Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
HENRIK SAUGMANDSGAARD ØE
presentate il 19 luglio 2016[1]

Cause riunite C-203/15 e C-698/15

Tele2 Sverige AB
contro
Post- och telestyrelsen (C-203/15)
e
Secretary of State for the Home Department
contro
Tom Watson,
Peter Brice,
Geoffrey Lewis (C-698/15)
con l'intervento di
Open Rights Group,
Privacy International,
Law Society of England and Wales

[domande di pronuncia pregiudiziale proposte dal Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (sezione civile), Regno Unito]

«Rinvio pregiudiziale — Direttiva 2002/58/CE — Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche — Normativa nazionale che prevede un obbligo generale di conservare i dati relativi alle comunicazioni elettroniche — Articolo 15, paragrafo 1 — Carta dei diritti fondamentali dell'Unione europea — Articolo 7 — Diritto al rispetto della vita privata — Articolo 8 — Diritto alla protezione dei dati di carattere personale — Ingerenza grave — Giustificazione — Articolo 52, paragrafo 1 — Condizioni — Obiettivo legittimo di lotta contro i reati gravi — Requisito di una base giuridica nel diritto nazionale — Requisito di stretta necessità — Requisito di proporzionalità in una società democratica»

Indice

1 — Lingua originale: il francese.

I – **Introduzione**

1. Nel 1788, James Madison, uno degli autori della Costituzione degli Stati Uniti, così scriveva: «If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself» [2].

2. Le presenti cause ci pongono al centro della «grande difficoltà» individuata da Madison. Esse vertono sulla compatibilità con il diritto dell'Unione di regimi nazionali che impongono ai fornitori di servizi di comunicazione elettronica accessibili al pubblico (in prosieguo: i «fornitori») un obbligo di conservazione dei dati relativi alle comunicazioni elettroniche (in prosieguo: i «dati relativi alle comunicazioni») riguardante tutti i mezzi di comunicazione e tutti gli utenti (in prosieguo: l'«obbligo generale di conservazione di dati»).

3. Da una parte, la conservazione dei dati relativi alle comunicazioni consente «al governo di controllare i governati» mettendo a disposizione delle autorità competenti un mezzo di indagine che presenta un'utilità certa nella lotta contro i reati gravi, e in particolare nella lotta contro il terrorismo. In sostanza, la conservazione di tali dati offre alle autorità una capacità limitata di «leggere il passato», accedendo ai dati relativi alle comunicazioni che una persona ha effettuato ancor prima di essere sospettata di avere un collegamento con un reato grave [3].

2 — «Se gli uomini fossero angeli, non sarebbe necessario alcun governo. Se ci fossero angeli a governare gli uomini, non sarebbero necessari controlli esterni o interni sul governo. Nel dar forma a un governo di uomini su uomini, la grande difficoltà consiste in questo: occorre anzitutto consentire al governo di controllare i governati, e poi obbligare quest'ultimo a controllare se stesso»: Madison, J., «Federalist No. 51», in Hamilton, A., Madison, J. e Jay, J., ed. Genovese, M.A., *The Federalist Papers*, Palsgrave Macmillan, New York, 2009, pag. 120; traduzione libera. Madison fu uno dei principali autori e uno dei 39 firmatari della Costituzione degli Stati Uniti (1787). In seguito, divenne il quarto presidente degli Stati Uniti (dal 1809 al 1817).

3 — Tale capacità limitata di «leggere il passato» può rivelarsi molto utile ai fini dell'identificazione di eventuali complici: v. paragrafi da 178 a 184 delle presenti conclusioni.

4. Dall'altra, tuttavia, è imperativo «obbligare il governo a controllare se stesso» per quanto riguarda sia la conservazione sia l'accesso ai dati conservati, tenuto conto dei gravi rischi causati dall'esistenza di siffatte banche dati che coprono la totalità delle comunicazioni effettuate sul territorio nazionale. Infatti, tali banche dati dalle dimensioni considerevoli offrono a qualsiasi persona che vi abbia accesso la possibilità di catalogare istantaneamente l'insieme della popolazione rilevante [4]. Detti rischi devono essere scrupolosamente presi in considerazione attraverso, in particolare, l'esame del carattere strettamente necessario e proporzionato di un obbligo generale di conservazione di dati, come quello di cui trattasi nei procedimenti principali.

5. Quindi, nell'ambito delle presenti cause, la Corte e i giudici del rinvio sono chiamati a definire un punto di equilibrio tra l'obbligo incombente agli Stati membri di garantire la sicurezza delle persone che si trovano sul loro territorio e il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati di carattere personale sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

6. È alla luce di detta «grande difficoltà» che esaminerò le questioni sottoposte alla Corte nelle presenti cause. Queste ultime riguardano, più in particolare, la compatibilità di regimi nazionali che stabiliscono un obbligo generale di conservazione di dati con la direttiva 2002/58/CE [5] nonché con gli articoli 7 e 8 della Carta. Per rispondere a tali questioni, la Corte dovrà segnatamente precisare quale interpretazione occorra dare in un contesto nazionale alla sentenza Digital Rights Ireland e a. (in prosieguo: la «sentenza DRI») [6], nella quale la Grande Sezione della Corte ha invalidato la direttiva 2006/24/CE [7].

7. Per i motivi che esporrò in prosieguo, ritengo che un obbligo generale di conservazione di dati imposto da uno Stato membro possa essere compatibile con i diritti fondamentali sanciti dal diritto dell'Unione purché sia strettamente inquadrato da una serie di garanzie che individuerò nel corso della mia esposizione.

II – **Contesto normativo**

A – *Direttiva 2002/58*

8. L'articolo 1 della direttiva 2002/58, intitolato «Finalità e campo d'applicazione», così dispone:

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

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

4 — V. paragrafi da 252 a 261 delle presenti conclusioni.

5 — Direttiva del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37), quale modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11).

6 — Sentenza dell'8 aprile 2014 (C-293/12 e C-594/12, EU:C:2014:238).

