CORTE DI GIUSTIZIA UE
GRANDE SEZIONE
8 APRILE 2014
CAUSE RIUNITE
C-293/12 C-594/12

PRESIDENTE: SKOURIS

RELATORE: VON DANWITZ

PARTI: DIGITAL RIGHTS IRELAND LTD

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**

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.

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 prosieguo: 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 prosieguo: 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 mediali 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'ar-

ticolo 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 giocoforza 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.

P.Q.M. — 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.

La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra

1. Una Sentenza attesa.

La sentenza resa dalla Corte di Giustizia l'8 aprile 2014 a definizione dei procedimenti C-293/12 e C-594/12 [1] segna una tappa importante nel percorso di affermazione delle libertà civili nell'ambito del processo di integrazione comunitaria. Essa, infatti, bilanciando il diritto alla vita privata e la protezione dei dati personali con l'esigenza di perseguire i reati, dichiara invalida la direttiva 2006/24/CE del Parlamento e del Consiglio sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o di reti pubbliche di comunicazione [2], per avere ecceduto, in modo sproporzionato, nella difesa di quest'ultima a danno dei diritti summenzionati.

Si tratta di una decisione che ha suscitato da subito entusiastiche prese di posizione, anche in sede istituzionale [3], da parte di chi auspicava una maggiore tutela per il diritto alla vita privata, e in effetti non si può negare che, nel suo complesso, la decisione possa apparire condivisibile, in quanto ispirata, come vedremo, ad un bilanciamento equilibrato tra tutti gli interessi in gioco. Nondimeno, non mancano nella pronuncia alcuni spunti a nostro avviso pericolosi sia in quanto espressivi di un non condivisibile eccessivo favore per la tutela della vita privata a fronte di

[1] Per la precisione, si tratta di due questioni pregiudiziali di validità sollevate ai sensi dell'art. 267 TFUE rispettivamente dalla *High Court* irlandese e dal *Verfassungsgerichtshof* austriaco.

[2] Ricordiamo, per inciso, che tale atto era già stato oggetto di una precedente decisione (causa C-301/06, in *curia.eu*) in cui la Corte di Giustizia aveva rigettato il ricorso dell'Irlanda, secondo la quale la direttiva non era strumento idoneo in quanto la disciplina sarebbe dovuta rientrare (allora) nel terzo e non nel primo pilastro dell'Unione. Sulla vicenda, per tutti, cfr. F. Fabbrini, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quad. cost.*, 2009, 419 ss.

[3] Come la dichiarazione resa dalla Vicepresidente della Commissione europea, secondo cui « La Corte di Giustizia ha confermato che la sicurezza non è un superdiritto che prevale sulla (legislazione della) protezione dei dati » (*cfr.* La Stampa, 8 aprile 2014) e il comunicato in pari data del Presidente dell'Autorità garante per la protezione dei dati personali, in cui si legge che « La sentenza della Corte di giustizia dell'Unione europea va nella direzione da noi sempre auspicata di una più marcata tutela dei diritti [...] La sentenza opera un riequilibrio tra due valori, sicurezza e privacy, che in questi anni si erano decisamente disallineati. Occorrerà una revisione dell'attuale sistema nel segno del principio di proporzionalità e delle garanzie per i cittadini ». Tali reazioni, del resto, non stupiscono, se si rammenta che la direttiva era stata oggetto di critiche fin dalla sua approvazione proprio da parte delle Autorità nazionali di garanzia per la protezione dei dati e che alcune Corti costituzionali — segnatamente quelle rumena e tedesca — avevano annullato le normative interne di attuazione lasciando trasparire una (non troppo celata) perplessità di fondo sul sistema generalizzato di conservazione dei dati introdotto dalla direttiva, ancorché questa non fosse stata impugnata. Per maggiori approfondimenti su queste posizioni cfr. C. Fatta, *La tutela della privacy alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*; e A. De Petris, *L'approccio giurisprudenziale alla tutela della privacy informatica: capacità innovativa e tradizione costituzionalistica*, entrambi in questa *Rivista* 2008, rispettivamente 408 ss. e 911 ss.; nonché M. Foglia, *Valori comuni in materia di privacy e trattamento dei dati personali*, in questa *Rivista*, 2010, 516 ss.

istanze di non minor valore sia perché forieri di possibili interpretazioni "estremizzanti", in sede di traduzione normativa tanto a livello comunitario quanto nazionale, che potrebbero dare luogo ad un deciso sbilanciamento nella garanzia dei diritti poc'anzi citati. Nel seguito ripercorreremo pertanto in sintesi i punti principali che, in positivo ed in negativo, ci sembra caratterizzino la decisione, per poi fornire qualche indicazione su eventuali risvolti che questa potrebbe avere sul nostro ordinamento.

2. L'INQUADRAMENTO DELLA QUESTIONE.

L'inquadramento generale della questione svolto dal giudice di Lussemburgo pare ineccepibile.

È infatti pienamente condivisibile la riconduzione della disciplina recata dalla direttiva agli artt. 7 ed 8 della Carta dei diritti fondamentali dell'Unione europea che riconoscono, rispettivamente, il diritto al rispetto della vita privata e quello alla protezione dei dati di carattere personale [4], così come del tutto corretta è la precisazione che la cd. ***data retention*** costituisce certamente un'ingerenza su (e quindi una limitazione di) tali situazioni soggettive [5]. Allo stesso modo è apprezzabile la precisazione che questa restrizione, ispirata, com'è, ad una *ratio* di salvaguardia della sicurezza pubblica e di lotta alla criminalità, può essere agevolmente ricondotta alla cura di un interesse generale meritevole di tutela, stante l'importanza e l'utilità che la conservazione dei dati delle conversazioni riveste ai fini investigativi [6]. Del resto, il giudice di Lussemburgo ben evidenzia che le previsioni della direttiva riguardano la possibilità di accedere solo ai dati esterni delle comunicazioni e non al loro contenuto, di modo che la limitazione subita dalle situazioni soggettive coinvolte non appare tale da potersi considerare come menomazione del nucleo centrale inviolabile dei diritti in parola, ciò che sarebbe precluso dall'art. 52, par. 1, della Carta dei diritti. L'unica critica che, da questo punto di vista, può muoversi alla pronuncia è quella di non aver richiamato, almeno *in parte qua*, i precedenti giurisprudenziali nei quali già si affermava che in ambito comunitario il diritto alla vita privata può (*rectius*: deve) essere bilanciato con altri interessi generali di rango primario con cui entrasse in conflitto [7]. Senza contare le numerose pronunce in tal senso della Corte

---

[4] Prescindiamo qui totalmente dalla problematica ricostruzione delle due situazioni soggettive come autonome, secondo la tesi fatta propria dalla Corte di giustizia, ovvero come declinazioni di un unico diritto, come ci pare preferibile. Per maggiori approfondimenti e riferimenti bibliografici ci permettiamo di rinviare a S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Roma 2013, spec. 31 ss. e 120 ss.

