

SENTENZA DELLA CORTE (Grande Sezione)

8 aprile 2014 (*)

«Comunicazioni elettroniche – Direttiva 2006/24/CE – Servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione – Conservazione di dati generati o trattati nell’ambito della fornitura di tali servizi – Validità – Articoli 7, 8 e 11 della Carta dei diritti fondamentali dell’Unione europea»

Nelle cause riunite C-293/12 e C-594/12,

aventi ad oggetto domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell’articolo 267 TFUE, dalla High Court (Irlanda) e dal Verfassungsgerichtshof (Austria), con decisioni, rispettivamente, del 27 gennaio e 28 novembre 2012, pervenute in cancelleria l’11 giugno e il 19 dicembre 2012, nei procedimenti

Digital Rights Ireland Ltd (C-293/12)

contro

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Irlanda,

The Attorney General,

con l’intervento di:

Irish Human Rights Commission,

e

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl e a.,

LA CORTE (Grande Sezione),

composta da V. Skouris, presidente, K. Lenaerts, vicepresidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relatore), E. Juhász, A. Borg Barthet, C.G. Fernlund e J.L. da Cruz Vilaça, presidenti di sezione, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader e C. Vajda, giudici,

avvocato generale: P. Cruz Villalón

cancelliere: K. Malacek, amministratore

vista la fase scritta del procedimento e in seguito all'udienza del 9 luglio 2013,

considerate le osservazioni presentate:

- per la Digital Rights Ireland Ltd, da F. Callanan, SC, e F. Crehan, BL, incaricati da S. McGarr, solicitor;
- per M. Seitlinger, da G. Otto, Rechtsanwalt;
- per C. Tschohl e a., da E. Scheucher, Rechtsanwalt;
- per l'Irish Human Rights Commission, da P. Dillon Malone, BL, incaricato da S. Lucey, solicitor;
- per l'Irlanda, da E. Creedon e D. McGuinness, in qualità di agenti, assistiti da E. Regan, SC, e D. Fennelly, JC;
- per il governo austriaco, da G. Hesse e G. Kunnert, in qualità di agenti;
- per il governo spagnolo, da N. Díaz Abad, in qualità di agente;
- per il governo francese, da G. de Bergues, D. Colas e B. Beaupère-Manokha, in qualità di agenti;
- per il governo italiano, da G. Palmieri, in qualità di agente, assistita da A. De Stefano, avvocato dello Stato;
- per il governo polacco, da B. Majczyna e M. Szpunar, in qualità di agenti;
- per il governo portoghese, da L. Inez Fernandes e C. Vieira Guerra, in qualità di agenti;
- per il governo del Regno Unito, da L. Christie, in qualità di agente, assistito da S. Lee, barrister;
- per il Parlamento europeo, da U. Rösslein, A. Caiola e K. Zejdová, in qualità di agenti;
- per il Consiglio dell'Unione europea, da J. Monteiro, E. Sitbon e I. Šulce, in qualità di agenti;
- per la Commissione europea, da D. Maidani, B. Martenczuk e M. Wilderspin, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 12 dicembre 2013,

ha pronunciato la seguente

Sentenza

1 Le domande di pronuncia pregiudiziale vertono sulla validità 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 L 105, pag. 54).

2 La domanda proposta dalla High Court (causa C-293/12) verte su una controversia che contrappone la Digital Rights Ireland Ltd (in prosieguito: la «Digital Rights») al Minister for Communications, Marine and Natural Resources, al Minister for Justice, Equality and Law Reform, al Commissioner of the Garda Síochána, all'Irlanda nonché all'Attorney General, in merito alla legittimità di misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche.

3 La domanda proposta dal Verfassungsgerichtshof (causa C-594/12) è relativa a ricorsi in materia costituzionale proposti dinanzi a tale organo giurisdizionale dalla Kärntner Landesregierung (governo del Land di Carinzia) nonché dai sigg. Seitlinger, Tschohl e da altri 11 128 ricorrenti, in merito alla compatibilità della legge che attua la direttiva 2006/24 nel diritto interno austriaco con la legge costituzionale federale (Bundes-Verfassungsgesetz).

Contesto normativo

La direttiva 95/46/CE

4 La direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31), è volta, conformemente al suo articolo 1, paragrafo 1, a garantire la tutela delle libertà e dei diritti fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

5 Per quanto riguarda la sicurezza del trattamento di tali dati, l'articolo 17, paragrafo 1, della suddetta direttiva così recita:

«Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere».

La direttiva 2002/58/CE

6 La 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 L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU L 337, pag. 11; in prosieguito: la «direttiva 2002/58»), ha per obiettivo, ai sensi dell'articolo 1, paragrafo 1, l'armonizzazione delle disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle

apparecchiature e dei servizi di comunicazione elettronica all'interno dell'Unione europea. Ai sensi del paragrafo 2 del medesimo articolo, le disposizioni di tale direttiva precisano e integrano la direttiva 95/46 ai fini di cui al summenzionato paragrafo 1.

7 Per quanto riguarda la sicurezza del trattamento dei dati, l'articolo 4 della direttiva 2002/58 dispone quanto segue:

«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/CE, 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.

Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire.

2. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili».

8 Quanto alla riservatezza delle comunicazioni e dei dati relativi al traffico, l'articolo 5, paragrafi 1 e 3, della suddetta direttiva così recita:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

(...)

3. Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito

unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, 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 Ai sensi dell'articolo 6, paragrafo 1, della direttiva 2002/58:

«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».

10 L'articolo 15 della direttiva 2002/58, al paragrafo 1, enuncia quanto segue:

«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/CE, 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».