7 — Direttiva del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54).

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

9. L'articolo 15, paragrafo 1, della direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», è così formulato:

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

B – *Diritto svedese*

10. La direttiva 2006/24, ormai invalidata, è stata trasposta nel diritto svedese dalle modifiche apportate alla lagen (2003:389) om elektronisk kommunikation (legge svedese 2003:389 sulle comunicazioni elettroniche; in prosieguo: la «LEK») e al förordningen (2003:396) om elektronisk kommunikation (regolamento 2003:396 sulle comunicazioni elettroniche; in prosieguo: il «FEK»), testi entrati in vigore il 1º maggio 2012.

1. Sulla portata dell'obbligo di conservazione

11. Dalle disposizioni dell'articolo 16 a del capo 6 della LEK risulta che i fornitori sono tenuti a conservare i dati relativi alle comunicazioni necessari per identificare la fonte e la destinazione di una comunicazione, per determinarne la data, l'ora, la durata e la natura, per individuare l'apparecchiatura di comunicazione utilizzata nonché per determinare l'ubicazione dell'apparecchiatura di comunicazione mobile utilizzata all'inizio e alla fine della comunicazione. I tipi di dati che devono essere conservati formano oggetto di disposizioni più dettagliate negli articoli da 38 a 43 del FEK.

12. Tale obbligo di conservazione riguarda i dati trattati nell'ambito di un servizio di telefonia, un servizio di telefonia da un punto di connessione mobile, di un sistema di messaggeria elettronica, di un servizio di accesso a Internet, nonché di un servizio di fornitura di capacità di accesso a Internet.

13. I dati da conservare includono non solo tutti quelli che dovevano essere conservati nell'ambito della direttiva 2006/24, ma anche quelli relativi a comunicazioni non riuscite, nonché quelli relativi all'ubicazione alla fine di una comunicazione mediante telefonia mobile. Analogamente al regime che era previsto da tale direttiva, i dati da conservare non includono il contenuto delle comunicazioni.

2. Sull'accesso ai dati conservati

14. L'accesso ai dati conservati è disciplinato da tre testi, vale a dire la LEK, il rättegångsbalken (codice sul procedimento giudiziario; in prosieguo: l'«RB») e la lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (legge svedese 2012:278 sulla comunicazione di dati relativi a comunicazioni elettroniche nell'ambito delle attività di intelligence delle autorità di contrasto).

a) La LEK

15. Secondo le disposizioni dell'articolo 22, primo comma, punto 2, del capo 6 della LEK, tutti i fornitori devono comunicare i dati relativi a un abbonamento su richiesta del pubblico ministero, della polizia, della Säkerhetspolisen (servizi di sicurezza svedesi; in prosieguo: la «Säpo») o di qualsiasi altra autorità preposta al contrasto della criminalità, ove tali dati si riferiscano ad un'ipotesi di reato. Tali disposizioni non richiedono che si tratti di un reato grave.

16. Per «dati relativi a un abbonamento» si intendono, in sostanza, i dati relativi al nome, al titolo, all'indirizzo postale, al numero e all'indirizzo IP dell'abbonato.

17. Ai sensi della LEK, la comunicazione di dati relativi a un abbonamento non è subordinata a un controllo preventivo, ma può essere oggetto di un controllo amministrativo a posteriori. Inoltre, il numero di autorità che possono avere accesso ai dati non è limitato.

b) L'RB

18. L'RB disciplina la messa sotto sorveglianza di comunicazioni elettroniche nel corso delle indagini preliminari.

19. In sostanza, la messa sotto sorveglianza di comunicazioni elettroniche può essere disposta soltanto quando un determinato individuo sia ragionevolmente sospettato di essere l'autore di un reato punibile con una pena detentiva non inferiore a sei mesi o di altri reati specificamente elencati, qualora tale misura sia particolarmente necessaria ai fini dell'indagine.

20. Oltre a tali casi, si può procedere a una siffatta messa sotto sorveglianza al fine di indagare su un reato punibile con una pena detentiva non inferiore a due anni, al fine di determinare chi possa essere ragionevolmente sospettato di esserne l'autore, qualora tale misura sia particolarmente necessaria ai fini dell'indagine.

21. Ai sensi dell'articolo 21 del capo 27 dell'RB, il pubblico ministero deve di norma ottenere l'autorizzazione del giudice competente prima di procedere alla messa sotto sorveglianza di comunicazioni elettroniche.

22. Tuttavia, qualora la necessità di adire il giudice competente prima di procedere alla messa sotto sorveglianza di comunicazioni elettroniche – misura nella fattispecie assolutamente indispensabile ai fini dell'indagine – sembri incompatibile con l'urgenza della sua attuazione o crei ostacoli, l'autorizzazione è concessa dal pubblico ministero in attesa della decisione del giudice competente. Quest'ultimo deve esserne immediatamente informato per iscritto dal pubblico ministero. Il giudice competente deve quindi valutare se la misura sia giustificata.

c) La legge 2012:278

23. Nell'ambito della ricerca di informazioni e ai sensi dell'articolo 1 della legge 2012:278, la polizia nazionale, la Säpo e la Tullverket (agenzia svedese delle dogane) possono, alle condizioni previste da tale legge e all'insaputa del fornitore, procedere alla raccolta di dati relativi alle comunicazioni.

24. A norma degli articoli 2 e 3 della legge 2012:278, i dati possono essere raccolti se, alla luce delle circostanze, tale misura sia particolarmente necessaria per prevenire, impedire o constatare un'attività criminale che comporti uno o più reati punibili con una pena detentiva non inferiore a due anni, oppure uno degli atti elencati all'articolo 3 (che comprende, in particolare, varie forme di sabotaggio e di spionaggio).

25. La decisione di procedere a una siffatta misura spetta al direttore dell'autorità interessata o a una persona delegata a tal fine.