[5] Come del resto, rispetto all'art. 8 CEDU anche la Corte europea dei diritti dell'uomo aveva stabilito fin dalla risalente pronuncia 2 agosto 1984 *Malone contro Regno Unito*, in *hudoc.echr.coe.int*, giustamente richiamata nella sentenza in commento. Per una sintetica rassegna dell'evoluzione successiva sul punto della giurisprudenza europea v. M. CARTA, *Diritto alla vita privata e Internet nell'esperienza giuridica europea ed internazionale*, in questa *Rivista*, 2014, 9 ss.

[6] In tema si vedano soprattutto i paragrafi 29-44 della pronuncia, dove, per la precisione, la Corte parla di un obiettivo di interesse generale dell'Unione in riferimento solo alla lotta al terrorismo ed alla criminalità grave. Per gli argomenti che inducono a non condividere questa specificazione rinviamo al successivo par. 3.

[7] Alludiamo, per esempio, alla sentenza *Adidas* (C-223/98, in *curia.eu*), ove la Corte di Giustizia aveva deciso nel senso

europea dei diritti dell'uomo, le quali tuttavia, a ben vedere, nella decisone in commento vengono in generale richiamate in modo decisamente limitato, nonostante il quesito espressamente formulato in tal senso da parte di uno dei giudici *a quibus*, così che la Corte di giustizia sembra orientata a dare al caso una soluzione tutta interna alla Carta comunitaria. Il che, probabilmente, è frutto di una precisa scelta di "politica giurisprudenziale", su cui non è qui possibile soffermarsi, volta ad emancipare il giudice comunitario da una sorta di tutela da parte dell'omologo internazionale nella garanzia dei diritti [8].

3. Nel merito: alcuni *pro*...

Se l'inquadramento della fattispecie appare corretto, possono essere in larga parte condivise anche le conseguenze che la Corte ne fa discendere circa il merito della questione, allorché essa, avallata in astratto la necessità di un bilanciamento tra i diritti e gli interessi generali coinvolti, passa a valutare in concreto il rispetto dei principi di necessità e di proporzionalità nelle scelte del legislatore.

Anzitutto, molto opportunamente il giudice comunitario, all'osservazione delle parti di uno dei processi *a quibus* e del Governo portoghese, secondo cui la eventuale insufficienza dei mezzi investigativi in questione per la possibilità che le comunicazioni criminali assumano forme diverse non rientranti nella sfera di applicazione dell'atto normativo impugnato avrebbe reso potenzialmente inutile l'invasione nella sfera privata e quindi illegittima la direttiva, risponde che non per questo la conservazione dei dati è per ciò stesso automaticamente una limitazione sproporzionata della riservatezza. Ché anzi, aggiungiamo noi, proprio il fatto che i criminali abbiano a disposizione altri mezzi non può indurre, sotto il profilo logico, a rinunciare agli strumenti, pur limitati, che si hanno a disposizione, pena la totale abdicazione ad ogni forma di lotta alla criminalità [9]. Al contrario, proprio tale circostanza dovrebbe portare a concludere, semmai, per la necessità di un allargamento dell'ambito di applicazione della normativa fino a cercare di ricomprendere ogni canale atto a perseguire gli autori di reati.

Sgombrato il campo da questa eccezione, il giudice comunitario procede quindi alla ricognizione dell'estensione della limitazione che il diritto alla vita privata subisce ad opera delle previsioni della direttiva, sia sotto il profilo soggettivo (ovvero gli interessati dalla misura restrittiva), sia sotto il profilo oggettivo (in relazione al tipo e quantità di dati oggetto di conservazione), sia infine sotto il profilo spazio-temporale (ovvero se

della contrarietà al diritto comunitario di una normativa che impedisse al titolare di un marchio registrato, in nome della riservatezza, di conoscere l'identità del destinatario dell'importazione di merci contraffatte.

[8] Il punto è oggetto di analisi da parte di L. Trucco, *La Corte di giustizia si rifà alla Carta dei diritti fondamentali dell'UE e bilancia diritto alla vita privata e lotta alla criminalità*, in corso di pubblicazione in *Giur. It.*, fasc. 8-9/2014 cui rinviamo per un'attenta disamina.

[9] Tanto più che, al contrario, l'acquisizione dei dati rappresenta proprio uno strumento indispensabile, se non insostituibile, in relazione all'accertamento di determinati reati, come evidenziano S. Aterno - A. Costerna, *Il legislatore interviene ancora sul* data retention, *ma non è finita*, in *Dir. pen. proc.*, 2009, 286.

esistano limiti di luogo e di tempo rispetto ai dati da conservare). E l'esito dell'operazione porta inevitabilmente alla constatazione che massima è l'ampiezza della possibile restrizione sotto tutti i profili evidenziati, poiché la conservazione dei dati concerne tutti i cittadini, per qualunque tipo di comunicazione, senza limiti temporali o territoriali. Solo sotto il profilo oggettivo vi è una sorta di controlimite rappresentato dal fatto, di non trascurabile rilevanza, che non il contenuto ma solo il fatto storico dell'avvenuta comunicazione (data e ora della chiamata, durata della conversazione, ecc.) può essere oggetto di conservazione e di acquisizione.

Eseguita questa mappatura dell'estensione dell'ingerenza nella vita privata operata dalla direttiva, la Corte di Giustizia procede infine all'esame del rispetto del principio di proporzionalità secondo uno stretto scrutinio, giungendo ad una valutazione negativa per una pluralità di ragioni.

Rinviando al paragrafo successivo l'esame degli argomenti addotti che a nostro avviso non sono condivisibili, possiamo qui anzitutto richiamare, tra le valutazioni negative del giudice di Lussemburgo che ci sembrano, viceversa, meritevoli di adesione, quella relativa alla mancata previsione nella direttiva della necessità che l'accesso ai dati avvenga per il tramite di un'autorità giudiziaria o di un'autorità amministrativa terza e indipendente che assicuri l'effettivo rispetto della sola finalità ammessa, ovvero la prevenzione ed il perseguimento dei reati. Si tratta, in effetti, di una garanzia forse anche più importante di quella relativa al limite temporale di conservazione, perché, se è vero che l'aumento di quest'ultimo porta con sé un prolungamento del rischio di potenziale lesione del diritto alla vita privata, non è men vero che allorché un'autorità pubblica accede ai dati si ha proprio in quel momento una limitazione certa e concreta del medesimo diritto, di modo che è principalmente in questa fase che l'ordinamento è chiamato a predisporre le idonee misure di garanzia [10].