La direttiva 2006/24

11 Dopo aver promosso una consultazione di rappresentanti delle autorità di contrasto, del settore delle comunicazioni elettroniche e di esperti in materia di protezione dei dati, la Commissione ha presentato, il 21 settembre 2005, una valutazione dell'impatto delle opzioni politiche relative a regole in tema di conservazione dei dati relativi al traffico (in prosieguo: la «valutazione dell'impatto»). Tale valutazione è servita come base per l'elaborazione della proposta di direttiva del Parlamento Europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE [COM(2005) 438 def; in prosieguo: la «proposta di direttiva»], presentata lo stesso giorno, sfociata nell'adozione della direttiva 2006/24 sulla base dell'articolo 95 CE.

12 Il considerando 4 della direttiva 2006/24 così recita:

«L'articolo 15, paragrafo 1, della direttiva 2002/58/CE enumera le condizioni a cui gli Stati membri possono limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi 1, 2, 3 e 4, e all'articolo 9 di tale direttiva. Ogni restrizione di questo tipo deve essere necessaria, opportuna e proporzionata, all'interno di una società democratica, per specifici fini di ordine pubblico, vale a dire per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, o per la prevenzione, indagine, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato dei sistemi di comunicazione elettronica».

13 Ai sensi della prima frase del considerando 5 della direttiva 2006/24, «[d]iversi Stati membri hanno adottato normative sulla conservazione di dati da parte dei fornitori dei servizi a fini di prevenzione, indagine, accertamento e perseguimento dei reati».

14 I considerando da 7 a 11 della direttiva 2006/24 sono formulati nel modo seguente:

«(7) Le conclusioni del Consiglio “Giustizia e affari interni” del 19 dicembre 2002 sottolineano che, a motivo dell’importante aumento delle possibilità offerte dalle comunicazioni elettroniche, i dati relativi all’uso di queste ultime costituiscono uno strumento particolarmente importante e valido nella prevenzione, indagine, accertamento e perseguimento dei reati, in particolare della criminalità organizzata.

(8) Con la dichiarazione sulla lotta al terrorismo, adottata il 25 marzo 2004, il Consiglio europeo ha incaricato il Consiglio di esaminare misure relative all’istituzione di norme sulla conservazione dei dati relativi al traffico delle comunicazioni da parte dei fornitori di servizi.

(9) In base all’articolo 8 della Convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali (CEDU) [firmata a Roma il 4 novembre 1950], ogni persona ha diritto al rispetto della sua vita privata e della sua corrispondenza. Non può esservi ingerenza della pubblica autorità nell’esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria tra l’altro per la sicurezza nazionale, l’ordine pubblico, la prevenzione di disordini o reati, la protezione dei diritti e delle libertà altrui. Giacché la conservazione dei dati si è dimostrata uno strumento investigativo necessario ed efficace per le autorità di contrasto in vari Stati membri, riguardanti in particolare reati gravi come la criminalità organizzata e il terrorismo, risulta necessario assicurare che i dati conservati restino a disposizione delle autorità di contrasto per un certo periodo di tempo alle condizioni previste dalla presente direttiva. (...)

(10) Il 13 luglio 2005 il Consiglio ha ribadito nella sua dichiarazione di condanna degli attacchi terroristici di Londra la necessità di adottare al più presto misure comuni in materia di conservazione dei dati relativi alle telecomunicazioni.

(11) Data l’importanza dei dati relativi al traffico e dei dati relativi all’ubicazione per l’indagine, l’accertamento e il perseguimento dei reati, come dimostrato da lavori di ricerca e dall’esperienza pratica di diversi Stati membri, è necessario garantire a livello europeo la conservazione, per un certo periodo di tempo, alle condizioni previste dalla presente direttiva, dei dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione».

15 I considerando 16, 21 e 22 di detta direttiva precisano quanto segue:

«(16) Gli obblighi incombenti ai fornitori di servizi per quanto concerne le misure atte ad assicurare la qualità dei dati, che derivano dall’articolo 6 della direttiva 95/46/CE e i loro obblighi concernenti le misure atte ad assicurare la riservatezza e la sicurezza dei trattamenti dei dati, derivanti dagli articoli 16 e 17 di tale direttiva, sono pienamente applicabili ai dati conservati ai sensi della presente direttiva.

(21) Poiché gli obiettivi della presente direttiva, ossia l’armonizzazione degli obblighi, per i fornitori, di conservare certi dati e di garantire che essi siano disponibili a fini di indagine, accertamento e perseguimento di reati gravi quali definiti da ciascuno Stato membro nella propria legislazione nazionale, non possono essere realizzati in misura sufficiente dagli Stati membri e

possono dunque, a causa della dimensione e degli effetti della presente direttiva, essere realizzati meglio a livello comunitario, la Comunità può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato. La presente direttiva si limita a quanto necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(22) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti, segnatamente nella Carta dei diritti fondamentali dell'Unione europea. In particolare, insieme alla direttiva 2002/58/CE, essa mira a garantire la piena osservanza dei diritti fondamentali del cittadino al rispetto della propria vita privata e delle proprie comunicazioni e alla protezione dei dati di carattere personale come previsto dagli articoli 7 e 8 della Carta».

16 La direttiva 2006/24 prevede, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o delle reti pubbliche di comunicazione, l'obbligo di conservare taluni dati da essi generati o trattati. Al riguardo, gli articoli da 1 a 9, 11 e 13 della detta direttiva dispongono quanto segue:

«Articolo 1

Oggetto e campo d'applicazione

1. La presente direttiva ha l'obiettivo di armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale.
2. 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.