26. La decisione deve indicare l'attività criminale, il periodo interessato nonché il numero di telefono, qualsiasi altro indirizzo, l'apparecchiatura di comunicazione elettronica o la zona geografica in questione. La durata dell'autorizzazione non deve protrarsi oltre il necessario e, per quanto riguarda il periodo che decorre dalla data della decisione di autorizzazione, la sua durata non deve superare un mese.

27. Tale tipo di misura non è soggetto a un controllo preventivo. Tuttavia, ai sensi dell'articolo 6 della legge 2012:278, la Säkerhets- och integritetsskyddsnämnden (commissione svedese per la protezione della sicurezza e dell'integrità, Svezia) deve essere informata di qualsiasi decisione di autorizzazione a procedere alla raccolta di dati. A norma dell'articolo 1 della lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (legge 2007:980 relativa alla vigilanza su talune attività di contrasto), tale organismo deve vigilare sull'applicazione della legge da parte delle autorità di contrasto.

3. Sulla durata di conservazione dei dati

28. Dalle disposizioni dell'articolo 16 d del capo 6 della LEK risulta che i dati di cui all'articolo 16 a del medesimo capo devono essere conservati per sei mesi a partire dal giorno in cui la comunicazione è stata conclusa. Essi devono poi essere immediatamente cancellati, salvo disposizioni contrarie dell'articolo 16 d, secondo comma, (del capo 6) della LEK. Ai sensi di queste ultime disposizioni, i dati di cui è stata chiesta la comunicazione prima della scadenza del termine di conservazione, ma che non sono ancora stati comunicati, devono essere cancellati subito dopo tale comunicazione.

4. Sulla protezione e la sicurezza dei dati conservati

29. L'articolo 20, primo comma, del capo 6 della LEK vieta a chiunque di diffondere o utilizzare senza autorizzazione dati relativi alle comunicazioni.

30. Secondo le disposizioni dell'articolo 3 a del capo 6 della LEK, i fornitori devono adottare misure di ordine tecnico e organizzativo idonee ad assicurare la protezione dei dati durante il trattamento. Dai lavori preparatori relativi a tali disposizioni risulta che non è consentito determinare il livello di protezione sulla base di un bilanciamento tra le considerazioni di ordine tecnico, i costi e i rischi di pirateria e di violazione della privacy.

31. Ulteriori prescrizioni in merito alla protezione dei dati figurano all'articolo 37 del FEK nonché nelle istruzioni e nelle linee guida della Post- och telestyrelsen (autorità svedese delle poste e telecomunicazioni; in prosieguo: la «PTS») sulle misure di protezione nell'ambito della conservazione e del trattamento di dati ai fini della lotta contro la criminalità (PTSFS n. 2012:4). Da tali testi risulta, in particolare, che i fornitori devono adottare misure di protezione dei dati contro la distruzione non

intenzionale o non autorizzata, contro la conservazione, il trattamento e l'accesso non autorizzati, nonché contro la divulgazione non autorizzata. Il fornitore deve inoltre vigilare costantemente e sistematicamente sulla sicurezza dei dati tenendo conto dei rischi specifici derivanti dall'obbligo di conservazione.

32. Il diritto svedese non contiene disposizioni in merito al luogo in cui devono essere conservati i dati.

33. Ai sensi del capo 7 della LEK, l'autorità di vigilanza ha il potere, qualora un fornitore non adempia i propri obblighi, di adottare nei suoi confronti misure di ingiunzione e di interdizione, eventualmente accompagnate da penalità, nonché di ordinargli la cessazione totale o parziale dell'attività.

C – *Diritto del Regno Unito*

34. Le disposizioni che disciplinano la conservazione dei dati figurano nel Data Retention and Investigatory Powers Act 2014 (legge del 2014 sulla conservazione dei dati e sui poteri d'indagine; in prosieguo: la «DRIPA»), nel Data Retention Regulations 2014 (SI 2014/2042) (regolamento del 2014 relativo alla conservazione dei dati; in prosieguo: il «regolamento del 2014»), nonché nel Retention of Communications Data Code of Practice (Codice delle buone pratiche relativo alla conservazione dei dati).

35. Le disposizioni che disciplinano l'accesso ai dati si trovano nel capitolo 2 della parte 1 del Regulation of Investigatory Powers Act 2000 (legge del 2000 recante regolamentazione dei poteri d'indagine; in prosieguo: la «RIPA»), nel Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) (ordinanza del 2015 recante regolamentazione dei poteri d'indagine in materia di dati relativi alle comunicazioni, come modificata dal Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228) nonché nell'Acquisition and Disclosure of Communications Data Code of Practice (codice delle buone pratiche relative all'acquisizione e alla divulgazione dei dati relativi alle comunicazioni; in prosieguo: il «codice relativo all'acquisizione dei dati»).

1. Sulla portata dell'obbligo di conservazione

36. Ai sensi dell'articolo 1 della DRIPA, il Secretary of State for the Home Department (Ministro dell'Interno, Regno Unito; in prosieguo: il «Ministro») può imporre ai fornitori l'obbligo di conservare tutti i dati relativi alle comunicazioni. In sostanza, tale obbligo può riguardare tutti i dati generati in occasione di una comunicazione veicolata da un servizio postale o da un sistema di telecomunicazione, ad eccezione del contenuto della comunicazione. Tali dati includono, in particolare, il luogo in cui si trova l'utente del servizio nonché i dati che consentono di determinare l'indirizzo IP (protocollo Internet) o qualsiasi altro codice identificativo appartenente al mittente o al destinatario di una comunicazione.