Allo stesso modo, si può ben aderire a quanto la Corte afferma laddove censura come non proporzionata la previsione di una durata minima e massima del periodo di conservazione senza che siano definiti criteri oggettivi atti a garantire che l'accesso ai dati sia consentito entro i limiti dello stretto necessario. In particolare, la direttiva non differenzia in alcun modo la durata del periodo né in relazione ai vari tipi di dati né relativamente alle persone cui questi si riferiscono, lasciando quindi aperta la possibilità agli Stati membri di fissare, in sede di attuazione, un unico termine generalizzato, prescindendo così da ogni valutazione di proporzionalità.

Un terzo ed ultimo motivo che sorregge la dichiarazione di illegittimità riguarda le misure di sicurezza. La direttiva, infatti — osserva il giudice comunitario — autorizza i fornitori di servizi di comunicazione a bilanciare le misure da assumere con il costo economico delle stesse, consentendo l'adozione di standards non particolarmente elevati, e non impone che detta conservazione avvenga nel territorio dell'Unione, talché i dati

[10] Il punto è messo in luce con particolare vigore da C. Conti, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in S. Lorusso (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova 2008, 30 ss.

potrebbero essere trattati in uno Stato privo di una Autorità indipendente di controllo, come invece richiesto dall'art. 8, par. 3 della Carta. Non solo, ma la direttiva, pur prevedendo che tra le misure debba essere prevista la distruzione dei dati allo scadere del periodo, non assicura però che questa sia definitiva. Osservazioni tutte condivisibili, sebbene il problema dei costi che la protezione dei dati comporta non sia aspetto da sottovalutare e vada attentamente tenuto in conto nella previsione delle misure di sicurezza, stimando quanto le finanze pubbliche sotto l'attuale tensione possano contribuire a sostenerle.

In buona sintesi, dunque, tutti questi elementi concorrono nel far affermare alla Corte di giustizia che la direttiva, pur introducendo una disciplina sì limitativa della vita privata ma non per questo illegittima in quanto tale, non assicura, però, al contempo, attraverso misure sufficientemente chiare e precise, che la restrizione dei diritti coinvolti non ecceda i confini dello stretto necessario. Sul punto è bene insistere perché esso ci appare centrale per bene comprendere — e circoscrivere alla sua effettiva portata — il senso della pronuncia. La opportunità e legittimità della scelta di consentire la conservazione (anche generalizzata) dei dati, in buona sostanza, non è di per sé illegittima alla luce della Carta dei diritti e non è incompatibile con la tutela della vita privata e la protezione dei dati personali, ma è solo l'insufficiente e inadeguata previsione di controlli e garanzie nell'accesso e nella conservazione stessa dei dati a giustificare la censura [11]. Una pronuncia, dunque, sotto questo profilo decisamente equilibrata, il cui seguito da parte del legislatore comunitario non presuppone necessariamente una restrizione in sé della possibilità di conservazione dei dati, quale invece era fatta propria dalla Commissione in sede di predisposizione di una proposta di modifica [12], ma semplicemente un aumento delle garanzie.

4. *Segue:* ... e alcuni *contra*.

Se per i profili sinora analizzati la sentenza appare condivisibile, in essa non mancano tuttavia alcuni elementi meritevoli di un commento critico.

[11] Di modo che, se il riferimento all'identità costituzionale tedesca ed il richiamo alla celebre pronuncia *Lissabon-urteil* da parte del *Bundesverfassungsgericht* nella pronuncia citata *supra*, nota 3 e di cui meglio si dirà nel paragrafo successivo, erano state lette (per esempio da parte di A. Di Martino, *Il* Bundesverfassungsgericht *dichiara l'incostituzionalità della* data retention *e torna sul rapporto tra libertà e sicurezza*, in *Giur. cost.*, 2014, 4058 ss.) come una critica di fondo alla conservazione generalizzata dei dati ed un segnale in questa direzione indirizzato al giudice comunitario, ci pare si possa affermare che, aldilà di qualche concessione alle argomentazioni del giudice tedesco, di cui pure si dirà nel paragrafo successivo, tale segnale non è stato nella sostanza recepito dalla Corte di giustizia.

[12] Occorre infatti ricordare che la Commissione, come annunciato nel *Report sullo stato di attuazione della direttiva 2006/24/CE* del 18 aprile 2011 COM(2011) 225 final, aveva avviato uno studio, anche attraverso il supporto dell'*International Working Group on Data Protection in Telecommunications*, per riformare la direttiva oggi invalidata, nel quale tra l'altro, si prevedeva una riduzione della durata dei termini di conservazione, secondo quanto riferito al Parlamento europeo dalla Commissaria Malmström nell'ottobre del 2012. Notizie sul punto nella Relazione 2012 del Garante per la protezione dei dati personali, in *www.garanteprivacy.it*, documento web 2470702, 297 ss.

Anzitutto, superflua e di per sé eccessiva ci sembra l'affermazione, che la Corte riprende direttamente dalle Conclusioni dell'Avvocato generale, secondo cui il fatto che la conservazione dei dati e l'accesso ad essi avvengano all'insaputa dell'utilizzatore è suscettibile di ingenerare tra le persone la sensazione che la propria vita privata sia oggetto di sorveglianza costante. Questo argomento, infatti, benché riprenda considerazioni già espresse anche dal Gruppo Art. 29 fin dalle prime osservazioni sulla direttiva [13] e sia stata sostenuta anche da autorevole dottrina [14], trascura il fatto che la mera conservazione dei dati, laddove sia effettuata secondo misure di sicurezza adeguate, non comporta in realtà di per sé alcuna effettiva lesione della riservatezza né alcuno stigma a danno di coloro che vedono registrati i propri dati, laddove invece i benefici che agli stessi possono derivarne, in termini di strumenti a disposizione per l'Autorità Giudiziaria nella lotta alla criminalità, ci paiono maggiormente concreti e significativi [15].

