,

con l'intervento di:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, A. Tizzano, vicepresidente, R. Silva de Lapuerta, T. von Danwitz (relatore), J. L. da Cruz Vilaça, E. Juhász e M. Vilaras, presidenti di sezione, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen e C. Lycourgos, giudici,

avvocato generale: H. Saugmandsgaard Øe

cancelliere: C. Strömholm, amministratore

vista la decisione del presidente della Corte in data 1° febbraio 2016 di trattare la causa C-698/15 secondo il procedimento accelerato previsto dall'articolo 105, paragrafo 1, del regolamento di procedura della Corte,

vista la fase scritta del procedimento e in seguito all'udienza del 12 aprile 2016,

considerate le osservazioni presentate:

– per la Tele2 Sverige AB, da M. Johansson e N. Torgerzon, advokater, nonché da E. Lagerlöf e S. Backman;

– per T. Watson, da J. Welch ed E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, nonché da D. Rose, QC;

– per P. Brice e G. Lewis, da A. Suterwalla e R. de Mello, barristers, R. Drabble, QC, nonché da S. Luke, solicitor;

– per Open Rights Group e Privacy International, da D. Carey, solicitor, nonché da R. Mehta e J. Simor, barristers;

– per The Law Society of England and Wales, da T. Hickman, barrister, nonché da N. Turner;

– per il governo svedese, da A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren e L. Swedenborg, in qualità di agenti;

– per il governo del Regno Unito, da S. Brandon, L. Christie e V. Kaye, in qualità di agenti, assistiti da D. Beard, G. Facenna e J. Eadie, QC, nonché da S. Ford, barrister;

– per il governo belga, da J.-C. Halleux, S. Vanrie e C. Pochet, in qualità di agenti;

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

– per il governo danese, da C. Thorning e M. Wolff, in qualità di agenti;

– per il governo tedesco, da T. Henze, M. Hellmann e J. Kemper, in qualità di agenti, assistiti da M. Kottmann e U. Karpenstein, Rechtsanwälte;

– per il governo estone, da K. Kraavi-Käerdi, in qualità di agente;

– per l'Irlanda, da E. Creedon, L. Williams e A. Joyce, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo spagnolo, da A. Rubio González, in qualità di agente;

– per il governo francese, da G. de Bergues, D. Colas, F.-X. Bréchot e C. David, in qualità di agenti;

– per il governo cipriota, da K. Kleanthous, in qualità di agente;

– per il governo ungherese, da M. Fehér e G. Koós, in qualità di agenti;

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

– per il governo polacco, da B. Majczyna, in qualità di agente;

– per il governo finlandese, da J. Heliskoski, in qualità di agente;

– per la Commissione europea, da H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira e J. Vondung, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 19 luglio 2016,

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 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 Tali domande sono state presentate nell'ambito di due controversie, la prima delle quali vede la Tele2 Sverige AB contrapporsi alla Post- och telestyrelsen (autorità svedese di sorveglianza delle poste e delle telecomunicazioni; in prosieguo: la «PTS»), in merito ad un'ingiunzione con cui quest'ultima ha ordinato alla Tele2 Sverige di procedere alla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione dei suoi abbonati ed utenti iscritti (causa C-203/15), mentre la seconda oppone i sigg. Tom Watson, Peter Brice e Geoffrey Lewis al Secretary of State for the Home Department (Ministro dell'Interno, Regno Unito di Gran Bretagna e Irlanda del Nord), in merito alla conformità al diritto dell'Unione dell'articolo 1 del Data Retention and Investigatory Powers Act 2014 (legge del 2014 sulla conservazione dei dati e sui poteri di indagine; in prosieguo: la «DRIPA») (causa C-698/15).

Contesto normativo

Diritto dell'Unione

Direttiva 2002/58

3 I considerando 2, 6, 7, 11, 21, 22, 26 e 30 della direttiva 2002/58 enunciano quanto segue:

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

(...)

(11) La presente direttiva, analogamente alla direttiva 95/46/CE [del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31)], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto 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, 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.

(...)

(21) Occorre prendere misure per prevenire l'accesso non autorizzato alle comunicazioni al fine di tutelare la riservatezza delle comunicazioni realizzate attraverso reti pubbliche di comunicazione e servizi di comunicazione elettronica accessibili al pubblico[,] compreso il loro contenuto e qualsiasi dato ad esse relativo. La legislazione di alcuni Stati membri vieta soltanto l'accesso intenzionale non autorizzato alle comunicazioni.

(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. (...)

(...)

(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. (...)

(...)

(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. (...)».

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

«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 che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale».

5 L'articolo 2 della direttiva 2002/58, intitolato «Definizioni», recita:

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

Si applicano inoltre le seguenti definizioni:

(...)

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

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

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

(...)».

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

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

7 L’articolo 4 di detta direttiva, intitolato «Sicurezza del trattamento», è così formulato:

«1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente.

1 bis. Fatta salva la direttiva [95/46], le misure di cui al paragrafo 1 quanto meno:

– garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati,

– tutelano i dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, e

– garantiscono l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali.

(...)».

8 L'articolo 5 della direttiva 2002/58, intitolato «Riservatezza delle comunicazioni», ha il seguente tenore:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite [una] 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, intitolato «Dati sul traffico», dispone quanto segue:

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

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

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

(...)

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

10 L'articolo 9 della medesima direttiva, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», prevede, al paragrafo 1, quanto segue:

«Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. (...)».

11 L'articolo 15 della citata direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», enuncia quanto segue:

«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 comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.

(...)

1 ter. I fornitori istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti sulla base delle disposizioni nazionali adottate a norma del paragrafo 1. Su richiesta, forniscono alla competente autorità nazionale informazioni su dette procedure, sul numero di richieste ricevute, sui motivi legali addotti e sulla loro risposta.

2. Le disposizioni del capo III della direttiva [95/46] relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

(...)».

Direttiva 95/46

12 L'articolo 22 della direttiva 95/46, contenuto nel capo III di quest'ultima, è formulato nei seguenti termini:

«Fatti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all'autorità di controllo di cui all'articolo 28, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione».

Direttiva 2006/24/CE

13 L'articolo 1 della 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), intitolato «Oggetto e campo d'applicazione», prevedeva, al paragrafo 2, quanto segue:

«La presente direttiva si applica ai dati relativi al traffico e ai dati relativi all'ubicazione delle persone sia fisiche che giuridiche, e ai dati connessi necessari per identificare l'abbonato o l'utente registrato. Non si applica al contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche».

14 Ai sensi dell'articolo 3 della medesima direttiva, intitolato «Obbligo di conservazione dei dati»:

1. In deroga agli articoli 5, 6 e 9 della direttiva [2002/58], gli Stati membri adottano misure per garantire che i dati di cui all'articolo 5 della presente direttiva, qualora siano generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati, da fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione nell'ambito della loro giurisdizione, siano conservati conformemente alle disposizioni della presente direttiva.

2. L'obbligo di conservazione stabilito al paragrafo 1 comprende la conservazione dei dati specificati all'articolo 5 relativi ai tentativi di chiamata non riusciti dove tali dati vengono generati o trattati e immagazzinati (per quanto riguarda i dati telefonici) oppure trasmessi (per quanto riguarda i dati Internet) da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione nell'ambito della giurisdizione dello Stato membro interessato nel processo di fornire i servizi di comunicazione interessati. La presente direttiva non richiede la conservazione dei dati per quanto riguarda le chiamate non collegate».

Diritto svedese

15 Risulta dalla decisione di rinvio nella causa C-203/15 che il legislatore svedese, al fine di trasporre la direttiva 2006/24 nell'ordinamento nazionale, ha modificato la lagen (2003:389) om elektronisk kommunikation [legge (2003:389) sulle comunicazioni elettroniche; in prosieguo: la «LEK»] e il förordningen (2003:396) om elektronisk kommunikation [regolamento (2003:396) sulle comunicazioni elettroniche]. Tali testi normativi contengono entrambi, nella versione applicabile nel procedimento principale, norme sulla conservazione dei dati relativi alle comunicazioni elettroniche nonché sull'accesso a tali dati da parte delle autorità nazionali.

16 L'accesso ai dati suddetti è inoltre disciplinato dalla lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande

myndigheternas underrättelseverksamhet [legge (2012:278) sulla comunicazione di dati relativi alle comunicazioni elettroniche nell'ambito delle attività di informazione delle autorità di repressione degli illeciti; in prosieguo: la «legge 2012:278»], nonché dal rättegångsbalken (codice dei procedimenti giurisdizionali; in prosieguo: il «RB»).

Sull'obbligo di conservazione dei dati relativi alle comunicazioni elettroniche

17 Secondo le indicazioni del giudice del rinvio nella causa C-203/15, le disposizioni di cui all'articolo 16 a del capo 6 della LEK, lette in combinato disposto con l'articolo 1 del capo 2 della medesima legge, prevedono un obbligo per i fornitori di servizi di comunicazione elettronica di conservare i dati la cui conservazione era prevista dalla direttiva 2006/24. Si tratta dei dati relativi agli abbonamenti e a tutte le comunicazioni elettroniche necessari per rintracciare e identificare la fonte e la destinazione di una comunicazione, per determinarne la data, l'ora, la durata e la natura, per identificare lo strumento di comunicazione utilizzato, nonché per localizzare le apparecchiature di comunicazione mobile utilizzate all'inizio e alla fine della comunicazione. L'obbligo di conservazione dei dati riguarda i dati generati o trattati nell'ambito di un servizio di telefonia, di un servizio di telefonia tramite un punto di connessione mobile, di un sistema di messaggeria elettronica, di un servizio di accesso a Internet, nonché di un servizio di fornitura di capacità di accesso a Internet (modalità di connessione). Tale obbligo include altresì i dati relativi alle comunicazioni non riuscite. Esso non riguarda però il contenuto delle comunicazioni.