37. Gli obiettivi che possono giustificare l'adozione di una tale misura di conservazione comprendono gli interessi della sicurezza nazionale, la prevenzione o l'accertamento dei reati e la prevenzione delle turbative dell'ordine pubblico, gli interessi del benessere economico del Regno Unito, nella misura in cui tali interessi siano anche rilevanti per gli interessi della sicurezza nazionale, gli interessi della sicurezza pubblica, la tutela della salute pubblica, la valutazione dell'imponibile o la riscossione delle imposte, dei contributi o delle altre somme dovute alla pubblica amministrazione, la prevenzione dei danni alla salute fisica o mentale nei casi di emergenza, l'assistenza nelle indagini sui casi di errori giudiziari, l'identificazione di una persona deceduta o non in grado di identificarsi autonomamente per

cause diverse da un reato (ad esempio, in caso di catastrofe naturale o di incidente), l'esercizio di funzioni relative alla regolamentazione dei servizi e dei mercati finanziari o della stabilità finanziaria, nonché qualsiasi altro scopo specificato in un'ingiunzione emanata dal Ministro ai sensi dell'articolo 22, paragrafo 2, della DRIPA.

38. La normativa nazionale non richiede che l'emissione di un avviso di conservazione sia soggetta ad una previa autorizzazione giudiziaria o di un'entità indipendente. Il Ministro deve verificare che l'obbligo di conservazione sia «necessario e proporzionato» ai fini di uno o più obiettivi per i quali i pertinenti dati relativi alle comunicazioni possono essere conservati.

2. Sull'accesso ai dati conservati

39. Ai sensi dell'articolo 22, paragrafo 4, della RIPA, le autorità pubbliche possono, secondo i termini di un avviso, esigere che i fornitori trasmettano loro dati relativi alle comunicazioni. La forma e il contenuto di tali avvisi sono disciplinati dall'articolo 23, paragrafo 2, della RIPA. Un siffatto avviso è limitato nel tempo da disposizioni relative al suo annullamento e al suo rinnovo.

40. L'acquisizione dei dati relativi alle comunicazioni dev'essere necessaria e proporzionata a uno o più degli obiettivi elencati nell'articolo 22 della RIPA, i quali corrispondono agli obiettivi idonei a giustificare la conservazione dei dati descritti al paragrafo 37 delle presenti conclusioni.

41. Dal codice relativo all'acquisizione dei dati risulta che è necessaria l'ordinanza emessa da un giudice nel caso di una domanda di accesso presentata al fine di individuare la fonte dei giornalisti nonché in caso di domanda di accesso formulata da autorità locali.

42. Al di fuori di tali ipotesi, l'accesso da parte delle autorità pubbliche è subordinato al rilascio di un'autorizzazione concessa dalle persone designate a tal fine nell'ambito dell'autorità pubblica interessata. Una persona designata a tal fine è una persona che detiene una funzione, un grado o una posizione prescritta all'interno dell'autorità pubblica interessata e che è stata designata ai fini dell'acquisizione dei dati relativi alle comunicazioni conformemente all'ordinanza del 2015 recante regolamentazione dei poteri d'indagine in materia di dati relativi alle comunicazioni, come modificata.

43. Non è necessaria alcuna autorizzazione giudiziaria o di un'entità indipendente per l'accesso ai dati relativi alle comunicazioni protette dal segreto professionale dei consulenti legali o ai dati relativi alle comunicazioni con medici, membri del Parlamento o ministri di culto. Il codice relativo all'acquisizione dei dati precisa soltanto che dev'essere prestata una particolare attenzione alla necessità e alla proporzionalità di una domanda di accesso a tali dati.

3. Sul periodo di conservazione dei dati

44. L'articolo 1, paragrafo 5, della DRIPA e la disposizione 4, paragrafo 2, del regolamento del 2014 prevedono un periodo massimo di dodici mesi per la conservazione dei dati. Secondo il codice delle buone pratiche relativo alla conservazione dei dati, il periodo di conservazione deve soltanto avere una durata che sia necessaria e proporzionata. La disposizione 6 del regolamento del 2014 impone al Ministro di riesaminare gli avvisi di conservazione.

4. Sulla protezione e la sicurezza dei dati conservati

45. A norma dell'articolo 1 della DRIPA, ai fornitori è vietato divulgare i dati conservati a meno che tale divulgazione sia conforme al capitolo 2 della parte 1 della RIPA, a una decisione giudiziaria o a un'altra autorizzazione o mandato giudiziario, oppure a un regolamento adottato dal Ministro ai sensi dell'articolo 1 della DRIPA.

46. Ai sensi delle disposizioni 7 e 8 del regolamento del 2014, i fornitori devono garantire l'integrità e la sicurezza dei dati conservati; proteggerli dalla distruzione accidentale o illecita, dalla perdita o dall'alterazione accidentale e dalla conservazione, dal trattamento, dall'accesso o dalla divulgazione non autorizzati o illeciti; distruggere i dati cosicché sia impossibile accedervi qualora la conservazione dei dati cessi di essere autorizzata; e predisporre sistemi di sicurezza. La disposizione 9 del regolamento del 2014 affida all'Information Commissioner (commissario per l'informazione) il compito di verificare il rispetto di tali obblighi da parte dei fornitori.

47. Le autorità alle quali i fornitori comunicano dati relativi alle comunicazioni devono trattare e conservare in maniera sicura tali dati, nonché qualsiasi copia, estratto o riassunto di essi. Ai sensi del codice relativo all'acquisizione dei dati, gli obblighi previsti dalla legge relativa alla protezione dei dati (Data Protection Act; in prosieguo: il «DPA»), che ha trasposto la direttiva 95/46, devono essere rispettati.

48. La RIPA istituisce un Interception of Communications Commissioner (commissario per l'intercettazione delle comunicazioni; in prosieguo: il «commissario per l'intercettazione»), il quale è incaricato di vigilare in modo indipendente sull'esercizio e sull'attuazione dei poteri e dei doveri previsti dal capitolo II della parte I della RIPA. Il commissario per l'intercettazione non vigila sul ricorso all'articolo 1 della DRIPA. Egli deve fornire regolarmente relazioni destinate al pubblico e al Parlamento (articolo 57, paragrafo 2, e articolo 58 del RIPA) e dichiarare ciò che è conservato e riferito dalle autorità pubbliche (codice relativo all'acquisizione dei dati, paragrafi da 6.1 a 6.8). È possibile inoltre presentare denunce presso l'Investigatory Powers Tribunal (Tribunale competente per i poteri d'indagine) qualora si ritenga che siano stati acquisiti dati in modo improprio (articolo 65 della RIPA).