Articolo 2

Definizioni

1. Ai fini della presente direttiva si applicano le definizioni contenute nella direttiva 95/46/CE, nella direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (...), e nella direttiva 2002/58/CE.
2. Ai fini della presente direttiva si intende per:
 - a) “dati”: i dati relativi al traffico e i dati relativi all'ubicazione, così come i dati connessi necessari per identificare l'abbonato o l'utente;
 - b) “utente”: qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per fini privati o professionali, senza essere necessariamente abbonata a tale servizio;
 - c) “servizio telefonico”: le chiamate telefoniche (incluse chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati), i servizi supplementari (inclusi l'inoltro e il trasferimento di

chiamata), la messaggeria e i servizi multimediali (inclusi servizi di messaggeria breve, servizi medialti avanzati e servizi multimediali);

d) “identificativo dell’utente”: un identificativo unico assegnato a una persona al momento dell’abbonamento o dell’iscrizione presso un servizio di accesso Internet o un servizio di comunicazione Internet;

e) “etichetta di ubicazione”: l’identità della cellula da cui una chiamata di telefonia mobile ha origine o nella quale si conclude;

f) “tentativo di chiamata non riuscito”: una chiamata telefonica che è stata collegata con successo ma non ha ottenuto risposta, oppure in cui vi è stato un intervento del gestore della rete.

Articolo 3

Obbligo di conservazione dei dati

1. In deroga agli articoli 5, 6 e 9 della direttiva 2002/58/CE, 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.

Articolo 4

Accesso ai dati

Gli Stati membri adottano misure per garantire che i dati conservati ai sensi della presente direttiva siano trasmessi solo alle autorità nazionali competenti, in casi specifici e conformemente alle normative nazionali. Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell’Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l’interpretazione della Corte europea dei diritti dell’uomo.

Articolo 5

Categorie di dati da conservare

1. Gli Stati membri provvedono affinché in applicazione della presente direttiva siano conservate le seguenti categorie di dati:

- a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:
 - 1) per la telefonia di rete fissa e la telefonia mobile:
 - i) numero telefonico chiamante;
 - ii) nome e indirizzo dell'abbonato o dell'utente registrato;
 - 2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet:
 - i) identificativo/i dell'utente;
 - ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica;
 - iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico;
- b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:
 - 1) per la telefonia di rete fissa e la telefonia mobile:
 - i) numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa;
 - ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i;
 - 2) per la posta elettronica su Internet e la telefonia via Internet:
 - i) identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet;
 - ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione;
- c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:
 - 1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione;
 - 2) per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet:
 - i) data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;
 - ii) data e ora del log-in e del log-off del servizio di posta elettronica su Internet o del servizio di telefonia via Internet sulla base di un determinato fuso orario;

- d) i dati necessari per determinare il tipo di comunicazione:
 - 1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato;
 - 2) per la posta elettronica Internet e la telefonia Internet: il servizio Internet utilizzato;
 - e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:
 - 1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati;
 - 2) per la telefonia mobile:
 - i) numeri telefonici chiamanti e chiamati;
 - ii) International Mobile Subscriber Identity (IMSI) del chiamante;
 - iii) International Mobile Equipment Identity (IMEI) del chiamante;
 - iv) l'IMSI del chiamato;
 - v) l'IMEI del chiamato;
 - vi) nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione;
 - 3) per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet:
 - i) numero telefonico chiamante per l'accesso commutato (dial-up access);
 - ii) digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione;
 - f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:
 - 1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;
 - 2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.
2. A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione.

Articolo 6

Periodi di conservazione

Gli Stati membri provvedono affinché le categorie di dati di cui all'articolo 5 siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione.

Articolo 7

Protezione e sicurezza dei dati

Fatte salve le disposizioni adottate in conformità della direttiva 95/46/CE e della direttiva 2002/58/CE, ogni Stato membro provvede a che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione rispettino, come minimo, i seguenti principi di sicurezza dei dati per quanto concerne i dati conservati in conformità della presente direttiva:

- a) i dati conservati sono della stessa qualità e sono soggetti alla stessa sicurezza e tutela dei dati in rete;
- b) i dati sono soggetti ad adeguate misure tecniche e organizzative intese a tutelarli da una distruzione accidentale o illecita, da un'alterazione o perdita accidentale, da immagazzinamento, trattamento, accesso o divulgazione non autorizzati o illeciti;
- c) i dati sono soggetti ad adeguate misure tecniche e organizzative intese a garantire che gli stessi possono essere consultati soltanto da persone appositamente autorizzate;

e

- d) i dati vengono distrutti alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati.

Articolo 8

Condizioni di immagazzinamento dei dati conservati

Gli Stati membri provvedono affinché i dati di cui all'articolo 5 siano conservati conformemente alla presente direttiva in modo che i dati conservati e ogni altra informazione necessaria ad essi collegata possano essere trasmessi immediatamente alle autorità competenti su loro richiesta.

Articolo 9

Autorità di controllo

1. Ogni Stato membro designa una o più autorità pubbliche quali responsabili del controllo dell'applicazione sul suo territorio delle disposizioni adottate dagli Stati membri in conformità dell'articolo 7 per quanto concerne la sicurezza dei dati conservati. Dette autorità possono essere le stesse autorità di cui all'articolo 28 della direttiva 95/46/CE.

2. Le autorità di cui al paragrafo 1 esercitano in totale indipendenza il controllo di cui al detto paragrafo.

(...)

Articolo 11

Modifica della direttiva 2002/58/CE

All'articolo 15 della direttiva 2002/58/CE è inserito il seguente paragrafo:

“1 *bis*. Il paragrafo 1 non si applica ai dati la cui conservazione è specificamente prevista dalla [direttiva 2006/24], ai fini di cui all’articolo 1, paragrafo 1, di tale direttiva”.