18 Gli articoli da 38 a 43 del regolamento (2003:396) sulle comunicazioni elettroniche precisano le categorie di dati che devono essere conservati. Riguardo ai servizi di telefonia, devono in particolare essere conservati i dati relativi alle chiamate e ai numeri chiamati nonché le date e le ore tracciabili di inizio e fine delle comunicazioni. Riguardo ai servizi di telefonia tramite un punto di connessione mobile, vengono imposti obblighi supplementari come, ad esempio, la conservazione dei dati relativi all'ubicazione dei luoghi di inizio e di fine della comunicazione. Riguardo ai servizi di telefonia che utilizzano un pacchetto IP, devono in particolare essere conservati, oltre ai dati sopra menzionati, quelli relativi agli indirizzi IP del chiamante e del chiamato. Riguardo ai sistemi di messaggeria elettronica, devono essere conservati, in particolare, i dati relativi ai numeri degli emittenti e dei destinatari, gli indirizzi IP ovvero qualsiasi altro indirizzo di messaggeria. Riguardo ai servizi di accesso a Internet, devono ad esempio essere conservati i dati relativi agli indirizzi IP degli utenti, nonché le date e le ore tracciabili di connessione e di disconnessione al servizio di accesso a Internet.

Sulla durata di conservazione dei dati

19 A norma dell'articolo 16 d del capo 6 della LEK, i dati contemplati all'articolo 16 a di questo capo devono essere conservati dai fornitori di servizi di comunicazione elettronica per un periodo di sei mesi a partire dal giorno della fine della comunicazione. Essi devono poi essere immediatamente distrutti, salvo contrarie disposizioni previste dall'articolo 16 d, secondo comma, del capo suddetto.

Sull'accesso ai dati conservati

20 L'accesso da parte delle autorità nazionali ai dati conservati è disciplinato dalle disposizioni della legge 2012:278, della LEK e del RB.

– La legge 2012:278

21 Nell'ambito delle attività di informazione, la polizia nazionale, la Säkerhetspolisen (polizia di sicurezza, Svezia) e la Tullverket (amministrazione delle dogane, Svezia) possono, sulla base dell'articolo 1 della legge 2012:278, alle condizioni prescritte da tale legge e all'insaputa del fornitore di una rete elettronica di comunicazioni o di un servizio di comunicazione elettronica autorizzato in applicazione della LEK, procedere alla raccolta di dati relativi ai messaggi trasmessi in una rete di comunicazioni elettroniche, agli strumenti di comunicazione elettronica che si trovano in una determinata zona geografica, nonché alla zona o alle zone geografiche in cui si trova o si trovava uno strumento di comunicazione elettronica.

22 Conformemente agli articoli 2 e 3 della legge 2012:278, i dati possono, in linea di principio, essere raccolti nel caso in cui, sulla base delle circostanze, la misura risulti particolarmente necessaria per prevenire, impedire o accertare un'attività criminale implicante una o più violazioni punite con una pena detentiva di almeno due anni, ovvero uno degli atti elencati all'articolo 3 della medesima legge comprendente violazioni punite con una pena detentiva inferiore a due anni. Le motivazioni che fondano tale misura devono prevalere sulle considerazioni relative alla lesione o al pregiudizio che essa comporta per la persona che ne è destinataria o per un interesse che si oppone ad essa. Conformemente all'articolo 5 della legge suddetta, la durata della misura non deve eccedere un mese.

23 La decisione di mettere in atto una misura siffatta compete al direttore dell'autorità interessata ovvero ad una persona delegata a tal fine. Essa non è sottoposta al controllo preventivo di un'autorità giurisdizionale o di un'autorità amministrativa indipendente.

24 In virtù dell'articolo 6 della legge 2012:278, la Säkerhets och integritetsskyddsnämnden (commissione per la sicurezza e la tutela dell'integrità, Svezia) deve essere informata di qualsiasi decisione che autorizzi la raccolta di dati. Conformemente all'articolo 1 della lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [legge (2007:980) relativa al controllo di talune attività repressive], detta autorità esercita una vigilanza sull'applicazione della legge da parte delle autorità sanzionatorie.

– La LEK

25 In virtù dell'articolo 22, primo comma, punto 2, del capo 6 della LEK, qualsiasi fornitore di servizi di comunicazione elettronica deve fornire i dati relativi ad un abbonamento su richiesta di un pubblico ministero, della polizia nazionale, della polizia di sicurezza o di qualsiasi altra autorità pubblica incaricata della repressione degli illeciti, qualora tali dati si riferiscano ad una presunta violazione. Secondo le indicazioni del giudice del rinvio nella causa C-203/15, non è necessario che si tratti di una violazione grave.

– Il RB

26 Il RB disciplina la comunicazione dei dati conservati alle autorità nazionali nell'ambito di indagini preliminari. Conformemente all'articolo 19 del capo 27 del RB, la «messa sotto sorveglianza di comunicazioni elettroniche» all'insaputa di soggetti terzi è, in linea di principio, autorizzata nell'ambito di indagini preliminari aventi ad oggetto, in particolare, violazioni sanzionate con una pena detentiva di almeno sei mesi. Per «messa sotto sorveglianza di comunicazioni elettroniche» occorre intendere, a norma dell'articolo 19 del capo 27 del RB, l'acquisizione di dati all'insaputa di soggetti terzi relativi ad un messaggio trasmesso tramite una rete di comunicazioni elettroniche, agli strumenti di comunicazione elettronica che si trovano o si trovavano in una zona geografica determinata, nonché alla zona o alle zone geografiche in cui un determinato strumento di comunicazione elettronica si trova o si trovava.

27 Secondo le indicazioni del giudice del rinvio nella causa C-203/15, non è possibile ottenere informazioni sul contenuto di un messaggio sulla base dell'articolo 19 del capo 27 del RB. In linea di principio, la messa sotto sorveglianza di comunicazioni elettroniche può essere ordinata, a norma dell'articolo 20 del capo 27 del RB, soltanto in presenza di indizi plausibili che consentano di sospettare che una persona sia l'autore di una violazione e che la misura sia particolarmente necessaria per le necessità dell'indagine, con la precisazione che quest'ultima deve altresì vertere su una violazione punita con una pena detentiva di almeno due anni ovvero sul tentativo, sulla preparazione o sull'intesa delittuosa finalizzati a commettere una violazione siffatta. Conformemente all'articolo 21 del capo 27 del RB, il pubblico ministero che procede deve, tranne nei casi di urgenza, chiedere al

giudice competente l'autorizzazione a procedere alla messa sotto sorveglianza di comunicazioni elettroniche.

Sulla sicurezza e sulla protezione dei dati conservati

28 A norma dell'articolo 3 a del capo 6 della LEK, i fornitori di servizi di comunicazione elettronica onerati da un obbligo di conservazione dei dati devono adottare le misure di ordine tecnico e organizzativo appropriate per garantire la protezione dei dati nell'ambito del loro trattamento. Secondo le indicazioni del giudice del rinvio nella causa C-203/15, il diritto svedese non prevede però alcuna disposizione in merito al luogo di conservazione dei dati.

Diritto del Regno Unito

La DRIPA

29 L'articolo 1 della DRIPA, intitolato «Poteri in materia di conservazione dei dati relativi a comunicazioni rilevanti, con previsione di garanzie», dispone quanto segue:

«(1) Il [Ministro dell'Interno] può, tramite un avviso (l'"avviso di conservazione"), imporre a un operatore di telecomunicazioni pubbliche di conservare dati rilevanti relativi a comunicazioni, qualora ritenga che tale prescrizione sia necessaria e proporzionata rispetto ad una o più tra le finalità previste ai punti da a) ad h) dell'articolo 22, paragrafo 2, del Regulation of Investigatory Powers Act 2000 [legge del 2000 recante disciplina dei poteri di indagine] (finalità per le quali possono essere acquisiti i dati relativi a comunicazioni).

(2) Un avviso di conservazione può:

(a) riguardare un particolare operatore o qualsiasi categoria di operatori;

(b) imporre la conservazione di tutti i dati o di qualsiasi categoria di dati;

(c) indicare il periodo o i periodi di tempo durante i quali i dati devono essere conservati;

(d) stabilire ulteriori prescrizioni, ovvero restrizioni, in relazione alla conservazione dei dati;

(e) fissare differenti disposizioni per finalità differenti;

(f) riguardare dati che siano o no esistenti al momento dell'emissione, o dell'entrata in vigore, dell'avviso.

(3) Il [Ministro dell'Interno] può, tramite regolamenti, fissare ulteriori disposizioni in relazione alla conservazione di dati rilevanti relativi alle comunicazioni.