49. Dal codice relativo all'acquisizione dei dati risulta che il commissario per l'intercettazione non ha il potere di deferire un caso a tale Tribunale, ma è semplicemente autorizzato ad informare una persona del sospetto che vi sia stato un uso illecito di competenze qualora possa «dimostrare che un individuo è stato danneggiato da una violazione intenzionale o colposa». Tuttavia, non è autorizzato a procedere a una divulgazione qualora quest'ultima minacci la sicurezza nazionale, ancorché ritenga che vi sia stata una violazione intenzionale o colposa.

III – **Procedimenti principali e questioni pregiudiziali**

A – *La causa C-203/15*

50. Il 9 aprile 2014, vale a dire il giorno successivo alla pronuncia della sentenza DRI, la Tele2 Sverige ha notificato alla PTS la propria decisione di cessare di procedere alla conservazione dei dati di cui al capo 6 della LEK. La Tele2 Sverige avrebbe inoltre proceduto alla cancellazione dei dati conservati fino ad allora in applicazione di tale capo. La Tele2 Sverige riteneva che la normativa svedese di trasposizione della direttiva 2006/24 non fosse conforme alla Carta.

51. Il 15 aprile 2014, la Rikspolisstyrelsen (direzione generale della polizia di stato, Svezia; in prosieguo: la «RPS») ha presentato una denuncia alla PTS lamentando che la Tele2 Sverige aveva cessato di comunicare ai suoi servizi i dati relativi a determinate comunicazioni elettroniche. Nella propria denuncia, la RPS affermava che il rifiuto della Tele2 Sverige avrebbe comportato gravi conseguenze sulle attività repressive della polizia.

52. Con ingiunzione del 27 giugno 2014, la PTS ha ordinato alla Tele2 Sverige di procedere alla conservazione dei dati, ai sensi dell'articolo 16 a del capo 6 della LEK e degli articoli da 37 a 43 del FEK, entro il 25 luglio 2014.

53. La Tele2 Sverige ha adito il Förvaltningsrätten i Stockholm (Tribunale amministrativo di Stoccolma, Svezia) con un ricorso avverso la decisione della PTS. Con sentenza del 13 ottobre 2014, il Förvaltningsrätten i Stockholm ha respinto tale ricorso.

54. La Tele2 Sverige ha impugnato la sentenza del Förvaltningsrätten i Stockholm dinanzi al giudice del rinvio al fine di ottenere l'annullamento della decisione contestata.

55. Constatando che sussistevano argomenti sia a favore sia contro la compatibilità di un obbligo di conservazione della portata di quello previsto dall'articolo 16 a del capo 6 della LEK con le disposizioni dell'articolo 15, paragrafo 1, della direttiva 2002/58 nonché con quelle degli articoli 7, 8 e 52, paragrafo 1, della Carta, il Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se un obbligo generalizzato di conservazione dei dati concernenti tutte le persone, tutti i mezzi di comunicazione elettronica e tutti i dati relativi al traffico senza distinzioni, limitazioni o eccezioni per finalità di contrasto alla criminalità [come descritto ai punti da 13 a 18 della domanda di pronuncia pregiudiziale] sia compatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, tenuto conto degli articoli 7, 8 e 52, paragrafo 1, della Carta.

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

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

   b) i requisiti di sicurezza sono disciplinati come [descritto ai punti da 38 a 43 della domanda di pronuncia pregiudiziale], e

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

B – *La causa C-698/15*

56. I sigg. Watson, Brice e Lewis hanno proposto dinanzi alla High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) [Alta Corte di giustizia (Inghilterra e Galles), divisione del Queen's Bench (sezione amministrativa)] ricorsi giurisdizionali volti al controllo di legittimità («judicial review») del regime di conservazione dei dati previsto dall'articolo 1 della DRIPA, che autorizza il Ministro ad imporre agli operatori di telecomunicazioni pubbliche la conservazione di tutti dati relativi a comunicazioni per un periodo massimo di dodici mesi, essendo esclusa la conservazione del contenuto delle comunicazioni.

57. L'Open Rights Group, la Privacy International e la Law Society of England and Wales sono stati autorizzati ad intervenire in ciascuno di tali ricorsi.

58. Con sentenza del 17 luglio 2015, tale giudice ha constatato che detto regime non è compatibile con il diritto dell'Unione in quanto non soddisfa i requisiti stabiliti dalla sentenza DRI, che esso ha ritenuto applicabili alle normative degli Stati membri in materia di conservazione dei dati relativi a comunicazioni elettroniche e di accesso a tali dati. Il Ministro ha interposto appello avverso detta sentenza dinanzi al giudice del rinvio.

59. In una sentenza del 20 novembre 2015, la Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (sezione civile), Regno Unito] ha dichiarato, in via provvisoria, che la sentenza DRI non ha stabilito esigenze imperative di diritto dell'Unione che le normative nazionali devono rispettare, ma ha semplicemente individuato e descritto alcune tutele che non erano presenti nel regime armonizzato dell'Unione.

60. Tuttavia, ritenendo che le risposte a tali questioni di diritto dell'Unione non fossero chiare e fossero necessarie per pronunciarsi in detti procedimenti, la Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (sezione civile) (Regno Unito)] ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

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

2) Se la sentenza [DRI] estenda l'ambito di applicazione degli articoli 7 e/o 8 della Carta UE oltre quello dell'articolo 8 della Convenzione europea dei diritti dell'uomo (in prosieguo: la "CEDU") come stabilito dalla giurisprudenza della Corte europea dei diritti dell'uomo (in prosieguo: la "Corte EDU")».

IV – **Procedimento dinanzi alla Corte**

61. Le domande di pronuncia pregiudiziale sono state registrate presso la cancelleria della Corte il 4 maggio 2015 nella causa C-203/15 e il 28 dicembre 2015 nella causa C-698/15.