(...)”.

Articolo 13

Ricorsi giurisdizionali, responsabilità e sanzioni

1. Ogni Stato membro adotta le misure necessarie per garantire che le misure nazionali di attuazione del capo III della direttiva 95/46/CE in materia di ricorsi giurisdizionali, responsabilità e sanzioni siano pienamente attuate con riferimento al trattamento di dati nel quadro della presente direttiva.

2. In particolare, ciascuno Stato membro adotta le misure necessarie per garantire che qualsivoglia accesso o trasferimento intenzionale di dati conservati in conformità della presente direttiva, che non sia autorizzato dalle disposizioni nazionali di attuazione della stessa, sia passibile di sanzioni, anche a carattere amministrativo o penale, che sono efficaci, proporzionate e dissuasive».

Procedimenti principali e questioni pregiudiziali

La causa C-293/12

17 L’11 agosto 2006 la Digital Rights ha presentato dinanzi alla High Court un ricorso nell’ambito del quale sostiene di essere proprietaria di un telefono cellulare che è stato registrato il 3 giugno 2006 e da essa utilizzato a partire da tale data. Essa mette in discussione la legittimità di misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche e chiede, in particolare, al giudice del rinvio di dichiarare la nullità della direttiva 2006/24 e della parte settima della legge del 2005 sulla giustizia penale (reati terroristici) [Criminal Justice (Terrorist Offences) Act 2005], la quale impone ai fornitori di servizi di telefonia di conservare i dati relativi al traffico e all’ubicazione per un lasso di tempo specificato dalla legge a fini di prevenzione, accertamento, indagini o perseguimento dei reati e di protezione della sicurezza dello Stato.

18 Ritenendo di non essere in grado di risolvere le questioni relative al diritto nazionale ad essa sottoposte senza che fosse stata prima esaminata la validità della direttiva 2006/24, la High Court ha deciso di sospendere il giudizio e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se la limitazione dei diritti della ricorrente in relazione all’utilizzo della telefonia mobile, derivante dalle disposizioni degli articoli 3, 4 e 6 della direttiva 2006/24/CE, sia incompatibile con l’articolo 5, paragrafo 4, TUE in quanto non proporzionata, non necessaria o non adeguata per il perseguimento dei seguenti obiettivi legittimi:

a) garantire la disponibilità di determinati dati a fini di indagine, accertamento e perseguimento di reati gravi,

e/o

b) garantire il corretto funzionamento del mercato interno dell’Unione europea.

2) In particolare,

- a) se la direttiva 2006/24/CE sia compatibile con il diritto dei cittadini di circolare e soggiornare liberamente nel territorio degli Stati membri sancito dall'articolo 21 TFUE;
- b) se la direttiva 2006/24/CE sia compatibile con il diritto al rispetto della vita privata sancito dall'articolo 7 della [Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la "Carta")] e dall'articolo 8 della [CEDU];
- c) se la direttiva 2006/24/CE sia compatibile con il diritto alla protezione dei dati di carattere personale sancito all'articolo 8 della Carta;
- d) se la direttiva 2006/24/CE sia compatibile con il diritto alla libertà di espressione sancito dall'articolo 11 della Carta e dall'articolo 10 della [CEDU];
- e) se la direttiva 2006/24/CE sia compatibile con il diritto ad una buona amministrazione contemplato dall'articolo 41 della Carta.

3) In che misura i Trattati – e, in particolare, il principio di leale collaborazione di cui all'articolo 4, paragrafo 3, TUE – impongano al giudice nazionale di esaminare e valutare la compatibilità delle misure nazionali volte a trasporre la direttiva 2006/24/CE con le garanzie previste dalla [Carta], ivi compreso il suo articolo 7 (come ispirato dall'articolo 8 della [CEDU])».

La causa C-594/12

19 All'origine della domanda di pronuncia pregiudiziale nella causa C-594/12 si trovano numerosi ricorsi presentati dinanzi al Verfassungsgerichtshof, proposti rispettivamente dalla Kärntner Landesregierung nonché dai sigg. Seitlinger, Tschohl e da altri 11 128 ricorrenti che chiedono l'annullamento dell'articolo 102 *bis* della legge sulle telecomunicazioni (Telekommunikationsgesetz 2003), articolo introdotto in tale legge dalla legge federale di modifica della stessa (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011) ai fini della trasposizione della direttiva 2006/24 nel diritto interno austriaco. Le suddette parti sostengono, in particolare, che l'articolo 102 *bis* viola il diritto fondamentale dei privati alla protezione dei propri dati.

20 Il Verfassungsgerichtshof si chiede, in particolare, se la direttiva 2006/24 sia compatibile con la Carta in quanto permette di immagazzinare una massa di dati relativi ad un numero illimitato di persone per un lungo tempo. La conservazione dei dati riguarderebbe quasi esclusivamente persone il cui comportamento non giustifica affatto la conservazione dei dati che le riguardano. Tali persone sarebbero esposte ad un rischio elevato di vedere le autorità ricercare i loro dati, venire a conoscenza del relativo contenuto, informarsi sulla loro vita privata e utilizzare tali dati per molteplici fini, tenuto conto, segnatamente, del numero incalcolabile di persone che hanno accesso ai dati per un periodo di almeno sei mesi. Secondo il giudice del rinvio, vi sono dubbi, da un lato, circa il fatto che la direttiva sia idonea al raggiungimento degli obiettivi da essa perseguiti e, dall'altro lato, circa la proporzionalità dell'ingerenza nei diritti fondamentali interessati.