(4) Tali disposizioni possono, in particolare, riguardare:

(a) prescrizioni antecedenti all'emissione di un avviso di conservazione;

(b) il periodo di tempo massimo durante il quale i dati devono essere conservati in applicazione di un avviso di conservazione;

(c) il contenuto, l'emissione, l'entrata in vigore, il riesame, la modifica o la revoca di un avviso di conservazione;

(d) l'integrità, la sicurezza o la protezione dei dati conservati ai sensi del presente articolo, l'accesso agli stessi, o la loro pubblicità o distruzione;

(e) la messa ad esecuzione di prescrizioni o restrizioni rilevanti, o la verifica dell'ottemperanza alle stesse;

(f) un codice di condotta relativo alle prescrizioni, alle restrizioni o ai poteri rilevanti;

(g) il rimborso da parte del [Ministro dell'Interno] (subordinato o no a condizioni) delle spese sostenute dagli operatori di telecomunicazioni pubbliche per ottemperare alle prescrizioni o alle restrizioni rilevanti;

(h) la cessazione dell'efficacia del [Data Retention (EC Directive) Regulations 2009 (regolamento del 2009 concernente la conservazione dei dati ai sensi della direttiva CE)] e il passaggio alla conservazione dei dati ai sensi del presente articolo.

(5) Il periodo di tempo massimo previsto ai sensi del paragrafo 4, lettera b), non deve eccedere i 12 mesi a partire dal giorno indicato in relazione ai dati di cui trattasi dai regolamenti contemplati dal paragrafo 3.

(...)».

30 L'articolo 2 della DRIPA definisce l'espressione «dati rilevanti relativi a comunicazioni» come riguardante i «dati rilevanti relativi a comunicazioni del tipo di quelli menzionati nell'allegato del regolamento del 2009 concernente la conservazione dei dati ai sensi della direttiva CE, purché tali dati siano generati o trattati nel Regno Unito da operatori di telecomunicazioni pubbliche, nell'ambito della fornitura dei servizi di telecomunicazione in questione».

La RIPA

31 L'articolo 21 della legge del 2000 recante disciplina dei poteri di indagine (in prosieguo: la «RIPA»), contenuto nel capo II di tale legge e intitolato «Acquisizione e divulgazione dei dati relativi a comunicazioni», precisa, al paragrafo 4, quanto segue:

«Nel presente capo, l'espressione "dati relativi a comunicazioni" può avere tutti i 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 servizio postale o di qualsiasi sistema di telecomunicazione tramite il quale la comunicazione viene trasmessa o può 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 qualunque soggetto:

(i) di qualsiasi servizio postale o servizio di telecomunicazioni; o

(ii) in relazione alla fornitura di un qualsivoglia servizio di telecomunicazioni a qualsiasi soggetto, o all'utilizzo, da parte di quest'ultimo, 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 soggetti destinatari del servizio, da un soggetto che presta un servizio postale o un servizio di telecomunicazioni».

32 Secondo le indicazioni contenute nella decisione di rinvio nella causa C-698/15, tali dati includono i «dati relativi all'ubicazione di un utente», ma non quelli relativi al contenuto di una comunicazione.

33 Quanto all'accesso ai dati conservati, l'articolo 22 della RIPA dispone quanto segue:

«(1) Il presente articolo si applica qualora una persona responsabile ai fini del presente capo ritenga che sia necessario per le ragioni ricadenti sotto il paragrafo 2 di questo articolo ottenere qualsiasi dato relativo a comunicazioni.

(2) È necessario per ragioni ricadenti sotto il presente paragrafo ottenere i dati relativi a comunicazioni qualora questi ultimi siano necessari:

(a) per motivi attinenti alla sicurezza nazionale;

(b) al fine di prevenire o accertare reati o di prevenire turbative all'ordine pubblico;

(c) nell'interesse del benessere economico del Regno Unito;

(d) nell'interesse della sicurezza pubblica;

(e) al fine della tutela della salute pubblica;

(f) al fine dell'accertamento o della riscossione di qualsiasi imposta, diritto, tributo o altra imposizione, contributo o onere dovuti all'amministrazione pubblica;

(g) in un'emergenza, al fine di prevenire la morte, le lesioni o qualsiasi danno alla salute fisica o psichica di una persona, o di attenuare qualsiasi lesione o danno alla salute fisica o psichica di una persona;

(h) per qualsiasi altra finalità (non ricadente sotto i punti da a) a g) precisata in un'ingiunzione emessa dal [Ministro dell'Interno].

(4) Fatto salvo il paragrafo 5, la persona responsabile può, qualora ritenga che un operatore di telecomunicazioni o un operatore postale sia in possesso di dati, potrebbe esserlo o potrebbe essere capace di esserlo, esigere, mediante richiesta all'operatore di telecomunicazioni o all'operatore postale, che tale operatore:

(a) ottenga i dati, ove questi non siano già in suo possesso, e

(b) comunque divulghi tutti i dati in proprio possesso o da esso successivamente ottenuti.

(5) La persona responsabile non deve rilasciare alcuna autorizzazione a norma del paragrafo 3 ovvero effettuare una richiesta a norma del paragrafo 4, salvo

qualora essa ritenga che l'acquisizione dei dati in questione risultante da un compartimento autorizzato o imposto in virtù di un'autorizzazione o di una richiesta sia proporzionata alle finalità perseguite tramite l'acquisizione dei dati».

34 Conformemente all'articolo 65 della RIPA, possono essere presentate delle denunce dinanzi all'Investigatory Powers Tribunal (Tribunale competente per i poteri di indagine, Regno Unito) qualora vi sia ragione di ritenere che dei dati siano stati ottenuti in maniera inappropriata.

Il Data Retention Regulations 2014

35 Il Data Retention Regulations 2014 (regolamento del 2014 sulla conservazione di dati), adottato sulla base della DRIPA, è diviso in tre parti, nella seconda delle quali sono contenuti gli articoli da 2 a 14 del regolamento stesso. L'articolo 4, intitolato «Richieste in materia di conservazione», prevede quanto segue:

«(1) Gli avvisi di conservazione dei dati devono precisare:

(a) l'operatore di telecomunicazioni pubbliche (o la descrizione degli operatori) cui l'avviso è rivolto;

(b) i dati rilevanti relativi a comunicazioni che devono essere conservati;

(c) il periodo o i periodi durante i quali i dati devono essere conservati;

(d) qualsiasi altra prescrizione o restrizione in correlazione alla conservazione dei dati.

(2) Un avviso di conservazione di dati non può imporre che un dato sia conservato per più di 12 mesi a partire:

(a) nel caso dei dati relativi al traffico o dei dati relativi all'utilizzazione del servizio, dal giorno della comunicazione di cui trattasi e,

(b) nel caso dei dati relativi agli abbonati, dal giorno in cui la persona in questione pone termine al servizio di comunicazione in questione, ovvero (se precedente) dal giorno in cui il dato viene modificato.

(...)».

36 L'articolo 7 di tale regolamento, intitolato «Integrità e sicurezza dei dati» stabilisce:

«(1) Un operatore di telecomunicazioni pubbliche che conservi dei dati in applicazione dell'articolo 1 della [DRIPA] deve:

(a) assicurarsi che i dati presentino la stessa integrità e siano sottoposti almeno al medesimo livello di sicurezza e di protezione dei dati dei sistemi dai quali provengono;

(b) assicurarsi, mediante misure tecniche e organizzative appropriate, che soltanto il personale specificamente autorizzato possa accedere ai dati, e

(c) proteggere, mediante misure tecniche e organizzative appropriate, i dati contro il rischio di distruzione accidentale o illecita, di perdita o alterazione accidentale, ovvero di conservazione, trattamento, accesso o divulgazione illeciti o non autorizzati.

(2) Un operatore di telecomunicazioni pubbliche che conservi dei dati relativi a comunicazioni a norma dell'articolo 1 della [DRIPA] deve distruggere i dati qualora la conservazione degli stessi cessi di essere autorizzata in virtù del presente articolo e non sia altrimenti autorizzata dalla legge.

(3) L'obbligo imposto dal paragrafo 2 di distruggere i dati è una prescrizione che impone di distruggere i dati in modo tale da rendere impossibile l'accesso a questi ultimi.

(4) È sufficiente per l'operatore adottare disposizioni tali per cui la distruzione dei dati abbia luogo con cadenza mensile o ad intervalli più brevi secondo le possibilità pratiche che si offrono all'operatore».

37 L'articolo 8 di detto regolamento, intitolato «Divulgazione dei dati conservati», dispone quanto segue:

«(1) Un operatore di telecomunicazioni pubbliche deve mettere in atto adeguati sistemi di sicurezza (comprendenti misure tecniche e organizzative) che disciplinino l'accesso ai dati relativi a comunicazioni conservati a norma dell'articolo 1 della [DRIPA] al fine di evitare qualsiasi divulgazione non ricadente sotto le previsioni dell'articolo 1, paragrafo 6, lettera a), della [DRIPA].

(2) Un operatore di telecomunicazioni pubbliche che conservi dei dati a norma dell'articolo 1 della [DRIPA] deve conservare i dati in modo da poterli trasmettere, senza indebito ritardo, in risposta a richieste presentate».

38 L'articolo 9 di questo stesso regolamento, intitolato «Controllo esercitato dal Commissario garante delle informazioni», enuncia quanto segue:

«Il Commissario garante delle informazioni deve verificare il rispetto delle prescrizioni o restrizioni dettate dalla presente Parte di questo regolamento riguardo all'integrità, alla sicurezza e alla distruzione dei dati conservati a norma dell'articolo 1 della [DRIPA]».

Il codice di condotta

39 L'Acquisition and Disclosure of Communications Data Code of Practice (codice di condotta in materia di acquisizione e divulgazione di dati relativi a comunicazioni; in prosieguo: il «codice di condotta») contiene, ai paragrafi da 2.5 a 2.9 e da 2.36 a 2.45, orientamenti in merito alla necessità e alla proporzionalità dell'acquisizione dei dati relativi a comunicazioni. Secondo i chiarimenti forniti dal giudice del rinvio nella causa C-698/15, deve essere prestata, in conformità dei paragrafi da 3.72 a 3.77 di detto codice, una particolare attenzione alla necessità e alla proporzionalità qualora i dati relativi a comunicazioni richiesti si riferiscano ad una persona che è membro di una professione beneficiante di informazioni tutelate dal segreto professionale o altrimenti riservate.