62. Con ordinanza del 1º febbraio 2016, la Corte ha deciso di sottoporre la causa C-698/15 al procedimento accelerato ai sensi dell'articolo 105, paragrafo 1, del regolamento di procedura della Corte.

63. Nella causa C-203/15, hanno presentato osservazioni scritte la Tele2 Sverige, i governi belga, ceco, danese, tedesco, estone, irlandese, spagnolo, francese, ungherese, neerlandese, svedese e del Regno Unito, nonché la Commissione europea.

64. Nella causa C-698/15, hanno presentato osservazioni scritte i sigg. Watson, Brice e Lewis, l'Open Rights Group, la Privacy International, la Law Society of England and Wales, i governi ceco, danese, tedesco, estone, irlandese, francese, cipriota, polacco, finlandese e del Regno Unito, nonché la Commissione

65. Con decisione della Corte del 10 marzo 2016, tali due cause sono state riunite ai fini della fase orale del procedimento e della sentenza.

66. Sono comparsi all'udienza del 12 aprile 2016, per esporre le proprie osservazioni, i rappresentanti della Tele2 Sverige, dei sigg. Watson, Brice e Lewis, dell'Open Rights Group, della Privacy International e della Law Society of England and Wales, dei governi ceco, danese, tedesco, estone, irlandese, spagnolo, francese, finlandese, svedese e del Regno Unito, nonché della Commissione.

V – **Analisi delle questioni pregiudiziali**

67. Con la prima questione sollevata nella causa C-203/15, il giudice del rinvio chiede alla Corte se, alla luce della sentenza DRI, l'articolo 15, paragrafo 1, della direttiva 2002/58, nonché gli articoli 7, 8 e 52, paragrafo 1, della Carta debbano essere interpretati nel senso che essi ostano a che uno Stato membro imponga ai fornitori un obbligo generale di conservazione di dati, come quelli di cui trattasi nei procedimenti principali, indipendentemente da eventuali garanzie che accompagnino tale obbligo.

68. In caso di risposta negativa a tale questione, la seconda questione sollevata nella causa C-203/15 e la prima questione sollevata nella causa C-698/15 mirano a determinare se dette disposizioni debbano essere interpretate nel senso che esse ostano a che uno Stato membro imponga ai fornitori un obbligo generale di conservazione di dati qualora tale obbligo non sia accompagnato dall'insieme delle garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI per quanto riguarda l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati.

69. Poiché tali tre questioni sono strettamente correlate, le esaminerò congiuntamente nel prosieguo della mia esposizione.

70. Per contro, la seconda questione sollevata nella causa C-698/15 dev'essere trattata separatamente. Con tale questione, il giudice del rinvio chiede alla Corte se la sentenza DRI abbia esteso l'ambito di applicazione degli articoli 7 e/o 8 della Carta al di là di quello dell'articolo 8 della CEDU. Esporrò nella sezione seguente i motivi per i quali ritengo che detta questione debba essere respinta in quanto irricevibile.

71. Prima di iniziare l'esame di dette questioni, mi sembra utile ricordare il tipo di dati oggetto degli obblighi di conservazione di cui trattasi nei procedimenti principali. Secondo gli accertamenti effettuati dai giudici del rinvio, la portata di tali obblighi è, in sostanza, equivalente a quella dell'obbligo che era previsto dall'articolo 5 della direttiva 2006/24[8]. Schematicamente, i dati relativi alle comunicazioni oggetto di tali obblighi di conservazione possono essere classificati in quattro categorie[9]:

— i dati che consentono di individuare sia la fonte che la destinazione della comunicazione;

— i dati che consentono di determinare l'ubicazione sia della fonte che della destinazione della comunicazione;

— i dati relativi alla data, all'ora e alla durata della comunicazione, e

— i dati che consentono di determinare il tipo di comunicazione e il tipo di apparecchiatura utilizzato.

72. Il contenuto delle comunicazioni è escluso dagli obblighi generali di conservazione di dati di cui trattasi nei procedimenti principali, al pari di quanto prevedeva l'articolo 5, paragrafo 2, della direttiva 2006/24.

A – *Sulla ricevibilità della seconda questione sollevata nella causa C-698/15*

73. La seconda questione sollevata nella causa C-698/15 invita la Corte a precisare se la sentenza DRI estenda l'ambito di applicazione degli articoli 7 e/o 8 della Carta al di là di quello dell'articolo 8 della CEDU quale interpretato dalla Corte EDU.

8 — Tale equivalenza è comprensibile, in quanto detti regimi nazionali miravano a trasporre la suddetta direttiva, ormai invalidata.

9 — V. descrizione dei regimi nazionali in questione nei procedimenti principali ai paragrafi da 11 a 13 e 36 delle presenti conclusioni.

74. Tale questione riflette, in particolare, un argomento addotto dal Ministro dinanzi al giudice del rinvio, secondo cui la giurisprudenza della Corte EDU non richiede, da una parte, che l'accesso ai dati sia subordinato alla previa autorizzazione di un organo indipendente né, dall'altra, che la conservazione e l'accesso a tali dati siano limitati alla lotta contro i reati gravi.

75. Ritengo che detta questione debba essere dichiarata irricevibile per i motivi seguenti. Con ogni evidenza, la motivazione e la soluzione adottate dalla Corte nella sentenza DRI rivestono un'importanza determinante ai fini della risoluzione delle controversie principali. Tuttavia, il fatto che tale sentenza abbia eventualmente esteso l'ambito di applicazione degli articoli 7 e/o 8 della Carta al di là di quello dell'articolo 8 della CEDU non è, di per sé, rilevante ai fini della risoluzione di dette controversie.

76. A questo proposito, occorre ricordare che, a norma dell'articolo 6, paragrafo 3, TUE, i diritti fondamentali, quali garantiti dalla CEDU, fanno parte del diritto dell'Unione in quanto principi generali. Tuttavia, in assenza di adesione dell'Unione a tale convenzione, quest'ultima non costituisce uno strumento giuridico formalmente integrato nell'ordinamento giuridico dell'Unione [10].