Del resto, questo passaggio della sentenza, che a ben vedere non costituisce che un *obiter dictum* senza influire sul merito della decisione finale, sembra più che altro una strizzata d'occhio al *Bundesverfassungsgericht* che, accogliendo migliaia di ricorsi presentati da Associazioni per i diritti civili, ha annullato, con la sentenza del 2 marzo 2010, la disciplina tedesca sulla *data retention* [16] — la quale peraltro stabiliva termini di conservazione pari al minimo previsto dalla direttiva — sul presupposto che sarebbe addirittura lo stesso funzionamento della democrazia ad essere messo a repentaglio, per il fatto che questa presuppone che

[13] Si veda infatti il parere n. 3 del 2006, in *www.garanteprivacy.it*, documento web 1411906, ove si legge che « la decisione di conservare i dati nell'intento di combattere i reati gravi è senza precedenti ed ha dimensione storica. Essa invade la vita quotidiana di ogni cittadino e può porre a repentaglio i valori di libertà fondamentali di cui godono e che rispettano tutti i cittadini europei ». Sugli interventi di questo organo precedenti l'adozione dell'atto in questione v. la ricostruzione di C. Fatta, *La tutela*, cit., 405 ss. Ricordiamo, per inciso, che il Gruppo di lavoro *ex* art. 29 è un organo consultivo e indipendente istituito appunto dall'art. 29 della direttiva 95/46/CE costituito da un rappresentante di ciascuna Autorità garante nazionale nonché dal Garante europeo per la protezione dei dati e da un rappresentante della Commissione europea.

[14] Nel nostro Paese si può citare, per tutti, S. Rodotà, *Intervista su privacy e libertà*, Roma-Bari 2005, 60; ripreso da M. Viggiano, *« Navigazione » in internet e acquisizione occulta di dati personali*, in questa *Rivista*, 2007, 380, la quale per questo motivo conclude che « il "costo assiologico" derivante dal sacrificio del diritto alla riservatezza [...] sembra troppo alto rispetto all'interesse di prevenzione dei reati ».

[15] Come scrive F. De Leo, *La conservazione dei dati di traffico davanti alla Corte costituzionale*, in *Quest. giust.*, 2005, 429, quando si va a bilanciare il rischio derivante dalla conservazione dei dati con le esigenze dell'istruttoria penale si verifica un caso in cui « di fronte a [una] situazione *reale* vi è una condizione potenziale e astratta, la condizione amorfa di dati la cui esistenza rappresenta un rischio eventuale e futuro » di « *contrasto ...tra un diritto e uno strumento* » (corsivi testuali). Non può pertanto nemmeno convenirsi con quanto sostiene M. Paissan, *La privacy è morta, viva la privacy*, Milano 2009, 60, a parere del quale « si mette oggi a rischio la riservatezza di tutti in vista di un possibile risultato domani, che potrà riguardare comunque un numero ristretto di persone », perché, se questo al massimo dimostra che entrambi gli aspetti (il pericolo di violazione della riservatezza e il beneficio derivante dalla conservazione dei dati per la lotta al crimine) possono avere carattere meramente potenziale allo stato attuale, non è però vero che l'accesso ai dati giovi a poche persone, perché se le vittime del reato ne traggono un vantaggio diretto, è chiaro che la persecuzione dei reati giova anche indirettamente alla società nel suo complesso.

[16] Le massime della sentenza sono consultabili in questa *Rivista*, 2010, 514 ss.

ciascuno si senta libero di utilizzare in sicurezza (anche) le comunicazioni elettroniche, mentre la consapevolezza che i dati siano conservati indurrebbe a modificare il proprio comportamento, negando appunto il pieno godimento di questa libertà [17].

Il punto della sentenza che tuttavia suscita a nostro avviso perplessità maggiori è il primo dei motivi che la Corte adduce a sostegno della illegittimità della direttiva, ovvero il fatto che essa non circoscrive l'accesso ai dati finalizzandolo alla sola repressione dei reati di particolare gravità, o meglio si limita, nell'art. 1, ad una previsione generica di tal fatta, lasciando però ciascuno Stato completamente libero di stabilire cosa rientri in questo concetto [18].

Ebbene, come abbiamo più ampiamente argomentato in altra sede in relazione alla disciplina nazionale in tema di intercettazioni di comunicazioni [19], qualunque reato, in quanto tale, giustifica sia la pretesa statale alla condanna del delinquente, sia la tutela della vittima che dal reato abbia visto leso un proprio diritto [20]: di fronte a queste esigenze, ci sembra che la tutela della vita privata non possa prevalere, laddove semmai è il ricorso allo strumento della sanzione penale che dovrebbe essere attentamente utilizzato dal legislatore e quindi riservato a fattispecie di effettiva gravità ed allarme sociale. Nella decisione in commento, insomma, ci pare che anche la Corte di Giustizia si adegui da questo punto di vista a quella (dominante) cultura giuridica — e non solo — che trascura come la potestà punitiva dello Stato non debba essere letta quale espressione di autorità che si oppone ai diritti di libertà dei consociati [21], poiché, esattamente al contrario, essa è strettamente funzionale alla

[17] Al riguardo M. Paissan, *La privacy*, cit., 69, riporta i dati emersi da uno studio condotto nel 2008 dalle associazioni ricorrenti, secondo cui, ad esempio, il 52% degli intervistati, dopo l'adozione dell'atto normativo impugnato, non utilizzava più canali telematici per determinate tipologie di servizi (consulenze matrimoniali, in tema di tossicodipendenza, ecc.).

[18] Nel senso fatto proprio dalla pronuncia del giudice comunitario si era già pronunciato il Gruppo Art. 29, ad esempio, in tempi recenti, nel parere n. 1 del 2012, reperibile in *www.garanteprivacy.it*, documento web 2572831, dove questo viene annoverato tra i limiti della direttiva. In termini analoghi, in riferimento alla normativa attuativa nazionale, si era espresso anche il Tribunale Costituzionale federale tedesco nella sentenza più volte citata.

[19] Ovvero S. Scagliarini, *Diritto alla riservatezza e pretesa punitiva dello Stato nella disciplina delle intercettazioni: un bilanciamento da ripensare*, in *Dir. soc.* 2012, spec. 513 ss., cui ci permettiamo di rinviare per un approfondimento maggiore.

[20] Il punto è bene evidenziato da F. De Leo, *La conservazione*, cit., 427, il quale contesta la tradizione della cultura giuridica che guarda alla dimensione autoritaria del diritto penale — e quindi si preoccupa maggiormente dei profili di oppressione verso il reo — di quanto non presti attenzione ai diritti di chi subisce il reato, ponendo perciò in secondo piano i profili di riparazione verso la vittima, la quale assume così un ruolo di « protagonista silenzioso », con cui si reitera l'offesa già subita con il reato.

[21] Cfr., per la critica di questa concezione, G. Gemma, *Diritto costituzionale e diritto penale: un rapporto da ridefinire*, in *Dir. soc.*, 1986, spec. 465 ss. e 484 ss. Simile, anche se poi difforme in alcune conclusioni, è la posizione di C. Sartoretti, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Torino 2008, 131, la quale afferma che tra sicurezza e diritti di libertà non vi è antinomia, la prima essendo funzionale ai secondi, anche se, proprio per questo, l'A. pone in particolare l'accento sul limite alla potestà punitiva derivante dal rispetto dei diritti inviolabili. *Contra*, in modo netto, si veda ad esempio T.E. Frosini, Privacy*: diritto fondamentale oppure no*, in *Federalismi.it*, n. 16/2008, secondo cui la costante prevalenza

garanzia della effettività dei diritti [22], di modo che una efficace garanzia delle libertà si ottiene proprio valorizzando ed agevolando per quanto possibile l'esigenza di accertamento dei reati e di punizione dei relativi responsabili [23].