21 Il Verfassungsgerichtshof ha pertanto deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Sulla validità degli atti delle istituzioni dell'Unione:

Se gli articoli da 3 a 9 della direttiva 2006/24 siano compatibili con gli articoli 7, 8 e 11 della [Carta].

2) Sull'interpretazione dei Trattati

a) Se, alla luce delle spiegazioni relative all'articolo 8 della Carta che, a norma dell'articolo 52, paragrafo 7, della stessa, sono state elaborate al fine di fornire orientamenti per l'interpretazione [di quest'ultima] e di cui il Verfassungsgerichtshof deve tenere debito conto, la direttiva 95/46 e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [GU 2001, L 8, pag. 1] debbano essere considerati equivalenti alle condizioni stabilite dall'articolo 8, paragrafo 2, e dall'articolo 52, paragrafo 1, della Carta per valutare l'ammissibilità delle ingerenze.

b) Quale sia il rapporto tra il "diritto dell'Unione", menzionato nell'articolo 52, paragrafo 3, ultima frase, della Carta, e le direttive in materia di protezione dei dati.

c) Se, dato che la direttiva 95/46/CE e il regolamento (...) n. 45/2001 pongono condizioni e limiti all'esercizio del diritto fondamentale alla protezione dei dati sancito dalla Carta, nell'interpretare l'articolo 8 [di quest'ultima] occorra tener conto dei cambiamenti derivanti dalle norme successive di diritto derivato.

d) Se, in considerazione dell'articolo 52, paragrafo 4, della Carta, dal principio della salvaguardia di livelli di protezione più elevati, di cui all'articolo 53 della Carta, discenda che i limiti che [quest'ultima] pone alle restrizioni che il diritto derivato può legittimamente apportare debbano essere applicati in base a criteri più rigorosi.

e) Se, tenuto conto dell'articolo 52, paragrafo 3, della Carta, del quinto comma del preambolo e delle spiegazioni relative all'articolo 7 [di quest'ultima], secondo cui i diritti garantiti da tale articolo corrispondono a quelli garantiti dall'articolo 8 della CEDU, la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'articolo 8 della CEDU possa fornire indicazioni interpretative rilevanti ai fini dell'interpretazione di quest'ultimo articolo».

22 Con decisione del presidente della Corte dell'11 giugno 2013, le cause C-293/12 e C-594/12 sono state riunite ai fini della fase orale e della sentenza.

Sulle questioni pregiudiziali

Sulla seconda questione, lettere da b) a d), nella causa C-293/12 e sulla prima questione nella causa C-594/12

23 Con la seconda questione, lettere da b) a d), nella causa C-293/12 e la prima questione nella causa C-594/12, che vanno esaminate congiuntamente, i giudici del rinvio chiedono in sostanza alla Corte di esaminare la validità della direttiva 2006/24 alla luce degli articoli 7, 8 e 11 della Carta.

Sulla rilevanza degli articoli 7, 8 e 11 della Carta con riferimento alla questione di validità della direttiva 2006/24

24 Dall'articolo 1 e dai considerando 4, 5, da 7 a 11, 21 e 22 della direttiva 2006/24 emerge che l'obiettivo principale di quest'ultima è quello di armonizzare le disposizioni degli Stati membri relative alla conservazione, da parte dei fornitori di servizi di comunicazione elettronica accessibili

al pubblico o di una rete pubblica di comunicazione, di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di prevenzione, indagine, accertamento e perseguimento di reati gravi, come quelli legati alla criminalità organizzata e al terrorismo, nel rispetto dei diritti sanciti agli articoli 7 e 8 della Carta.

25 L'obbligo dei fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, previsto dall'articolo 3 della direttiva 2006/24, di conservare i dati elencati all'articolo 5 della stessa al fine di renderli all'occorrenza accessibili alle autorità nazionali competenti solleva questioni relative alla protezione tanto della vita privata quanto delle comunicazioni, sancita dall'articolo 7 della Carta, alla tutela dei dati personali, prevista dall'articolo 8 della stessa, nonché al rispetto della libertà di espressione, garantita dall'articolo 11 della Carta.

26 In proposito, va rilevato che i dati che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione debbono conservare, ai sensi degli articoli 3 e 5 della direttiva 2006/24, sono, in particolare, i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, per stabilire la data, l'ora, la durata e il tipo di una comunicazione, le attrezzature di comunicazione degli utenti nonché per determinare l'ubicazione delle apparecchiature di comunicazione mobile, dati tra i quali figurano, segnatamente, il nome e l'indirizzo dell'abbonato o dell'utente registrato, il numero telefonico chiamante e quello chiamato, nonché un indirizzo IP per i servizi Internet. I suddetti dati permettono, in particolare, di sapere quale sia la persona con cui un abbonato o un utente registrato ha comunicato e con quale mezzo, così come di stabilire il tempo della comunicazione e il luogo dal quale questa è avvenuta. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con talune persone nel corso di un determinato periodo.

27 Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati.

28 Di conseguenza, sebbene la direttiva 2006/24 non autorizzi, come emerge dagli articoli 1, paragrafo 2, e 5, paragrafo 2 della stessa, la conservazione del contenuto della comunicazione e delle informazioni consultate utilizzando una rete di comunicazione elettronica, non è escluso che la conservazione dei dati di cui trattasi possa incidere sull'utilizzo, da parte degli abbonati o degli utenti registrati, dei mezzi di comunicazione cui fa riferimento la suddetta direttiva e, di conseguenza, sull'esercizio, da parte di questi ultimi, della loro libertà di espressione, garantita dall'articolo 11 della Carta.