77. È pur vero che la prima frase dell'articolo 52, paragrafo 3, della Carta stabilisce una regola di interpretazione secondo la quale, laddove quest'ultima contenga diritti corrispondenti a quelli garantiti dalla CEDU, «il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione».

78. Tuttavia, a termini della seconda frase dell'articolo 52, paragrafo 3, della Carta, «[tale] disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa». A mio avviso, da tale frase risulta che la Corte può, qualora lo ritenga necessario nel contesto del diritto dell'Unione, estendere l'ambito di applicazione delle disposizioni della Carta al di là di quello delle disposizioni corrispondenti della CEDU.

79. Aggiungo, in subordine, che l'articolo 8 della Carta, quale interpretato dalla Corte nella sentenza DRI, stabilisce un diritto che non corrisponde ad alcun diritto garantito dalla CEDU, vale a dire il diritto alla protezione dei dati di carattere personale, il che è confermato peraltro dalle spiegazioni relative all'articolo 52 della Carta [11]. Pertanto, la regola d'interpretazione stabilita dall'articolo 52, paragrafo 3, prima frase, della Carta non è, in ogni caso, applicabile all'interpretazione dell'articolo 8 della Carta, come hanno rilevato i sigg. Brice e Lewis, l'Open Rights Group e la Privacy International, la Law Society of England and Wales, nonché i governi ceco, irlandese e finlandese.

80. Da quanto precede, consegue che il diritto dell'Unione non osta a che gli articoli 7 e 8 della Carta accordino una protezione più ampia di quella prevista dalla CEDU. Pertanto, il fatto che la sentenza DRI abbia eventualmente esteso l'ambito di applicazione di tali disposizioni della Carta al di là di quello dell'articolo 8 della CEDU non è, di per sé, rilevante ai fini della risoluzione delle controversie principali. La soluzione di tali controversie dipende essenzialmente dalle condizioni alle quali un obbligo generale di conservazione di dati può essere considerato compatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58, nonché con gli articoli 7, 8 e 52, paragrafo 1, della Carta, interpretati alla luce della sentenza DRI, il che costituisce precisamente l'oggetto delle altre tre questioni sollevate nelle presenti cause.

10 — Parere 2/13, del 18 dicembre 2014 (EU:C:2014:2454, punto 179), e sentenza del 15 febbraio 2016, N. (C-601/15 PPU, EU:C:2016:84, punto 45 e giurisprudenza citata).

11 — Ai sensi dell'articolo 6, paragrafo 1, terzo comma, TUE e dell'articolo 52, paragrafo 7, della Carta, le spiegazioni relative alla Carta devono essere prese in considerazione ai fini della sua interpretazione (v. sentenze del 26 febbraio 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punto 20, e del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 47). Secondo tali spiegazioni, l'articolo 7 della Carta corrisponde all'articolo 8 della CEDU, mentre l'articolo 8 della Carta non corrisponde ad alcun diritto della CEDU.

81. Secondo giurisprudenza costante, il rigetto di una domanda proposta da un giudice nazionale è possibile soltanto qualora appaia in modo manifesto che l'interpretazione richiesta del diritto dell'Unione non ha alcun rapporto con la realtà effettiva o con l'oggetto del procedimento principale, oppure qualora la questione sia di natura ipotetica, o anche quando la Corte non disponga degli elementi di fatto e di diritto necessari per rispondere in modo utile alle questioni che le sono sottoposte [12].

82. Nel caso di specie, e per i motivi sopra esposti, la seconda questione sollevata nella causa C-698/15 presenta, a mio avviso, soltanto un interesse teorico, in quanto una eventuale risposta a tale questione non consentirebbe di sviluppare elementi interpretativi del diritto dell'Unione che il giudice del rinvio possa utilmente utilizzare per poter risolvere, in base a tale diritto, la controversia dinanzi ad esso pendente [13].

83. Ciò posto, ritengo che detta questione debba essere dichiarata irricevibile, come hanno sostenuto giustamente il sig. Watson, la Law Society of England and Wales e il governo ceco.

B – *Sulla compatibilità di un obbligo generale di conservazione di dati con il regime stabilito dalla direttiva 2002/58*

84. La presente sezione verte sulla possibilità, per gli Stati membri, di avvalersi della facoltà offerta dall'articolo 15, paragrafo 1, della direttiva 2002/58 per imporre un obbligo generale di conservazione di dati. Essa non esamina, invece, i requisiti particolari che devono essere rispettati dagli Stati membri che intendono avvalersi di tale facoltà, i quali saranno ampiamente analizzati in una sezione successiva [14].

85. Invero, l'Open Rights Group e la Privacy International hanno sostenuto che un tale obbligo sarebbe incompatibile con il regime armonizzato stabilito dalla direttiva 2002/58, indipendentemente dal rispetto dei requisiti previsti dall'articolo 15, paragrafo 1, della direttiva 2002/58, in quanto esso vanificherebbe il contenuto essenziale dei diritti e del regime stabiliti da tale direttiva.

86. Prima di esaminare tale argomento, occorre verificare se un obbligo generale di conservazione di dati rientri nell'ambito di applicazione di detta direttiva.

1. Sull'inclusione di un obbligo generale di conservazione di dati nell'ambito di applicazione della direttiva 2002/58

87. Nessuna delle parti che hanno presentato osservazioni alla Corte ha messo in discussione il fatto che un obbligo generale di conservazione di dati, come quello di cui trattasi nei procedimenti principali, rientri nella nozione di «trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell['Unione]» ai sensi dell'articolo 3 della direttiva 2002/58.