In tal senso, del resto, si è espressa a più riprese anche la Corte europea dei diritti dell'uomo, secondo la quale da diverse norme convenzionali discende l'obbligo positivo per il legislatore sia di tutelare penalmente determinati beni sia di rendere effettiva ed efficace la sanzione penale [24], ed in dottrina analogo ragionamento è stato svolto proprio con riferimento alla Carta europea dei diritti fondamentali, che appunto, secondo una lettura cui ci sentiamo di aderire, impone essa stessa il ricorso allo strumento penale per contrastare le offese a (parte dei) diritti ivi riconosciuti [25]. Limitarsi, quindi, a sottolineare — come pure opportunamente fa il giudice comunitario — che è la stessa Carta dei diritti fondamentali ad annoverare all'art. 6 quello alla sicurezza, si inquadra solo parzialmente in questa prospettiva, giacché il discorso appare assai più ampio e generalizzato.

Insomma, quello che ci pare carente nella decisione in commento è una piena consapevolezza della strumentalità della repressione penale ad un'adeguata protezione delle libertà, ciò che avrebbe portato a non considerare un vizio di legittimità la mancata previsione, quale ulteriore garanzia in tema di accesso ai dati, di una limitazione di esso a gravi reati chiaramente specificati.

Né qui si pone il problema che la mancanza di limiti oggettivi all'ammissibilità di un accesso ai dati conservati comporti un impiego eccessivo

dei diritti dei cittadini « anche di fronte al diritto allo svolgimento dell'azione penale [...] non è garantismo, ma piuttosto costituzionalismo ».

[22] Si pensi, per fare un esempio evidente, alla funzionalità della repressione penale dell'omicidio ai fini di una reale tutela del diritto alla vita. In generale, sul tema, si vedano le argomentazioni, pienamente condivisibili, di P. Häberle, *Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz*, Heidelberg 1983, trad. it. *Le libertà fondamentali nello Stato costituzionale*, a cura di P. Ridola, Firenze 1993, 57 ss., il quale chiaramente afferma che essa è funzionale a « rendere operativi i valori che sono oggetto a loro volta dei diritti fondamentali », così che il suo scopo « non solo non è contrastare i diritti fondamentali, bensì opera[re] a favore loro e quindi anche a favore dell'individuo », configurandosi semmai « come *conseguenza* stessa delle libertà » (corsivo testuale).

[23] Come scrive O. Höffe, *Gibt es ein interkulturelles Strafrecht?*, trad. it. *Globalizzazione e diritto penale*, Torino 2001, IX, « il diritto penale rappresenta un elemento irrinunciabile dell'organizzazione di una società [...] nella funzione concreta di scudo protettivo dei diritti umani ed espressione del legame della società con le vittime della loro violazione ».

[24] In tal senso v., per esempio, la sentenza 14 ottobre 2010 *A. contro Croazia*, in *hudoc.echr.coe.int*, spec. paragrafo 67, ove si ritiene che proprio dall'art. 8 CEDU discenda l'obbligo di sanzionare penalmente la violenza domestica. Una significativa disamina di questi casi in cui la Corte di Strasburgo ritiene vi sia un obbligo positivo di tutela penale si rinviene in E. Nicosia, *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino 2006, 255 ss., il quale evidenzia che così la giurisprudenza aderisce alla tesi secondo cui il diritto penale non è solo uno strumento statale pericoloso per i diritti, ma anche uno strumento « utile, se non necessario e indispensabile, per una effettiva protezione ed affermazione degli stessi ». In tema, ampiamente, v. anche F. Bestagno, *Diritti umani e impunità*, Milano 2003, spec. 75 ss.

[25] Così, V. Militello, *I diritti fondamentali come oggetto di tutela penale*, in *Dir. pen. XXI secolo*, 2003, spec. 54 ss.; e C. Paonessa, *Gli obblighi di tutela penale*, Pisa 2009, spec. 193 ss., ove l'A. analizza anche qualche apertura nella giurisprudenza della Corte di Giustizia verso la possibilità per il legislatore comunitario di richiedere agli Stati membri l'adozione di normative penali.

di risorse di tempo, umane ed economiche se applicato a reati di minore gravità, come può affermarsi per le intercettazioni [26], perché in questo caso tutte le comunicazioni vengono comunque ed *a priori* tracciate, non potendosi sapere prima cosa risulterà utile per una indagine penale, di modo che rinunciare per fattispecie meno gravi, ma pur sempre qualificabili come criminose, ad utilizzare dati disponibili, ove naturalmente ne sia dimostrata l'utilità a fini investigativi, equivale semplicemente a rinunciare ad una efficace attività di lotta alla criminalità che non trova alcuna giustificazione nella Carta dei diritti fondamentali ed anzi, come abbiamo testé cercato di dimostrare, va soltanto a detrimento delle situazioni soggettive che essa si cura di tutelare.

5. I (POSSIBILI?) RIFLESSI DELLA PRONUNCIA SULLA NORMATIVA ITALIANA.

Resta ora da chiarire, come ci eravamo prefissi, quali conseguenze la pronuncia della Corte di giustizia può avere — in attesa del seguito che il legislatore comunitario è tenuto a dare — sul nostro ordinamento. In particolare, ci si potrebbe chiedere se la normativa interna di recepimento possa dirsi essa stessa, per l'operare del meccanismo di cui all'art. 117, comma 1, Cost., incostituzionale in quanto contrastante con i parametri evocati innanzi al giudice di Lussemburgo [27].

Per rispondere al quesito, occorre anzitutto rammentare che la materia è regolata dall'art. 132 del d. lgs. n. 196 del 2003, come novellato da ultimo dal d. lgs. n. 109 del 2008, proprio in recepimento della direttiva ora annullata [28]. Tale disposizione stabilisce oggi che i dati di traffico telefonico devono essere conservati per 24 mesi (12 per il traffico telematico, 30 giorni per le chiamate senza risposta) per le esigenze di accertamento e repressione dei reati e che essi sono acquisiti con decreto motivato del Pubblico Ministero. È inoltre prevista la possibilità per il Ministro dell'interno ed alcuni soggetti da questi eventualmente delegati di ordinare al fornitore del servizio di conservare e proteggere, per un periodo non superiore a novanta giorni e prorogabile fino al termine massimo di sei mesi, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, per lo svolgimento delle investigazioni preventive in tema di criminalità organizzata o di terrorismo, ovvero per finalità di accertamento e repressione di specifici reati. In questo caso, tuttavia, i provvedimenti dell'Autorità di polizia sono comunicati, per iscritto ed entro quarantotto ore dalla notifica al destinatario, al Pubblico Ministero del luogo di esecuzione per la eventuale convalida [29].