40 In virtù dei paragrafi da 3.78 a 3.84 del codice summenzionato, è richiesta l'ordinanza di un giudice nel caso particolare di una richiesta vertente su dati relativi a comunicazioni, effettuata al fine di identificare la fonte di giornalisti. Secondo i paragrafi da 3.85 a 3.87 di questo medesimo codice, è richiesta un'approvazione giudiziaria in caso di richiesta di accesso formulata da autorità locali. Per contro, non è richiesta alcuna autorizzazione giudiziaria o proveniente da un'entità indipendente per quanto riguarda l'accesso a dati relativi a comunicazioni tutelate da un segreto professionale legale o riferiti a dottori in medicina, a membri del Parlamento o a ministri di culto.

41 Il paragrafo 7.1 del codice di condotta dispone che i dati relativi a comunicazioni acquisiti od ottenuti in virtù delle disposizioni della RIPA, nonché tutti gli estratti, i riassunti e le copie di tali dati devono essere trattati e memorizzati in modo sicuro. Inoltre, devono essere rispettate le prescrizioni contenute nel Data Protection Act (legge relativa alla protezione dei dati).

42 Conformemente al paragrafo 7.18 del codice di condotta, qualora un'autorità pubblica del Regno Unito stia considerando la possibile divulgazione ad autorità straniere di dati relativi a comunicazioni, essa deve, in particolare, verificare se tali dati saranno protetti in maniera adeguata. Tuttavia, risulta dal paragrafo 7.22 di detto codice che un trasferimento dei dati verso paesi terzi può essere effettuato qualora sia necessario per ragioni attinenti ad un interesse pubblico rilevante, anche quando il paese terzo non assicuri un livello di protezione adeguato. Secondo le indicazioni fornite dal giudice del rinvio nella causa C-698/15, il

Ministro dell'Interno può emettere un certificato di sicurezza nazionale che esenta alcuni dati dal rispetto delle disposizioni previste dalla normativa.

43 Al paragrafo 8.1 di detto codice, viene ricordato che la RIPA ha istituito l'Interception of Communications Commissioner (Commissario garante per le intercettazioni di comunicazioni, Regno Unito), il cui ruolo è, in particolare, di vigilare in maniera indipendente sull'esercizio e sulla messa in atto dei poteri e dei doveri enunciati nel capo II della parte I della RIPA. Come risulta dal paragrafo 8.3 di questo medesimo codice, il commissario suddetto, qualora possa «dimostrare che un individuo è stato leso in conseguenza di una violazione intenzionale o per imprudenza», è autorizzato a informare tale individuo che sussiste un sospetto di uso illecito di competenze.

Procedimenti principali e questioni pregiudiziali

Causa C-203/15

44 Il 9 aprile 2014, la Tele2 Sverige, fornitore di servizi di comunicazione elettronica con sede in Svezia, ha notificato alla PTS che, a seguito dell'invalidazione della direttiva 2006/24 per effetto della sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238; in prosieguo: la «sentenza Digital Rights»), essa avrebbe cessato, a partire dal 14 aprile 2014, di conservare i dati relativi alle comunicazioni elettroniche, contemplati dalla LEK, e avrebbe proceduto alla soppressione dei dati conservati fino al giorno sopra indicato.

45 Il 15 aprile 2014, la Rikspolisstyrelsen (direzione generale della polizia nazionale, Svezia) ha presentato dinanzi alla PTS una denuncia a motivo del fatto che la Tele2 Sverige aveva cessato di comunicarle i dati in questione.

46 Il 29 aprile 2014, il Justitieminister (Ministro della Giustizia, Svezia) ha designato un relatore speciale incaricato di esaminare la normativa svedese in questione alla luce della sentenza Digital Rights. In una relazione datata 13 giugno 2014, intitolata «Datalagring, EU-rätten och svensk rätt, n. Ds 2014:23» (Conservazione di dati, diritto dell'Unione e diritto svedese; in prosieguo: la «relazione del 2014»), il relatore speciale ha concluso che la normativa nazionale in materia di conservazione di dati, quale prevista dagli articoli da 16 a fino a 16 f della LEK, non era contraria né al diritto dell'Unione né alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 (in prosieguo: la «CEDU»). Il relatore speciale ha sottolineato che la sentenza Digital Rights non poteva essere interpretata nel senso che essa avesse censurato il principio stesso di una conservazione generalizzata e indifferenziata dei dati. Dal suo punto di vista, la sentenza Digital Rights non doveva neppure essere intesa nel senso che la Corte avesse con essa stabilito una serie di criteri da soddisfarsi nella loro totalità affinché una normativa potesse considerarsi

proporzionata. Sarebbe stato necessario valutare tutte le circostanze al fine di accertare la conformità della normativa svedese al diritto dell'Unione, come l'ampiezza della conservazione dei dati alla luce delle disposizioni sull'accesso ai dati stessi, sulla durata della loro conservazione, sulla loro protezione, nonché sulla loro sicurezza.

47 Su tale base la PTS, in data 19 giugno 2014, ha comunicato alla Tele2 Sverige che essa violava gli obblighi imposti dalla normativa nazionale omettendo di conservare i dati contemplati dalla LEK per un periodo di sei mesi a scopi di lotta contro la criminalità. Con ingiunzione datata 27 giugno 2014, la PTS le ha quindi ordinato di procedere, al più tardi il 25 luglio 2014, alla conservazione di tali dati.

48 Ritenendo che la relazione del 2014 fosse fondata su un'errata interpretazione della sentenza Digital Rights e che l'obbligo di conservazione dei dati fosse contrario ai diritti fondamentali garantiti dalla Carta, la Tele2 Sverige ha proposto un ricorso dinanzi al Förvaltningsrätten i Stockholm (Tribunale amministrativo di Stoccolma, Svezia) contro l'ingiunzione del 27 giugno 2014. Avendo tale giudice respinto il ricorso con sentenza in data 13 ottobre 2014, la Tele2 Sverige ha proposto appello contro questa pronuncia dinanzi al giudice del rinvio.

49 Ad avviso del giudice del rinvio, la compatibilità della normativa svedese con il diritto dell'Unione deve essere valutata alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58. Infatti, mentre questa direttiva fisserebbe il principio secondo cui i dati relativi al traffico e i dati relativi all'ubicazione devono essere cancellati o resi anonimi qualora non siano più necessari per la trasmissione di una comunicazione, l'articolo 15, paragrafo 1, della medesima direttiva introdurrebbe una deroga a tale principio in quanto autorizzerebbe gli Stati membri, ove ciò sia giustificato da uno dei motivi enunciati da tale norma, a limitare il suddetto obbligo di cancellazione o di anonimizzazione od anche a prevedere la conservazione di dati. Dunque, il diritto dell'Unione permetterebbe, in certe situazioni, la conservazione dei dati relativi alle comunicazioni elettroniche.

50 Il giudice del rinvio si chiede nondimeno se un obbligo generalizzato e indifferenziato di conservazione dei dati relativi alle comunicazioni elettroniche, come quello controverso nel procedimento principale, sia compatibile, in considerazione della sentenza Digital Rights, con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta. Tenuto conto delle opinioni divergenti delle parti sul punto, occorrerebbe che la Corte si pronunciasse in maniera univoca sulla questione se, come sostenuto dalla Tele2 Sverige, la conservazione generalizzata e indifferenziata dei dati relativi alle comunicazioni elettroniche sia di per sé stessa incompatibile con gli articoli 7 e 8 nonché con l'articolo 52, paragrafo 1, della Carta, o se, come risulterebbe dalla relazione del 2014, la compatibilità di una siffatta conservazione di dati debba essere valutata alla luce delle norme

disciplinanti l'accesso ai dati, la protezione di questi ultimi e la loro sicurezza, nonché la durata della loro conservazione.

51 È alla luce di tali circostanze che il giudice del rinvio ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se un obbligo generalizzato di conservazione dei dati, concernente tutte le persone, tutti i mezzi di comunicazione elettronica e tutti i dati relativi al traffico, senza che sia prevista alcuna distinzione, limitazione o eccezione in funzione dell'obiettivo della lotta alla criminalità (...), sia compatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58, tenuto conto degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta.

2) In caso di risposta negativa alla prima questione, se la conservazione possa nondimeno essere consentita quando:

a) l'accesso da parte delle autorità nazionali ai dati conservati è stabilito secondo le modalità descritte ai punti da 19 a 36 [della decisione di rinvio], e

b) i requisiti di protezione e di sicurezza sono disciplinati come descritto ai punti da 38 a 43 [della decisione di rinvio], e

c) tutti i dati pertinenti devono essere conservati per sei mesi, calcolati dalla data della fine della comunicazione, e successivamente cancellati come descritto al punto 37 [della decisione di rinvio]».

Causa C-698/15

52 I sigg. Watson, Brice e Lewis hanno presentato tutti, dinanzi alla High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Alta Corte di giustizia (Inghilterra e Galles), divisione del Queens' Bench (sezione divisionale), Regno Unito], un ricorso giurisdizionale inteso alla verifica della legittimità dell'articolo 1 della DRIPA, invocando in particolare l'incompatibilità di tale articolo con gli articoli 7 e 8 della Carta nonché con l'articolo 8 della CEDU.