29 La conservazione dei dati affinché le autorità nazionali competenti possano eventualmente accedervi, come prevista dalla direttiva 2006/24, riguarda in modo specifico e diretto la vita privata e, di conseguenza, i diritti garantiti dall'articolo 7 della Carta. Inoltre, tale conservazione dei dati rientra altresì nell'articolo 8 di quest'ultima, poiché costituisce un trattamento dei dati di carattere personale ai sensi del suddetto articolo e deve, pertanto, necessariamente rispondere ai requisiti di protezione dei dati derivanti da tale articolo (sentenza Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punto 47).

30 Benché i rinvii pregiudiziali nelle presenti cause sollevino, in particolare, la questione di principio di stabilire se i dati degli abbonati e degli utenti registrati possano o meno essere conservati, alla luce dell'articolo 7 della Carta, essi riguardano altresì la questione se la direttiva 2006/24 risponda alle esigenze di protezione dei dati personali derivanti dall'articolo 8 della Carta.

31 Tenuto conto delle considerazioni che precedono, al fine di rispondere alla seconda questione, lettere da b) a d), nella causa C-293/12 e la prima questione nella causa C-594/12, occorre esaminare la validità della direttiva alla luce degli articoli 7 e 8 della Carta.

Sull'esistenza di un'ingerenza nei diritti sanciti dagli articoli 7 e 8 della Carta

32 Imponendo la conservazione dei dati elencati all'articolo 5, paragrafo 1, della direttiva 2006/24 e permettendo l'accesso delle autorità nazionali competenti a questi ultimi, la suddetta direttiva, come rilevato dall'avvocato generale in particolare ai paragrafi 39 e 40 delle sue conclusioni, deroga al regime di tutela del diritto al rispetto della vita privata, istituito dalle direttive 95/46 e 2002/58, con riferimento al trattamento dei dati personali nel settore delle comunicazioni elettroniche, in quanto le suddette direttive hanno previsto la riservatezza delle comunicazioni e dei dati relativi al traffico nonché l'obbligo di cancellare o di rendere anonimi i dati stessi quando non siano più necessari alla trasmissione di una comunicazione, a meno che non siano necessari per la fatturazione e solo fintanto che tale necessità perduri.

33 Per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, poco importa che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (v., in tal senso, sentenza *Österreichischer Rundfunk* e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 75).

34 Di conseguenza, l'obbligo, imposto dagli articoli 3 e 6 della direttiva 2006/24 ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica, di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni, come quelli previsti dall'articolo 5 della suddetta direttiva, costituisce di per sé un'ingerenza nei diritti garantiti dall'articolo 7 della Carta.

35 Inoltre, l'accesso delle autorità nazionali competenti ai dati costituisce un'ingerenza supplementare in tale diritto fondamentale (v., per quanto riguarda l'articolo 8 della CEDU, sentenze della Corte EDU, *Leander c. Svezia*, del 26 marzo 1987, serie A n. 116, § 48; *Rotaru c. Romania* [GC], n. 28341/95, § 46, CEDU 2000-V, nonché *Weber e Saravia c. Germania* (dec.), n. 54934/00, § 79, CEDU 2006-XI). Pertanto, anche gli articoli 4 e 8 della direttiva 2006/24, i quali prevedono regole relative all'accesso delle autorità nazionali competenti ai dati, sono costitutivi di un'ingerenza nei diritti garantiti dall'articolo 7 della Carta.

36 Parimenti, la direttiva 2006/24 è costitutiva di un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, poiché prevede un trattamento dei dati personali.

37 È giocoforza constatare che l'ingerenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta si rivela essere, come peraltro osserva l'avvocato generale, in particolare ai paragrafi 77 e 80 delle sue conclusioni, di vasta portata e va considerata particolarmente grave. Inoltre, il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate, come rilevato dall'avvocato generale ai paragrafi 52 e 72 delle sue conclusioni, la sensazione che la loro vita privata sia oggetto di costante sorveglianza.

Sulla giustificazione dell'ingerenza nei diritti garantiti dagli articoli 7 e 8 della Carta

38 Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge, rispettare il loro contenuto essenziale e, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a detti diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

39 Per quanto riguarda il contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all'articolo 7 della Carta, si deve rilevare che, sebbene la conservazione dei dati imposta dalla direttiva 2006/24 costituisca un'ingerenza particolarmente grave in tali diritti, essa non è tale da pregiudicare il suddetto contenuto poiché, come deriva dall'articolo 1, paragrafo 2, della stessa direttiva, quest'ultima non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale.

40 Tale conservazione dei dati non è neppure idonea a pregiudicare il contenuto essenziale del diritto fondamentale alla protezione dei dati personali, sancito all'articolo 8 della Carta, considerato che la direttiva 2006/24 prevede, all'articolo 7, una regola relativa alla protezione e alla sicurezza dei dati ai sensi della quale, fatte salve le disposizioni adottate in conformità delle direttive 95/46 e 2002/58, i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati, principi in base ai quali gli Stati membri assicurano l'adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l'alterazione accidentale dei dati.

41 Quanto alla questione consistente nell'accertare se la suddetta ingerenza risponda a un obiettivo di interesse generale, occorre rilevare che, sebbene la direttiva 2006/24 sia destinata ad armonizzare le disposizioni degli Stati membri relative agli obblighi dei suddetti fornitori in materia di conservazione di taluni dati da essi generati o trattati, l'obiettivo sostanziale della direttiva consiste, come risulta dall'articolo 1, paragrafo 1, della stessa, nel garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale. L'obiettivo sostanziale della direttiva è pertanto quello di contribuire alla lotta contro la criminalità grave e, di conseguenza, in ultima analisi, alla sicurezza pubblica.