[26] Tanto che, proprio per questo motivo, possono giustificarsi i limiti di ammissibilità che per esse sono stabiliti dal nostro codice di procedura. Ci permettiamo di rinviare nuovamente a S. SCAGLIARINI, *Diritto*, cit., 514 ss.

[27] Sugli artt. 7 ed 8 della Carta dei diritti fondamentali dell'Unione europea quali fondamento costituzionale interposto, *ex* art. 117, comma 1, Cost., del diritto alla riservatezza, in quanto « "rami alti" di un sistema multilivello » parla C. SARTORETTI, *Contributo*, cit., 59 ss., da cui è tratta l'espressione virgolettata. Per maggiori approfondimenti si veda anche, volendo, S. SCAGLIARINI, *La riservatezza*, cit., 121 ss.

[28] Per una ricostruzione delle formulazioni precedenti di questa travagliata disposizione cfr. E. BASSOLI, *Acquisizione dei tabulati* vs. privacy*: la* data retention *al vaglio della Consulta*, in *Dir. internet*, 2007, 240 ss.

[29] Ricordiamo che tali ultime previsioni sono state introdotte con la legge n. 48

Ebbene, è nostra opinione che pure dopo la sentenza in esame la legittimità della disciplina nazionale non venga meno, dato che, se esaminiamo il d. lgs. n. 196 del 2003 alla luce delle motivazioni che sorreggono la pronuncia della Corte di giustizia, è facile avvedersi di come i profili di mancato rispetto del principio di proporzionalità non possano addebitarsi anche alla nostra disciplina interna [30].

In primo luogo, infatti, il nostro ordinamento non consente un accesso indiscriminato ai dati, bensì richiede un atto motivato del Pubblico Ministero, figura che, come noto, è riconducibile all'ampia nozione di Autorità Giudiziaria [31], né sono consentiti interventi dell'Autorità di polizia se non convalidati dal medesimo Pubblico Ministero. Insomma, il requisito del controllo giurisdizionale, la cui mancanza rappresenta uno dei vizi della direttiva, appare invece soddisfatto, sia pure oggi nella più blanda forma del decreto del P.M. [32], dalla nostra legislazione attuativa. Né il mancato intervento del giudice in senso stretto pare censurabile, essendo opinione largamente condivisa in dottrina [33] — e fatta propria anche dalla Corte costituzionale [34] e dalla Cassazione [35] — che anche la stringente disciplina dell'art. 15 Cost., a nostro avviso più severa e restrittiva di quella comunitaria, sia pienamente soddisfatta dal decreto del Pubblico Ministero, laddove l'intervento del G.I.P. in questa fase e per una restrizione limitata della privacy quale la mera apprensione dei

del 2008 in attuazione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica: in tema, v., anche con considerazioni critiche sulla coerenza rispetto alla disciplina generale, A. Stracuzzi, *Data retention: il faticoso percorso dell'art. 132 Codice privacy nella disciplina della conservazione dei dati di traffico*, in questa *Rivista* 2008, 609 ss.

[30] Non potendosi pertanto condividere il severo giudizio di C. Fatta, *La tutela*, cit., 395 ss. che critica ampiamente non solo la normativa interna precedente l'attuazione della direttiva, ma anche quella vigente, per il fatto di essersi appiattita sulla (criticabile, ad avviso dell'A.) disciplina comunitaria « senza un significativo incremento di garanzie per la tutela della vita privata ».

[31] La considerazione è pacifica in dottrina (ove, per tutti, v. di recente N. Zanon - F. Biondi, *Il sistema costituzionale della magistratura*, Bologna 2006, 127) ed è peraltro condivisa dalla Consulta, che si è pronunciata in tal senso fin dalla sentenza n. 96 del 1975, consultabile in *Giur. cost.* 1975, 835 ss.

[32] Ricordiamo infatti che nella precedente formulazione la norma prevedeva il controllo del giudice, addirittura senza nemmeno la possibilità di un intervento in caso di urgenza da parte del P.M. Del resto, come afferma correttamente F. De Leo, *Due o tre cose su dati di traffico e tutela della privacy*, in *Quest. giust.*, 2004, 835, la previsione precedente dell'intervento del giudice si giustificava per l'esistenza del doppio binario, di modo che l'acquisizione dei dati oltre i primi 24 mesi di conservazione presupponeva un filtro giudiziale per verificare la sussistenza dei più restrittivi presupposti previsti dalla legge per questa ipotesi.

[33] *Ex plurimis*, G. Illuminati, *La disciplina processuale delle intercettazioni*, Milano 1983, 61; A. Camon, *Le intercettazioni nel processo penale*, Milano 1996, 109; nonché C. Parodi, *Le intercettazioni*, Torino 2002, 57. *Contra*, M. Viggiano, « *Navigazione* », cit., 380 ss., che ritiene non adeguatamente assolta la riserva di giurisdizione per la potenziale conoscibilità del contenuto della comunicazione derivante dall'accesso al mero dato esterno di una comunicazione telematica; e R. Miranda, *Gli obblighi del gestore: esigenze di "data protection" o di "data retention"?* in A. Pace - R. Zaccaria - G. De Minico (a cura di), *Mezzi di comunicazione e riservatezza*, Napoli 2008, 230 ss., che critica l'attribuzione di questa funzione al Pubblico Ministero in quanto organo privo della richiesta terzietà.

[34] Ci riferiamo alle sentenze nn. 81 del 1993 e 281 del 1998, consultabili in *Giur. cost.* rispettivamente 1993, 731 ss. e 1998, 2167 ss.

[35] Per la posizione della Suprema Corte si veda Cass. pen., Sez. un., 23 febbraio 2000, in *Giur. it.*, 2001, 1701 ss.

dati esterni della comunicazione rappresenterebbe soltanto un appesantimento procedurale non compensato da alcuna maggiore garanzia [36].