53 Con sentenza in data 17 luglio 2015, la High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Alta Corte di giustizia (Inghilterra e Galles), divisione del Queens' Bench (sezione divisionale)], ha constatato che la sentenza Digital Rights enunciava «requisiti imperativi di diritto dell'Unione» applicabili alle normative degli Stati membri in materia di conservazione dei dati relativi a comunicazioni nonché all'accesso a tali dati. Secondo detto giudice, poiché in tale sentenza la Corte ha affermato che la direttiva 2006/24 era

incompatibile con il principio di proporzionalità, una normativa nazionale dal contenuto identico a quello di tale direttiva non potrebbe neanch'essa essere compatibile con il suddetto principio. Risulterebbe dalla logica sottesa alla sentenza Digital Rights che una normativa istituente un regime generalizzato di conservazione dei dati relativi a comunicazioni viola i diritti garantiti dagli articoli 7 e 8 della Carta, a meno che tale normativa non sia completata da un regime di accesso ai dati, definito dal diritto nazionale, il quale preveda garanzie sufficienti per la salvaguardia di tali diritti. Dunque, l'articolo 1 della DRIPA non sarebbe compatibile con gli articoli 7 e 8 della Carta in quanto esso non stabilirebbe regole chiare e precise disciplinanti l'accesso e l'utilizzazione dei dati conservati e non subordinerebbe l'accesso a tali dati ad un controllo preventivo esercitato da un giudice o da un'entità amministrativa indipendente.

54 Il Ministro dell'Interno ha proposto appello contro detta sentenza dinanzi alla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile), Regno Unito].

55 Tale giudice rileva che l'articolo 1, paragrafo 1, della DRIPA legittima il Ministro dell'Interno ad adottare, in assenza di qualsivoglia autorizzazione preventiva di un giudice o di un'entità amministrativa indipendente, un regime generale che impone agli operatori di telecomunicazioni pubbliche di conservare tutti i dati riguardanti qualsiasi servizio postale o qualsiasi servizio di telecomunicazioni per un periodo massimo di dodici mesi, qualora esso ritenga che una prescrizione siffatta sia necessaria e proporzionata per perseguire le finalità enunciate nella normativa del Regno Unito. Anche se tali dati non comprendono il contenuto di una comunicazione, essi potrebbero avere un carattere particolarmente invasivo per la vita privata degli utenti di servizi di comunicazione.

56 Il giudice del rinvio, nella decisione di rinvio e nella sua sentenza del 20 novembre 2015, pronunciata nell'ambito del procedimento di appello e mediante la quale esso ha deciso di sottoporre alla Corte la presente domanda di pronuncia pregiudiziale, afferma che le norme nazionali relative alla conservazione dei dati ricadono necessariamente sotto l'articolo 15, paragrafo 1, della direttiva 2002/58 e devono dunque rispettare le prescrizioni scaturenti dalla Carta. Tuttavia, alla luce di quanto disposto dall'articolo 1, paragrafo 3, di tale direttiva, il legislatore dell'Unione non avrebbe armonizzato le norme disciplinanti l'accesso ai dati conservati.

57 Quanto all'incidenza della sentenza Digital Rights sulle questioni sollevate nel procedimento principale, il giudice del rinvio osserva che, nella causa sfociata in detta sentenza, la Corte era stata chiamata a pronunciarsi sulla validità della direttiva 2006/24 e non su quella di una normativa nazionale. Tenuto conto in particolare dello stretto rapporto esistente tra la conservazione dei dati e l'accesso a questi ultimi, sarebbe stato indispensabile che la direttiva di cui sopra fosse accompagnata da una serie di garanzie e che la sentenza Digital Rights

esaminasse, in sede di verifica della legittimità del regime di conservazione dei dati istituito da detta direttiva, le norme relative all'accesso ai dati medesimi. La Corte non avrebbe dunque inteso enunciare, in detta pronuncia, prescrizioni imperative applicabili alle normative nazionali in materia di accesso ai dati non recanti attuazione del diritto dell'Unione. Inoltre, il ragionamento della Corte sarebbe stato strettamente legato all'obiettivo perseguito da questa medesima direttiva. Tuttavia, una normativa nazionale dovrebbe essere valutata alla luce degli obiettivi da essa perseguiti e non del suo contesto.

58 Per quanto riguarda la necessità di effettuare un rinvio pregiudiziale alla Corte, il giudice del rinvio evidenzia il fatto che, alla data di adozione della decisione di rinvio, sei giudici di altri Stati membri, cinque dei quali di ultima istanza, avevano annullato delle normative nazionali fondandosi sulla sentenza Digital Rights. La risposta alle questioni sollevate non sarebbe dunque evidente, ma sarebbe necessaria per statuire sulle cause pendenti dinanzi ad esso giudice.

59 Alla luce di tali circostanze, la Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile)] ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se la sentenza Digital Rights (con particolare riferimento ai punti da 60 a 62 della stessa) fissi requisiti imperativi di diritto dell'Unione, applicabili al regime nazionale di uno Stato membro che disciplina l'accesso ai dati conservati ai sensi della normativa nazionale, al fine di rispettare gli articoli 7 e 8 della Carta.

2) Se la sentenza Digital Rights estenda l'ambito di applicazione degli articoli 7 e/o 8 della Carta oltre quello dell'articolo 8 della CEDU, come stabilito dalla giurisprudenza della Corte europea dei diritti dell'uomo».

Sul procedimento dinanzi alla Corte

60 Con ordinanza del 1º febbraio 2016, Davis e a. (C-698/15, non pubblicata, EU:C:2016:70), il presidente della Corte ha deciso di accogliere la domanda della Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile)] volta ad ottenere che la causa C-698/15 sia trattata in base al procedimento accelerato previsto dall'articolo 105, paragrafo 1, del regolamento di procedura della Corte.

61 Con decisione del presidente della Corte del 10 marzo 2016, le cause C-203/15 e C-698/15 sono state riunite ai fini della fase orale del procedimento e della sentenza.

Sulle questioni pregiudiziali

Sulla prima questione nella causa C-203/15

62 Con la sua prima questione nella causa C-203/15, il Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma) chiede, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che esso osta ad una normativa nazionale, come quella in discussione nel procedimento principale, la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati ed utenti iscritti concernente tutti i mezzi di comunicazione elettronica.

63 Tale questione trae origine, in particolare, dal fatto che la direttiva 2006/24, cui la normativa nazionale in discussione nel procedimento principale ha inteso dare attuazione, è stata dichiarata invalida dalla sentenza Digital Rights, ma le parti controvertono sulla portata di tale pronuncia e sulla sua incidenza sulla normativa suddetta, tenendo presente che tale normativa disciplina la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nonché l'accesso a tali dati da parte delle autorità nazionali.

64 Occorre preliminarmente verificare se una normativa nazionale quale quella in discussione nel procedimento principale rientri nell'ambito di applicazione del diritto dell'Unione.

Sull'ambito di applicazione della direttiva 2002/58

65 Gli Stati membri che hanno presentato osservazioni scritte alla Corte hanno espresso opinioni divergenti sul punto se e in quale misura normative nazionali 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, per finalità di lotta contro la criminalità, rientrino nell'ambito di applicazione della direttiva 2002/58. Infatti, mentre, in particolare, i governi belga, danese, tedesco, estone e l'Irlanda, nonché il governo neerlandese, hanno espresso il parere che una questione siffatta esiga una risposta affermativa, il governo ceco ha proposto di rispondere in senso negativo a tale questione, facendo osservare come le normative suddette abbiano quale unico obiettivo la lotta contro la criminalità. Quanto al governo del Regno Unito, esso fa valere che nell'ambito di applicazione della citata direttiva rientrano soltanto le normative vertenti sulla conservazione dei dati e non quelle riguardanti l'accesso ai dati stessi da parte delle autorità nazionali competenti in materia di repressione degli illeciti.

66 Quanto, infine, alla Commissione, essa ha invero sostenuto, nelle sue osservazioni scritte presentate alla Corte nella causa C-203/15, che la normativa nazionale in

discussione nel procedimento principale rientra nell'ambito di applicazione della direttiva 2002/58, ma ha asserito, nelle sue osservazioni scritte nella causa C-698/15, che soltanto le norme nazionali relative alla conservazione dei dati, e non anche quelle relative all'accesso delle autorità nazionali a tali dati, rientrano nell'ambito di applicazione di detta direttiva. Queste ultime norme dovrebbero però, a suo parere, essere prese in considerazione al fine di valutare se una normativa nazionale disciplinante la conservazione dei dati da parte dei fornitori di servizi di comunicazione elettronica costituisca una ingerenza proporzionata nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta.

67 A questo proposito, occorre rilevare che l'ampiezza dell'ambito di applicazione della direttiva 2002/58 deve essere valutata tenendo conto in particolare dell'economia generale di quest'ultima.

68 A termini 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, e in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche.

69 L'articolo 1, paragrafo 3, della citata direttiva esclude dall'ambito di applicazione di quest'ultima le «attività dello Stato» nei settori contemplati dalla disposizione stessa, e precisamente le attività dello Stato in materia penale e quelle riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato, ivi compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato (v., per analogia, per quanto riguarda l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, sentenze del 6 novembre 2003, Lindqvist, C-101/01, EU:C:2003:596, punto 43, nonché del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, punto 41).

70 Quanto all'articolo 3 della direttiva 2002/58, esso enuncia che tale 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 direttiva di cui sopra deve essere considerata come disciplinante le attività dei fornitori di tali servizi.