42 Come emerge dalla giurisprudenza della Corte, la lotta contro il terrorismo internazionale finalizzata al mantenimento della pace e della sicurezza internazionali costituisce un obiettivo di interesse generale dell'Unione (v., in tal senso, sentenze Kadi e Al Barakaat International Foundation/Consiglio e Commissione, C-402/05 P e C-415/05 P, EU:C:2008:461, punto 363, nonché Al-Aqsa/Consiglio, C-539/10 P e C-550/10 P, EU:C:2012:711, punto 130). Lo stesso vale per la lotta contro la criminalità grave al fine di garantire la sicurezza pubblica (v., in tal senso, sentenza Tsakouridis, C-145/09, EU:C:2010:708, punti 46 e 47). Inoltre, va rilevato, a tal proposito, che l'articolo 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma altresì alla sicurezza.

43 Al riguardo, dal considerando 7 della direttiva 2006/24 emerge che, a motivo dell'importante aumento delle possibilità offerte dalle comunicazioni elettroniche, il Consiglio «Giustizia e affari interni» del 19 dicembre 2002 ha considerato che i dati relativi all'uso di queste ultime costituiscono uno strumento particolarmente importante e valido nella prevenzione dei reati e nella lotta contro la criminalità, in particolare della criminalità organizzata.

44 È gioco forza constatare quindi che la conservazione dei dati per permettere alle autorità nazionali competenti di disporre di un accesso eventuale agli stessi, come imposto dalla direttiva 2006/24, risponde effettivamente a un obiettivo di interesse generale.

45 Di conseguenza, è necessario verificare la proporzionalità dell'ingerenza constatata.

46 A questo proposito, si deve ricordare che il principio di proporzionalità esige, secondo una costante giurisprudenza della Corte, che gli atti delle istituzioni dell'Unione siano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi (v., in tal senso, sentenze *Afton Chemical*, C-343/09, EU:C:2010:419, punto 45; *Volker und Markus Schecke e Eifert*, EU:C:2010:662, punto 74; *Nelson e a.*, C-581/10 e C-629/10, EU:C:2012:657, punto 71; *Sky Österreich*, C-283/11, EU:C:2013:28, punto 50, nonché *Schaible*, C-101/12, EU:C:2013:661, punto 29).

47 Per quanto riguarda il controllo giurisdizionale del rispetto delle suddette condizioni, allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi garantito dalla Carta, la natura e la gravità dell'ingerenza nonché la finalità di quest'ultima (v., per analogia, per quanto riguarda l'articolo 8 della CEDU, sentenza Corte EDU, *S e Marper c. Regno Unito* [GC], nn. 30562/04 e 30566/04, § 102, CEDU 2008-V).

48 Nel caso di specie, tenuto conto, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, della portata e della gravità dell'ingerenza in tale suddetto diritto che la direttiva 2006/24 comporta, il potere discrezionale del legislatore dell'Unione risulta ridotto e di conseguenza è necessario procedere ad un controllo stretto.

49 Per quel che riguarda la questione consistente nell'accertare se la conservazione dei dati sia idonea a realizzare l'obiettivo perseguito dalla direttiva 2006/24, si deve constatare che, tenuto conto della crescente importanza dei mezzi di comunicazione elettronica, i dati che debbono essere conservati in attuazione della detta direttiva permettono alle autorità nazionali competenti in materia di perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi e, al riguardo, costituiscono quindi uno strumento utile per le indagini penali. Pertanto, la conservazione dei suddetti dati può essere considerata come idonea a realizzare l'obiettivo perseguito dalla suddetta direttiva.

50 Questa valutazione non può essere rimessa in discussione dal fatto, invocato in particolare dai sigg. Tschohl e Seitlinger nonché dal governo portoghese nelle loro osservazioni scritte presentate alla Corte, che esistono diversi modi di comunicazione elettronica i quali non ricadono nell'ambito di applicazione della direttiva 2006/24 o che permettono una comunicazione anonima. Benché questo fatto possa, in effetti, relativizzare l'idoneità della misura di conservazione dei dati a raggiungere l'obiettivo perseguito, esso non è tuttavia tale da rendere detta misura inadeguata, come rilevato dall'avvocato generale al punto 137 delle sue conclusioni.

51 Quanto al carattere necessario della conservazione dei dati imposta dalla direttiva 2006/24, si deve constatare che, invero, la lotta contro la criminalità grave, in particolare contro la criminalità organizzata e il terrorismo, è di capitale importanza per garantire la sicurezza pubblica e la sua efficacia può dipendere in larga misura dall'uso delle moderne tecniche di indagine. Tuttavia, simile obiettivo di interesse generale, per quanto fondamentale, non può di per sé giustificare il fatto che

una misura di conservazione, come quella istituita dalla direttiva 2006/24, sia considerata necessaria ai fini della suddetta lotta.

52 Per quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale, secondo la costante giurisprudenza della Corte, richiede in ogni caso che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario (sentenza IPI, C-473/12, EU:C:2013:715, punto 39 e giurisprudenza ivi citata).

53 A questo proposito, occorre ricordare che la tutela dei dati personali, risultante dall'obbligo esplicito previsto all'articolo 8, paragrafo 1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita provata sancito dall'articolo 7 della stessa.

54 Pertanto, la normativa dell'Unione di cui trattasi deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati (v., per analogia, per quanto riguarda l'articolo 8 della CEDU, sentenze Corte EDU, *Liberty* e altri c. Regno Unito, n. 58243/00, §§ 62 e 63, del 1° luglio 2008; *Rotaru* c. Romania, cit., §§ da 57 a 59, nonché *S e Marper* c. Regno Unito, cit., § 99).