In secondo luogo, è vero che l'attuale disciplina nazionale non distingue in base alla gravità del reato per cui si indaga al fine di graduare il periodo di durata della conservazione, ma questo perché il maggiore o minore disvalore del fatto [37] incide semmai (anche se sul punto abbiamo già espresso le nostre riserve su cui torneremo a breve) sulla disciplina dell'accesso e non già della conservazione, che comunque è destinata a durare fino allo spirare del termine previsto per il più grave dei reati. Ciò non toglie, inoltre, che il legislatore italiano abbia comunque introdotto un criterio per graduare la durata assumendo a parametro il tipo di dato conservato [38], distinguendo perciò il caso di quelli telefonici (per i quali è confermato il periodo di 24 mesi già previsto nella formulazione della norma precedente la direttiva [39]) rispetto a quello dei dati telematici (12 mesi), dimostrando così di ritenere troppo invasiva la conservazione prolungata di questi ultimi, sul presupposto che per essi il dato esteriore della comunicazione può coincidere con l'identificazione del contenuto della medesima [40]. Sennonché, appare forse eccessivo ridurre il termine addirittura della metà, perché non solo si deve osservare che analogo potere rivelatore possiedono i dati di alcune chiamate telefoniche (si pensi per esempio ad una linea erotica) [41], ma soprattutto, dopo l'entrata in vigore del d. lgs. n. 109 del 2008, che elenca i dati oggetto di conserva-

[36] Così argomenta M. Pinna, *"Doppio binario" di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giur. cost.* 2006, 3929 ss., che evidenzia come in assenza di criteri normativi l'intervento del giudice non sarebbe servito che a prendere atto della richiesta di un altro soggetto, peraltro non tenuto a motivare la propria istanza e ne avrebbe comportato una inopportuna ingerenza nella scelta degli strumenti investigativi.

[37] Come ha ricordato anche la Corte costituzionale nella sentenza n. 372 del 2006 (in *Giur. cost.*, 2006, 3916 ss.), in cui, nel rigettare la questione di costituzionalità sulla norma al nostro esame nella sua formulazione precedente, il giudice delle leggi aveva ritenuto giustificabile il protrarsi (per un periodo doppio di quello attuale!) del termine di conservazione soltanto per reati di maggiore gravità perché in quel modo veniva mantenuta una proporzione tra lesività del reato e ampiezza della limitazione della riservatezza.

[38] Analogamente, peraltro, a quanto faceva il progetto originariamente proposto dalla Commissione: in generale, sulle modifiche subite dal testo della direttiva nel corso del suo *iter* cfr. S. Monteleone, *La tutela dei dati personali nelle comunicazioni elettroniche tra esigenze di* Data Protection *e obblighi di* Data Retention, in P. Costanzo - G. De Minico - R. Zaccaria (a cura di), *I « tre codici » della Società dell'informazione*, Torino 2006, spec. 348 ss.

[39] Si osservi, per inciso, che l'Italia non si è avvalsa dalla facoltà, prevista dall'art. 12 della direttiva, di ampliare il termine di conservazione, previa notifica alla Commissione e comunicazione agli altri Stati membri, per circostanze eccezionali, magari conservando quello già vigente di 48 mesi. Sul punto v. C. Conti, *L'attuazione*, cit., 16 ss., la quale, pur rilevando che la presenza strutturale della criminalità organizzata nel nostro Paese avrebbe in effetti impedito di poterla ricondurre alla clausola eccezionale di deroga di cui alla direttiva, non nasconde la oggettiva difficoltà che ne consegue per le indagini su tali reati, all'evidenza lunghe e complesse, così che « la disciplina fa prevalere la tutela della riservatezza sul diritto alla prova e sull'interesse all'accertamento dei fatti ». Laddove, peraltro, come ricorda M. Carta, *Diritto*, cit., 10, la Corte europea dei diritti dell'uomo, almeno in relazione a reati particolarmente gravi, in un suo precedente ha ritenuto giustificabile persino un termine di conservazione di 30 anni.

[40] L'osservazione è ricorrente in dottrina; *ex plurimis*, cfr. R. Miranda, *Gli obblighi*, cit., 234.

[41] Così F. Cajani, Internet Protocol. *Questioni operative in tema di investigazioni penali e riservatezza*, in *Dir. internet* 2008, 554.

zione, tra questi non compaiono i siti internet visitati, che da questo punto di vista rappresenterebbero ciò che più si avvicina al contenuto della comunicazione [42]. Di modo che la riduzione del periodo di conservazione per i dati telematici può semmai essere criticata in quanto difficilmente giustificabile ed eccessivamente breve rispetto alle esigenze delle indagini e non certo essere considerata illegittima per il fatto di determinare un'eccessiva restrizione della riservatezza [43]. E se questo può sostenersi per quanto concerne la limitazione della conservazione a soli 12 mesi per i dati di traffico telematico, *a fortiori* ciò vale per quella di 30 giorni per le chiamate senza risposta. Infatti, queste possono, sì, rivestire un contenuto comunicativo [44], ma ciò è vero esclusivamente in alcune circostanze e peraltro solo in presenza di altri riscontri fattuali e probatori, dato che, di per sé e in assoluto, non è certo possibile determinare *a priori* il valore contenutistico della chiamata senza risposta. Insomma, appare davvero uno sbilanciamento a favore della privacy impedire agli inquirenti di apprendere un dato così poco limitativo della riservatezza come quello *de quo*, quando esso può essere estremamente utile nella lotta alla criminalità, ed è quasi impossibile immaginare che gli inquirenti possano avere contezza della sua necessità in un lasso temporale tanto inferiore rispetto a quello previsto per gli altri dati [45]. Sicché, sotto questo profilo si potrebbe forse semmai ritenere che, ostacolando in modo eccessivo e sproporzionato l'accertamento delle responsabilità penali, la normativa in questione debba considerarsi incostituzionale per violazione dell'art. 112 Cost.

Va ricordato, inoltre, quanto alle misure di sicurezza, che l'art. 132 del Codice della privacy rinvia all'art. 17 del medesimo atto normativo, ove si prevede che i trattamenti che comportano rischi specifici avvengano nel rispetto di adeguate misure ed accorgimenti stabiliti dal Garante. Ed in effetti tale disposizione è stata adempiuta con il provvedimento dell'Autorità del 17 gennaio 2008 [46], ove si stabiliscono appunto misure stringenti per i fornitori di servizi di comunicazione, al fine di garantire

---

[42] Cfr. C. Conti, *L'attuazione*, cit., 15.

[43] Il rilievo è avanzato dagli Autori citati nelle due note precedenti.

[44] Come nel caso in cui lo squillo sia un segnale cui corrisponde un valore preconcordato tra le persone comunicanti, come l'avviso che qualcuno è in arrivo o che è giunto il momento di commettere l'azione criminale. Cfr., in senso critico, C. Conti, *L'attuazione*, cit., 17, la quale ritiene che la brevità del termine sia una soluzione compromissoria a fronte di una natura ambigua di questi dati i quali, pur essendo chiaramente esterni, non di rado rivestono appunto un valore comunicativo.