71 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». L'articolo 15, paragrafo 1, seconda frase, della medesima direttiva identifica, a titolo di esempio di misure che possono essere così adottate dagli Stati membri, le misure «le quali prevedano che i dati siano conservati».

72 Certo, le disposizioni legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 si riferiscono ad attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 51). Inoltre, le finalità che, in forza del citato articolo 15, paragrafo 1, le disposizioni legislative suddette devono soddisfare – nella fattispecie, la salvaguardia della sicurezza nazionale, della difesa e della sicurezza pubblica, nonché la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati ovvero dell'uso non autorizzato del sistema di comunicazione elettronica – coincidono sostanzialmente con le finalità perseguite dalle attività contemplate dall'articolo 1, paragrafo 3, della medesima direttiva.

73 Tuttavia, alla luce dell'economia generale della direttiva 2002/58, gli elementi rilevati al punto precedente della presente sentenza non consentono di concludere che le misure legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 siano escluse dall'ambito di applicazione di tale direttiva, a pena di privare detta disposizione di qualsiasi effetto utile. Infatti, il citato articolo 15, paragrafo 1, presuppone necessariamente che le misure nazionali da esso contemplate, come quelle relative alla conservazione di dati per finalità di lotta contro la criminalità, rientrino nell'ambito di applicazione di questa medesima direttiva, dato che quest'ultima autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare le condizioni da essa previste.

74 Inoltre, le misure legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 disciplinano, per le finalità menzionate in tale disposizione, l'attività dei fornitori di servizi di comunicazione elettronica. Pertanto, il suddetto articolo 15, paragrafo 1, letto in connessione con l'articolo 3 della medesima direttiva, deve essere interpretato nel senso che siffatte misure legislative rientrano nell'ambito di applicazione della direttiva stessa.

75 In particolare, rientra in tale ambito di applicazione una misura legislativa, quale quella in discussione nei procedimenti principali, la quale imponga a detti fornitori di conservare i dati relativi al traffico e i dati relativi all'ubicazione, in quanto una siffatta attività implica necessariamente un trattamento, da parte di tali soggetti, di dati personali.

76 Rientra del pari nel suddetto ambito di applicazione una misura legislativa riguardante, come nel procedimento principale, l'accesso delle autorità nazionali ai dati conservati dai fornitori di servizi di comunicazione elettronica.

77 Infatti, la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico afferenti alle stesse, garantita dall'articolo 5, paragrafo 1, della direttiva 2002/58, si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di persone o di entità private oppure di entità statali. Come confermato dal considerando 21 di detta direttiva,

quest'ultima mira ad impedire «l'accesso» non autorizzato alle comunicazioni, ivi compreso «qualsiasi dato (...) relativo [a tali comunicazioni]», al fine di tutelare la riservatezza delle comunicazioni elettroniche.

78 Date tali circostanze, una misura legislativa mediante la quale uno Stato membro, sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58, imponga ai fornitori di servizi di comunicazione elettronica, per le finalità menzionate da tale disposizione, di accordare alle autorità nazionali, alle condizioni previste dalla misura stessa, l'accesso ai dati conservati da tali fornitori, ha ad oggetto attività di trattamento di dati personali realizzate da questi ultimi, attività che rientrano nell'ambito di applicazione della direttiva in parola.

79 Inoltre, poiché la conservazione di dati viene effettuata al solo scopo di rendere, eventualmente, i dati accessibili alle autorità nazionali competenti, una normativa nazionale che preveda la conservazione di dati implica necessariamente, in linea di principio, l'esistenza di disposizioni in materia di accesso delle autorità nazionali competenti ai dati conservati dai fornitori di servizi di comunicazione elettronica.

80 Tale interpretazione è corroborata dall'articolo 15, paragrafo 1 ter, della direttiva 2002/58, a mente del quale i fornitori istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti sulla base delle disposizioni nazionali adottate a norma del paragrafo 1 del medesimo articolo 15.

81 Risulta da quanto precede che una normativa nazionale quale quella in discussione nei procedimenti principali di cui alle cause C-203/15 e C-698/15 rientra nell'ambito di applicazione della direttiva 2002/58.

Sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta

82 Occorre rilevare che, a norma dell'articolo 1, paragrafo 2, della direttiva 2002/58, le disposizioni di quest'ultima «precisano e integrano» la direttiva 95/46. Come enunciato nel suo considerando 2, la direttiva 2002/58 mira a garantire, in particolare, il pieno rispetto dei diritti sanciti dagli articoli 7 e 8 della Carta. A questo proposito, risulta dall'esposizione delle motivazioni 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».

83 A questo scopo, la direttiva 2002/58 contiene specifiche disposizioni preordinate, come risulta in particolare dai suoi considerando 6 e 7, a proteggere gli utenti dei servizi di comunicazione elettronica dinanzi ai pericoli per i dati personali e per la

vita privata derivanti dalle nuove tecnologie e dall'accresciuta capacità di memorizzazione e di trattamento automatizzati di dati.

84 In particolare, l'articolo 5, paragrafo 1, di detta direttiva stabilisce che gli Stati membri devono garantire, mediante norme di legge nazionali, la riservatezza delle comunicazioni effettuate per il tramite una rete pubblica di comunicazione e di servizi di comunicazione elettronica accessibili al pubblico, nonché la riservatezza dei relativi dati sul traffico.

85 Il principio di riservatezza delle comunicazioni istituito dalla direttiva 2002/58 implica, tra l'altro, come risulta dall'articolo 5, paragrafo 1, seconda frase, di quest'ultima, un divieto imposto, in linea di principio, nei confronti di qualsiasi soggetto diverso dagli utenti di memorizzare, senza il consenso di questi ultimi, i dati relativi al traffico attinenti alle comunicazioni elettroniche. Le uniche eccezioni riguardano le persone autorizzate legalmente ai sensi dell'articolo 15, paragrafo 1, della citata direttiva e la memorizzazione tecnica necessaria alla trasmissione di una comunicazione (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 47).

86 Così, e come confermato dai considerando 22 e 26 della direttiva 2002/58, il trattamento e la memorizzazione dei dati relativi al traffico sono autorizzati, ai sensi dell'articolo 6 della direttiva stessa, soltanto nella misura e per la durata necessaria per la fatturazione dei servizi, per la commercializzazione di questi ultimi e per la fornitura di servizi a valore aggiunto (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punti 47 e 48). Per quanto riguarda, in particolare, la fatturazione dei servizi, tale trattamento è autorizzato soltanto fino alla fine del periodo nel corso del quale la fattura può essere legalmente contestata ovvero fino a quando possono essere avviate azioni per ottenerne il pagamento. Una volta terminato tale periodo, i dati che sono stati trattati e memorizzati devono essere cancellati o resi anonimi. Per quanto riguarda i dati relativi all'ubicazione diversi dai dati relativi al traffico, l'articolo 9, paragrafo 1, di detta direttiva stabilisce che tali dati possono essere trattati soltanto in presenza di determinate condizioni e dopo essere stati resi anonimi oppure con il consenso degli utenti o degli abbonati.

87 La portata delle disposizioni degli articoli 5 e 6 e dell'articolo 9, paragrafo 1, della direttiva 2002/58, i quali mirano a garantire la riservatezza delle comunicazioni e dei dati ad esse relativi, nonché a minimizzare i rischi di abuso, deve inoltre essere valutata alla luce del considerando 30 della medesima direttiva, a termini del quale «[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».

88 Vero è che l'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio, enunciato all'articolo 5,

paragrafo 1, di detta direttiva, di garantire la riservatezza dei dati personali, nonché ai corrispondenti obblighi, menzionati segnatamente negli articoli 6 e 9 della medesima direttiva (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 50).

89 Nondimeno, l'articolo 15, paragrafo 1, della direttiva 2002/58, consentendo agli Stati membri di limitare la portata dell'obbligo di principio di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico a queste correlati, deve essere interpretato, conformemente alla consolidata giurisprudenza della Corte, in maniera restrittiva (v., per analogia, sentenza del 22 novembre 2012, Probst, C-119/12, EU:C:2012:748, punto 23). Pertanto, una disposizione siffatta non può giustificare che la deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati, previsto dall'articolo 5 della medesima direttiva, divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata.

90 In proposito, occorre rilevare come l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 stabilisca che le misure legislative che esso prevede e che derogano al principio della riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati debbono avere come obiettivo «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», oppure devono perseguire uno degli altri obiettivi contemplati dall'articolo 13, paragrafo 1, della direttiva 95/46, cui l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 rinvia (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 53). Una siffatta elencazione di obiettivi presenta carattere esaustivo, come risulta dall'articolo 15, paragrafo 1, seconda frase, della citata direttiva 2002/58, a mente del quale le misure legislative devono essere giustificate sulla scorta dei «motivi enunciati» nella prima frase del medesimo articolo 15, paragrafo 1. Pertanto, gli Stati membri non possono adottare misure siffatte per finalità diverse da quelle elencate in quest'ultima disposizione.

91 Inoltre, l'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 dispone che «[t]utte le misure di cui [all'articolo 15, paragrafo 1, di tale direttiva] sono conformi ai principi generali del diritto [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [UE]», tra i quali figurano i principi generali e i diritti fondamentali ormai garantiti dalla Carta. L'articolo 15, paragrafo 1, della direttiva 2002/58 deve dunque essere interpretato alla luce dei diritti fondamentali garantiti dalla Carta (v., per analogia, per quanto riguarda la direttiva 95/46, sentenze del 20 maggio 2003, Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68; del 13 maggio 2014, Google Spain e Google, C-131/12, EU:C:2014:317, punto 68, nonché del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 38).