55 La necessità di disporre di siffatte garanzie è tanto più importante allorché, come prevede la direttiva 2006/24, i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (v., per analogia, con riguardo all'articolo 8 della CEDU, sentenze Corte EDU, *S e Marper* c. Regno Unito, cit., § 103, nonché *M.K.* c. Francia, n. 19522/09, § 35, del 18 aprile 2013).

56 Quanto alla questione consistente nell'accertare se l'ingerenza che la direttiva 2006/24 comporta sia limitata allo stretto necessario, si deve rilevare che tale direttiva impone, conformemente al suo articolo 3, in combinato disposto con l'articolo 5, paragrafo 1, della stessa, la conservazione di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l'accesso a Internet, la posta elettronica su Internet nonché la telefonia via Internet. Pertanto, essa concerne tutti i mezzi di comunicazione elettronica il cui uso è estremamente diffuso e di importanza crescente nella vita quotidiana di ciascuno. Inoltre, conformemente all'articolo 3, la direttiva riguarda tutti gli abbonati e gli utenti registrati. Essa implica pertanto un'ingerenza nei diritti fondamentali della quasi totalità della popolazione europea.

57 A questo proposito, si deve rilevare, in primo luogo, che la direttiva 2006/24 riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi.

58 Infatti, da un lato, la direttiva 2006/24 riguarda in maniera globale l'insieme delle persone che fanno uso dei mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali. Essa pertanto si applica anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi. Inoltre, essa non prevede alcuna deroga, e pertanto si applica anche a persone le cui comunicazioni sono soggette, in base alle norme del diritto nazionale, al segreto professionale.

59 Dall'altro lato, pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per

la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi.

60 In secondo luogo, alla suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'articolo 1, paragrafo 1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno.

61 Inoltre, per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative. L'articolo 4 della direttiva, che regola l'accesso di tali autorità ai dati conservati, non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative, ma si limita a prevedere che ciascuno Stato membro definisca le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità.

62 In particolare, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito. Soprattutto, l'accesso ai dati conservati da parte delle autorità nazionali competenti non è subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente la cui decisione sia diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per raggiungere l'obiettivo perseguito e intervenga a seguito di una richiesta motivata delle suddette autorità presentata nell'ambito di procedure di prevenzione, di accertamento o di indagini penali. Non è neppure stato previsto un obbligo preciso degli Stati membri volto a stabilire simili limitazioni.

63 In terzo luogo, quanto alla durata di conservazione dei dati, la direttiva 2006/24 impone, all'articolo 6, la conservazione degli stessi per un periodo di almeno sei mesi senza che venga effettuata alcuna distinzione tra le categorie di dati previste all'articolo 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate.

64 Tale durata, inoltre, si colloca tra un minimo di sei mesi e un massimo di ventiquattro mesi, senza che venga precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario.

65 Da quanto precede deriva che la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.

66 Per di più, per quanto riguarda le norme riguardanti la sicurezza e la protezione dei dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, si deve constatare che la direttiva 2006/24 non prevede garanzie sufficienti, come richieste dall'articolo 8 della Carta, che permettano di assicurare una protezione efficace dei dati conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati. Infatti, in primo luogo, l'articolo 7 della direttiva 2006/24 non prevede norme specifiche e adatte alla vasta quantità dei dati di cui la direttiva impone la conservazione, al carattere sensibile dei suddetti dati nonché al rischio di accesso illecito a questi ultimi, norme che servirebbero, in particolare, a regolare in maniera chiara e precisa la protezione e la sicurezza dei dati di cui trattasi, al fine di garantirne la piena integrità e riservatezza. Inoltre, non è stato neppure previsto un obbligo preciso degli Stati membri di stabilire siffatte norme.

67 L'articolo 7 della direttiva 2006/24, in combinato disposto con gli articoli 4, paragrafo 1, della direttiva 2002/58 e 17, paragrafo 1, secondo comma, della direttiva 95/46, non garantisce che sia applicato dai detti fornitori un livello particolarmente elevato di protezione e di sicurezza attraverso misure tecniche e organizzative, ma autorizza in particolare i suddetti fornitori a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato, per quanto riguarda i costi di attuazione delle misure di sicurezza. In particolare, la direttiva 2006/24 non garantisce la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi.

68 In secondo luogo, si deve aggiungere che tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti. Orbene, siffatto controllo, effettuato in base al diritto dell'Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali (v., in tal senso, sentenza Commissione/Austria, C-614/10, EU:C:2012:631, punto 37).

69 Alla luce dell'insieme delle osservazioni che precedono, si deve considerare che, adottando la direttiva 2006/24, il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta.

70 Di conseguenza, non vi è motivo di esaminare la validità della direttiva 2006/24 alla luce dell'articolo 11 della Carta.

71 Occorre pertanto rispondere alla seconda questione, lettere da b) a d), nella causa C-293/12 e alla prima questione nella causa C-594/12 dichiarando che la direttiva 2006/24 è invalida.

Sulla prima questione e sulla seconda questione, lettere a) ed e), nonché sulla terza questione nella causa C-293/12 e sulla seconda questione nella causa C-594/12

72 Da quanto dichiarato al punto precedente deriva che non vi è motivo di rispondere alla prima questione, alla seconda questione, lettere a) ed e), e alla terza questione nella causa C-293/21, né alla seconda questione nella causa C-594/12.

Sulle spese

73 Nei confronti delle parti nei procedimenti principali le presenti cause costituiscono un incidente sollevato dinanzi ai giudici nazionali, 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:

La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, è invalida.