[45] Su questo punto insiste particolarmente G. Da Valle, *Art. 12*/ter, in AA.VV., *D.l. 23.2.2009 n. 11, conv. con modif., in l. 23.4.2009 n. 38 - Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*, in *Legisl. pen.*, 2009, spec. 536 ss.

[46] Il provvedimento, adottato dal Garante anche tenendo conto dei risultati di un'istruttoria pubblica, si può consultare sul sito istituzionale *http.www.garanteprivacy.it*, documento web 1482111, ove si trova anche il successivo provvedimento di modifica del 24 luglio 2008, documento web 1538224. Si osservi che, proprio al dichiarato fine di « verificare il rispetto della normativa in materia di trattamento dei dati personali, nell'ottica di un bilanciamento tra le ragioni di giustizia e di sicurezza e l'interesse alla riservatezza della vita privata dei cittadini » nel mese di marzo 2013 il Garante ha promosso tra l'altro la vasta operazione di controllo denominata "*Data retention*" con la quale la Guardia di finanza ha verificato presso fornitori di servizi di telefonia e internet proprio il rispetto delle prescrizioni in questione (notizie sul

la sicurezza dei dati e la loro automatica cancellazione al termine del periodo di conservazione previsto dalla legge [47].

Né è vero quanto sostenuto da parte della dottrina che la disciplina interna sia carente per la mancanza di indicazioni chiare e precise dei casi e modi di acquisizione, del loro utilizzo nel processo e dei criteri per valutare la legittimità dell'acquisizione [48], dato che per questi profili, pur effettivamente non regolati dall'art. 132 del Codice della privacy, trova applicazione la disciplina del codice di rito penale, così che i tabulati vengono acquisiti nel processo con le modalità di cui agli artt. 495 e 507 come le altre prove [49] e per essi si applica la sanzione della inutilizzabilità ai sensi dell'art. 191 laddove siano stati acquisiti in violazione di legge (quindi senza rispettare le previsioni degli artt. 11 e 132 del d. lgs. 196 del 2003) [50].

Dunque, l'unico argomento utilizzato nella decisione della Corte di giustizia che potrebbe essere opposto anche alla norma interna è il fatto che questa non circoscrive l'accesso ai dati ai soli reati di particolare gravità, ma ritiene condizione necessaria e sufficiente il collegamento con una (qualunque) indagine penale [51]. Sennonché questo argomento, come abbiamo già sottolineato, non è condivisibile, né in ottica sovranazionale né tantomeno alla luce della nostra Costituzione, poiché ogni fatto di reato, in quanto tale — ledendo interessi fondamentali che il legislatore ha ritenuto di proteggere con sanzioni di natura così grave — merita e giustifica pienamente l'esercizio dell'azione penale e quindi postula che possano essere utilizzati i mezzi già a disposizione per un efficace esercizio di essa [52].

medesimo sito dell'Autorità, documento web 2300180). Per un'analisi dei provvedimenti — e delle misure di sicurezza giudicate come notevolmente accurate e specifiche — cfr. A. Stracuzzi, *Data retention*, cit., 607 ss.

[47] Il provvedimento del Garante è richiamato da C. Conti, *L'attuazione*, cit., 32 come un sistema di garanzie atto a dare corpo ad un modello di tutela della riservatezza alternativo a quello della direttiva annullata, tutto impostato, secondo l'A., solo sulla amputazione dei tempi di conservazione, a discapito delle esigenze processuali.

[48] La critica è di A. Di Martino, *Il* Bundesverfassungsgericht, cit., 4070.

[49] Cfr. Cass. pen., sez. I, 3 dicembre 2003, n. 23961/04, in *Riv. Pen.*, 2005, 776.

[50] Così R. Miranda, *Gli obblighi*, cit., 233, che vi aggiunge il richiamo all'art. 188 c.p.p. in tema di divieto di mezzi di prova che siano lesivi della libertà morale, intesa come autodeterminazione, della persona; nonché C. Conti, *L'attuazione*, cit., 13 e 29, ove l'A. ricorda anche la disciplina sanzionatoria *ad hoc* introdotta dal d.lgs. 109 del 2008.

[51] Sull'assenza della necessità di giustificare un *fumus boni juris* essendo sufficiente la mera esistenza di un'indagine penale cfr. ancora C. Conti, *L'attuazione*, loc. cit.

[52] Per la stessa ragione non condivisibile ci pare la critica di A. Balsamo - A. Tamietti, *Le intercettazioni, tra garanzie formali e sostanziali*, in A. Balsamo - R. E. Kostoris (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino 2008, 466, per i quali la generica finalità di accertamento dei reati finisce per giustificare anche un blando collegamento con un reato per limitare la riservatezza dell'indagato (con evidenti ricadute sui terzi coinvolti nelle comunicazioni). Infatti, ci pare difficile e comunque inutile graduare il collegamento tra reato e tabulato che si intende acquisire, dovendosi ritenere condizione necessaria e sufficiente la pertinenza, secondo una ragionevole valutazione *rebus sic stantibus*, dello strumento investigativo rispetto all'indagine in corso, la cui reale sussistenza dovrà essere dimostrata nella motivazione dell'atto.

6. Considerazioni conclusive.

Concludendo, allora, riteniamo che la sentenza della Corte di giustizia, da un lato, abbia l'indubbio pregio di non limitarsi a riprodurre il « cliché dell'affermazione convegnistica circa la necessità di un bilanciamento tra privacy e sicurezza » [53], ma di fornire indicazioni in gran parte corrette per questo bilanciamento, non impedendo la conservazione dei dati ma richiedendo esclusivamente che questa avvenga con adeguate garanzie sotto il profilo tanto della conservazione quanto della accessibilità; nonché, dall'altro, non possa giustificare in alcun modo valutazioni di illegittimità estensibili alla normativa italiana, che anzi dimostrandosi maggiormente restrittiva rispetto a quella comunitaria oggi annullata, predispone semmai una « supertutela della privacy, penalizzando soverchiamente le esigenze investigative » [54].

L'auspicio, quindi, è che il legislatore comunitario, ora, sappia cogliere l'esatta portata del *dictum* del giudice di Lussemburgo e non si adegui alla dominante cultura ipersensibile alla privacy, seguendo piuttosto l'equilibrata posizione che la Corte ha suggerito, nella speranza, inoltre, che quest'ultima possa mutare, in futuro, in relazione al (solo) profilo critico qui rilevato.

Simone Scagliarini

[53] Per usare l'espressione di F. De Leo, *La conservazione*, cit., 424.

[54] C. Conti, *L'attuazione*, cit., 4 e 25, ove questo è ritenuto l'effetto generale della riforma.