92 A questo proposito, occorre sottolineare che l'obbligo imposto ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale quale quella in discussione nei procedimenti principali, di conservare i dati relativi al traffico ai fini di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7 e 8 della Carta, che sono esplicitamente menzionati nelle questioni pregiudiziali, ma anche della libertà di espressione garantita dall'articolo 11 della Carta stessa (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punti 25 e 70).

93 Così, l'importanza sia del diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto alla protezione dei dati personali, sancito dall'articolo 8 di quest'ultima, quale emerge dalla giurisprudenza della Corte (v., in tal senso, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 39 e la giurisprudenza ivi citata), deve essere presa in considerazione in sede di interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58. Lo stesso vale per il diritto alla libertà di espressione alla luce della particolare importanza che riveste tale libertà in qualsiasi società democratica. Tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata (v., in tal senso, sentenze del 12 giugno 2003, Schmidberger, C-112/00, EU:C:2003:333, punto 79, nonché del 6 settembre 2011, Patriciello, C-163/10, EU:C:2011:543, punto 31).

94 A questo proposito, occorre ricordare che, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge e rispettare il loro contenuto essenziale. Nel rispetto del principio di proporzionalità, possono essere apportate delle limitazioni all'esercizio dei diritti e delle libertà summenzionati soltanto qualora esse siano necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (sentenza del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 50).

95 A quest'ultimo proposito, l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 prevede che gli Stati membri possano adottare una misura derogante al principio della riservatezza delle comunicazioni e dei dati relativi al traffico correlati a queste ultime qualora essa sia «necessaria, opportuna e proporzionata all'interno di una società democratica», in rapporto agli obiettivi enunciati dalla disposizione suddetta. Quanto al considerando 11 della citata direttiva, esso precisa che una misura di questa natura deve essere «strettamente» proporzionata allo scopo perseguito. Per quanto riguarda, in particolare, la conservazione di dati, l'articolo 15, paragrafo 1, seconda frase, della direttiva 2002/58 esige che essa abbia luogo soltanto «per un periodo di tempo limitato» e quando ciò sia giustificato da uno degli obiettivi previsti dall'articolo 15, paragrafo 1, prima frase, della medesima direttiva.

96 Il rispetto del principio di proporzionalità discende altresì dalla consolidata giurisprudenza della Corte secondo cui la tutela del diritto fondamentale al rispetto della vita privata a livello dell'Unione esige che le deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario (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, punto 77; Digital Rights, punto 52, nonché del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 92).

97 Per quanto riguarda la questione se una normativa nazionale quale quella in discussione nella causa C-203/15 soddisfi le condizioni suddette, occorre rilevare che tale normativa prevede una conservazione generalizzata e indifferenziata 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, e che essa obbliga i fornitori di servizi di comunicazione elettronica a conservare tali dati in maniera sistematica e continua, e ciò senza alcuna eccezione. Come risulta dalla decisione di rinvio, le categorie di dati contemplati da tale normativa corrispondono, in sostanza, a quelle la cui conservazione era prevista dalla direttiva 2006/24.

98 I dati che devono così essere conservati dai fornitori di servizi di comunicazione elettronica permettono di ritrovare e di identificare la fonte di una comunicazione e la destinazione di quest'ultima, di stabilire la data, l'ora, la durata e il tipo di una comunicazione, nonché il materiale di comunicazione degli utenti, e di localizzare il materiale di comunicazione mobile. Nel novero di tali dati figurano, in particolare, il nome e l'indirizzo dell'abbonato o dell'utente iscritto, il numero di telefono del chiamante e il numero chiamato, nonché un indirizzo IP per i servizi Internet. Tali dati permettono, in particolare, di sapere quale sia la persona con la quale un abbonato o un utente iscritto ha comunicato e attraverso quale mezzo, come pure di stabilire il tempo della comunicazione, nonché il luogo a partire dal quale quest'ultima ha avuto luogo. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente iscritto con talune persone durante un periodo determinato (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 26).

99 Presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 27). In particolare, tali dati forniscono gli strumenti per stabilire – come ha rilevato l'avvocato generale ai paragrafi 253, 254 e da 257 a 259 delle sue conclusioni – il profilo delle persone interessate, informazione tanto sensibile, in

rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni.

100 L'ingerenza che una normativa siffatta determina nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta risulta essere di vasta portata e deve essere considerata particolarmente grave. La circostanza che la conservazione dei dati venga effettuata senza che gli utenti dei servizi di comunicazione elettronica ne siano informati è idonea a ingenerare nello spirito delle persone riguardate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua (v., per analogia, per quanto concerne la direttiva 2006/24, sentenza Digital Rights, punto 37).

101 Anche se una normativa siffatta non autorizza la conservazione del contenuto di una comunicazione e, di conseguenza, non è idonea a pregiudicare il contenuto essenziale dei suddetti diritti (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 39), la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione potrebbe nondimeno avere un'incidenza sull'utilizzazione dei mezzi di comunicazione elettronica e, dunque, sull'esercizio, da parte degli utenti, di tali mezzi della loro libertà di espressione, garantita dall'articolo 11 della Carta (v., per analogia, per quanto concerne la direttiva 2006/24, sentenza Digital Rights, punto 28).

102 Tenuto conto della gravità dell'ingerenza nei diritti fondamentali in questione derivante da una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, la conservazione di dati relativi al traffico e di dati relativi all'ubicazione, soltanto la lotta contro la criminalità grave è idonea a giustificare una misura del genere (v., per analogia, a proposito della direttiva 2006/24, sentenza Digital Rights, punto 60).

103 Inoltre, anche se l'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine, un siffatto obiettivo di interesse generale, per quanto fondamentale esso sia, non vale di per sé solo a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 51).

104 A questo proposito, occorre rilevare, da un lato, che una normativa siffatta, alla luce delle sue caratteristiche descritte al punto 97 della presente sentenza, porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, quando invece il sistema istituito dalla direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione.

105 Dall'altro lato, una normativa nazionale come quella in discussione nei procedimenti principali, la quale riguarda in maniera generalizzata tutti gli abbonati ed utenti iscritti e ha ad oggetto tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico, non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito. Essa concerne in maniera globale l'insieme delle persone che si avvalgono di servizi di comunicazione elettronica, senza che tali persone si trovino, anche solo indirettamente, in una situazione suscettibile di dar luogo ad azioni penali. Essa si applica dunque finanche a persone per le quali non esiste alcun indizio di natura tale da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi. Inoltre, essa non prevede alcuna eccezione, di modo che essa si applica anche a persone le cui comunicazioni sono sottoposte, secondo le norme del diritto nazionale, al segreto professionale (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punti 57 e 58).

106 Una normativa siffatta non richiede alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica. In particolare, essa non è limitata ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 59).

107 Una normativa nazionale come quella in discussione nei procedimenti principali travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede 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.

108 Per contro, l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario.

109 Per soddisfare i requisiti enunciati al punto precedente della presente sentenza, la suddetta normativa nazionale deve, in primo luogo, prevedere norme chiare e precise che disciplinino la portata e l'applicazione di una siffatta misura di conservazione dei dati e fissino un minimo di requisiti, di modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti tali da permettere

di proteggere efficacemente i loro dati personali contro i rischi di abuso. Essa deve in particolare indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario (v., per analogia, a proposito della direttiva 2006/24, sentenza Digital Rights, punto 54 e la giurisprudenza ivi citata).

110 In secondo luogo, per quanto riguarda le condizioni sostanziali che devono essere soddisfatte da una normativa nazionale che permetta, nel contesto della lotta contro la criminalità, la conservazione, a titolo preventivo, dei dati relativi al traffico e dei dati relativi all'ubicazione, al fine di garantire che essa sia limitata allo stretto necessario, occorre rilevare che, se certo tali condizioni possono variare in funzione delle misure adottate ai fini della prevenzione, della ricerca, dell'accertamento e del perseguimento della criminalità grave, la conservazione dei dati deve comunque rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato.

111 Per quanto riguarda la delimitazione di una misura siffatta sotto il profilo del pubblico e delle situazioni potenzialmente riguardati, la normativa nazionale deve essere fondata su elementi oggettivi, che permettano di prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica. Una siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo.

112 Alla luce dell'insieme delle considerazioni che precedono, occorre rispondere alla prima questione nella causa C-203/15 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 ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata 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.

Sulla seconda questione nella causa C-203/15 e sulla prima questione nella causa C-698/15

113 Occorre rilevare, in via preliminare, che il Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma) ha sollevato la seconda questione nella causa C-203/15 soltanto per l'ipotesi di una risposta negativa alla prima questione

in tale causa. Tuttavia, tale seconda questione è indipendente dal carattere generalizzato o mirato di una conservazione dei dati, nel senso contemplato ai punti da 108 a 111 della presente sentenza. Pertanto, occorre rispondere congiuntamente alla seconda questione nella causa C-203/15 e alla prima questione nella causa C-698/15, la quale viene posta indipendentemente dall'ampiezza dell'obbligo di conservazione dei dati che sarebbe imposto ai fornitori di servizi di comunicazione elettronica.

114 Con la seconda questione nella causa C-203/15 e la prima questione nella causa C-698/15, i giudici di rinvio chiedono, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre tale accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione.

115 Per quanto riguarda gli obiettivi idonei a giustificare una normativa nazionale che deroghi al principio della riservatezza delle comunicazioni elettroniche, occorre ricordare che, poiché – come si è constatato ai punti 90 e 102 della presente sentenza – l'elencazione degli obiettivi figurante all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 presenta carattere esaustivo, l'accesso ai dati conservati deve rispondere in modo effettivo e rigoroso ad uno di questi obiettivi. Inoltre, poiché l'obiettivo perseguito da questa normativa deve essere correlato alla gravità dell'ingerenza nei diritti fondamentali che tale accesso determina, ne consegue che, in materia di prevenzione, ricerca, accertamento e perseguimento di violazioni penali, soltanto la lotta contro la criminalità grave è idonea a giustificare un simile accesso ai dati conservati.

116 Per quanto riguarda il rispetto del principio di proporzionalità, una normativa nazionale che disciplini le condizioni alle quali i fornitori di servizi di comunicazione elettronica devono consentire alle autorità nazionali competenti l'accesso ai dati conservati deve assicurare, conformemente a quanto constatato ai punti 95 e 96 della presente sentenza, che tale accesso abbia luogo soltanto entro i limiti dello stretto necessario.

117 Inoltre, dato che le misure legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 devono, conformemente al considerando 11 di tale direttiva, «essere soggette ad idonee garanzie», una misura di tal genere deve prevedere – come risulta dalla giurisprudenza citata al punto 109 della presente sentenza – norme chiare e precise che indichino in quali circostanze e a quali condizioni i fornitori di servizi di comunicazione elettronica devono concedere alle autorità nazionali competenti l'accesso ai dati. Allo stesso modo, una misura

di questa natura deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale.

118 Al fine di garantire che l'accesso delle autorità nazionali competenti ai dati conservati sia limitato allo stretto necessario, spetta senza dubbio al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazione elettronica devono consentire tale accesso. Tuttavia, la normativa nazionale in questione non può limitarsi ad esigere che l'accesso risponda ad uno degli obiettivi contemplati dall'articolo 15, paragrafo 1, della direttiva 2002/58, quand'anche questo fosse la lotta contro la criminalità grave. Infatti, una normativa nazionale siffatta deve prevedere anche le condizioni sostanziali e procedurali che disciplinano l'accesso delle autorità nazionali competenti ai dati conservati (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 61).

119 Pertanto, e poiché un accesso generale a tutti i dati conservati, indipendentemente da una qualche connessione, almeno indiretta, con la finalità perseguita, non può essere considerato limitato allo stretto necessario, la normativa nazionale in questione deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati degli abbonati o degli utenti iscritti. A questo proposito, un accesso può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta (v., per analogia, Corte EDU, 4 dicembre 2015, Zakharov c. Russia, CE:ECHR:2015:1204JUD004714306, § 260). Tuttavia, in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone potrebbe essere parimenti concesso quando sussistano elementi oggettivi che consentano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro simili attività.

120 Al fine di garantire, in pratica, il pieno rispetto di tali condizioni, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 62; v. anche, per analogia, per quanto concerne l'articolo 8 della CEDU, Corte EDU, 12 gennaio 2016, Szabó e Vissy c. Ungheria, CE:ECHR:2016:0112JUD003713814, §§ 77 e 80).

121 Allo stesso modo, occorre che le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate. Infatti, tale informazione è, de facto, necessaria per consentire a dette persone di esercitare, in particolare, il diritto di ricorso, esplicitamente previsto dall'articolo 15, paragrafo 2, della direttiva 2002/58, letto in connessione con l'articolo 22 della direttiva 95/46, in caso di violazione dei loro diritti (v., per analogia, sentenze del 7 maggio 2009, Rijkeboer, C-553/07, EU:C:2009:293, punto 52, nonché del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 95).

122 Per quanto riguarda le norme aventi ad oggetto la sicurezza e la protezione dei dati conservati dai fornitori di servizi di comunicazione elettronica, occorre constatare che l'articolo 15, paragrafo 1, della direttiva 2002/58 non consente agli Stati membri di derogare all'articolo 4, paragrafo 1, nonché all'articolo 4, paragrafo 1 bis, di tale direttiva. Queste ultime disposizioni esigono che i suddetti fornitori prendano le misure tecniche e organizzative appropriate che consentano di garantire un'efficace protezione dei dati conservati contro il rischio di abusi, nonché contro qualsiasi accesso illecito a tali dati. Tenuto conto della quantità di dati conservati, del carattere sensibile dei dati stessi, nonché del rischio di accesso illecito a questi ultimi, i fornitori di servizi di comunicazione elettronica devono, al fine di assicurare la piena integrità e la riservatezza dei dati suddetti, garantire un livello particolarmente elevato di protezione e di sicurezza mediante misure tecniche e organizzative appropriate. In particolare, la normativa nazionale deve prevedere la conservazione nel territorio dell'Unione nonché la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punti da 66 a 68).

123 Ad ogni modo, gli Stati membri devono garantire il controllo, da parte di un'autorità indipendente, del rispetto del livello di protezione garantito dal diritto dell'Unione in materia di tutela delle persone fisiche riguardo al trattamento dei dati personali, stante che tale controllo è esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta e costituisce, secondo la costante giurisprudenza della Corte, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali. Se così non fosse, le persone i cui dati personali sono stati conservati sarebbero private del diritto, garantito dall'articolo 8, paragrafi 1 e 3, della Carta, di presentare alle autorità nazionali di controllo una richiesta finalizzata alla protezione dei loro dati (v., in tal senso, sentenze Digital Rights, punto 68, nonché del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punti 41 e 58).

124 Spetta ai giudici del rinvio verificare se e in quale misura le normative nazionali in discussione nei procedimenti principali rispettino le prescrizioni scaturenti 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, come chiarite ai punti da 115 a 123 della presente sentenza, per quanto riguarda sia l'accesso delle autorità nazionali competenti ai dati conservati, sia la protezione e il livello di sicurezza di tali dati.

125 Alla luce dell'insieme delle considerazioni che precedono, occorre rispondere alla seconda questione nella causa C-203/15 e alla prima questione nella causa C-698/15 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 ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione.

Sulla seconda questione nella causa C-698/15

126 Con la seconda questione nella causa C-698/15, la Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile)] chiede in sostanza se, nella sentenza Digital Rights, la Corte abbia interpretato gli articoli 7 e/o 8 della Carta in un senso che va al di là di quello attribuito all'articolo 8 della CEDU dalla Corte europea dei diritti dell'uomo.

127 In limine, occorre ricordare che, anche se, come conferma l'articolo 6, paragrafo 3, TUE, i diritti fondamentali riconosciuti dalla CEDU fanno parte del diritto dell'Unione in quanto principi generali, tale convenzione non costituisce però, fintantoché l'Unione non vi avrà aderito, uno strumento giuridico formalmente integrato nell'ordinamento giuridico dell'Unione (v., in tal senso, sentenza del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 45 e la giurisprudenza ivi citata).

128 Così, l'interpretazione della direttiva 2002/58, che viene in discussione nel caso di specie, deve essere effettuata unicamente alla luce dei diritti fondamentali garantiti dalla Carta (v., in tal senso, sentenza del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 46 e la giurisprudenza ivi citata).

129 Inoltre, occorre ricordare che le spiegazioni relative all'articolo 52 della Carta precisano che l'articolo 52, paragrafo 3, di quest'ultima intende assicurare la necessaria coerenza tra la Carta stessa e la CEDU, «senza che ciò pregiudichi l'autonomia del diritto dell'Unione e della Corte di giustizia dell'Unione europea» (sentenza del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 47). In

particolare, come espressamente previsto dall'articolo 52, paragrafo 3, seconda frase, della Carta, l'articolo 52, paragrafo 3, prima frase, di quest'ultima non osta a che il diritto dell'Unione conceda una protezione più estesa di quella offerta dalla CEDU. A ciò si aggiunge infine il fatto che l'articolo 8 della Carta riguarda un diritto fondamentale distinto rispetto a quello sancito all'articolo 7 della Carta e che non trova alcun equivalente nella CEDU.

130 Orbene, secondo una consolidata giurisprudenza della Corte, la ragione che giustifica una domanda di pronuncia pregiudiziale non è la formulazione di opinioni consultive su questioni generiche o ipotetiche, bensì il bisogno inerente all'effettiva soluzione di una controversia vertente sul diritto dell'Unione (v., in tal senso, sentenze del 24 aprile 2012, Kamberaj, C-571/10, EU:C:2012:233, punto 41; del 26 febbraio 2013, Åkerberg Fransson, C-617/10, punto 42, nonché del 27 febbraio 2014, Pohotovosť, C-470/12, punto 29).

131 Nel caso di specie, alla luce delle considerazioni svolte in particolare ai punti 128 e 129 della presente sentenza, la questione se la protezione conferita dagli articoli 7 e 8 della Carta vada al di là di quella garantita dall'articolo 8 della CEDU non è idonea a influire sull'interpretazione della direttiva 2002/58, letta alla luce della Carta, che viene in discussione nel procedimento principale nella causa C-698/15.

132 Dunque, non consta che una risposta al secondo quesito nella causa C-698/15 possa apportare elementi di interpretazione del diritto dell'Unione che siano necessari per la soluzione, alla luce di tale diritto, della controversia suddetta.

133 Ne consegue che la seconda questione nella causa C-698/15 è irricevibile.

Sulle spese

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

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

1) L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre

2009, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata 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.

2) L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione.

3) La seconda questione sollevata dalla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (divisione per le cause in materia civile), Regno Unito] è irricevibile.

Firme