88. Nondimeno, i governi ceco, francese, polacco e del Regno Unito hanno sostenuto che un obbligo generale di conservazione di dati rientra nell'esclusione prevista dall'articolo 1, paragrafo 3, della direttiva 2002/58. Da una parte, le disposizioni nazionali che disciplinano l'accesso ai dati e l'utilizzo degli stessi da parte delle autorità di polizia o giudiziarie degli Stati membri riguarderebbero la

12 — V., in particolare, sentenze del 9 novembre 2010, Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662, punto 40 e giurisprudenza citata), nonché del 24 aprile 2012, Kamberaj (C-571/10, EU:C:2012:233, punto 42 e giurisprudenza citata).

13 — V., in particolare, sentenza del 16 settembre 1982, Vlaeminck (132/81, EU:C:1982:294, punto 13); ordinanza del 24 marzo 2011, Abt e a. (C-194/10, EU:C:2011:182, punti 36 e 37 nonché giurisprudenza citata), e sentenza del 24 ottobre 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, punto 46 e giurisprudenza citata).

14 — V. paragrafi da 126 a 262 delle presenti conclusioni.

sicurezza pubblica, la difesa o la sicurezza dello Stato o rientrerebbero, quanto meno, nel diritto penale. Dall'altra, l'unico obiettivo della conservazione dei dati consisterebbe nel consentire a tali autorità di polizia o giudiziarie di accedervi e di utilizzarli. Di conseguenza, un obbligo di conservazione dei dati sarebbe escluso dall'ambito di applicazione di detta direttiva, ai sensi della disposizione sopra citata.

89. Tale ragionamento non mi convince per i seguenti motivi.

90. In primo luogo, la formulazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 conferma che gli obblighi di conservazione imposti dagli Stati membri rientrano nell'ambito di applicazione di tale direttiva. A termini di detta disposizione, infatti, «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». Mi sembra quanto meno difficile sostenere che gli obblighi di conservazione siano esclusi dall'ambito di applicazione di tale direttiva, laddove l'articolo 15, paragrafo 1, di quest'ultima disciplina la facoltà di adottare siffatti obblighi.

91. In realtà, come hanno affermato il sig. Watson, i sigg. Brice e Lewis, i governi belga, danese, tedesco e finlandese, nonché la Commissione, un obbligo generale di conservazione di dati, come quelli di cui trattasi nei procedimenti principali, costituisce un'attuazione dell'articolo 15, paragrafo 1, della direttiva 2002/58.

92. In secondo luogo, il fatto che le disposizioni che disciplinano l'accesso possano rientrare nell'esclusione di cui all'articolo 1, paragrafo 3, della direttiva 2002/58 [15] non implica che l'obbligo di conservazione vi rientri parimenti e si collochi pertanto al di fuori dell'ambito di applicazione di tale direttiva.

93. A questo proposito, la Corte ha già avuto l'opportunità di precisare che le attività menzionate nell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46/CE [16], il cui testo ha una portata equivalente a quello dell'articolo 1, paragrafo 3, della direttiva 2002/58, erano attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli [17].

94. Orbene, come ha rilevato la Commissione, gli obblighi di conservazione di cui trattasi nei procedimenti principali sono imposti ad operatori privati nell'ambito di attività private di fornitura di servizi di comunicazione elettronica. Inoltre, tali obblighi sono imposti indipendentemente da qualsiasi richiesta di accesso da parte delle autorità di polizia o giudiziarie, nonché, più in generale, indipendentemente da qualsiasi atto delle autorità statali riguardante la sicurezza pubblica, la difesa, la sicurezza dello Stato o il diritto penale.

95. Inoltre, la soluzione adottata dalla Corte nella sentenza Irlanda/Parlamento e Consiglio conferma che un obbligo generale di conservazione di dati non rientra nella materia penale [18]. Infatti, la Corte ha dichiarato che la direttiva 2006/24, che stabiliva un siffatto obbligo, riguardava non già la materia penale, bensì il funzionamento del mercato interno, cosicché l'articolo 95 CE (divenuto articolo 114 TFUE) costituiva il fondamento normativo adeguato per l'adozione di tale direttiva.

15 — V. paragrafi da 123 a 125 delle presenti conclusioni.

16 — Direttiva 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).

17 — Sentenza del 6 novembre 2003, Lindqvist (C-101/01, EU:C:2003:596, punti 43 e 44).

18 — Sentenza del 10 febbraio 2009 (C-301/06, EU:C:2009:68).

96. Per giungere a tale conclusione, la Corte ha constatato, segnatamente, che le disposizioni di detta direttiva erano essenzialmente limitate alle attività dei fornitori di servizi e non disciplinavano né l'accesso ai dati né il loro uso da parte delle autorità di polizia o giudiziarie degli Stati membri [19]. Ne deduco che neanche le disposizioni di diritto nazionale che stabiliscono un obbligo di conservazione simile a quello previsto dalla direttiva 2006/24 riguardano la materia penale.

97. Alla luce di quanto precede, ritengo che un obbligo generale di conservazione di dati non rientri nell'esclusione stabilita dall'articolo 1, paragrafo 3, della direttiva 2002/58 e, pertanto, ricada nell'ambito di applicazione di tale direttiva.

2. Sulla possibilità di derogare al regime stabilito dalla direttiva 2002/58 istituendo un obbligo generale di conservazione di dati

98. Occorre adesso determinare se un obbligo generale di conservazione di dati sia compatibile con il regime stabilito dalla direttiva 2002/58.

99. A tale riguardo, si pone la questione se sia possibile, per uno Stato membro, avvalersi della facoltà offerta dall'articolo 15, paragrafo 1, della direttiva 2002/58 al fine di imporre un siffatto obbligo.

100. Quattro argomenti sono state addotti contro una tale possibilità, segnatamente dall'Open Rights Group e dalla Privacy International.

101. Secondo un primo argomento, concedere agli Stati membri il potere di adottare un obbligo generale di conservazione di dati rimetterebbe in discussione l'obiettivo di armonizzazione che costituisce la ragion d'essere della direttiva 2002/58. Infatti, secondo il suo articolo 1, paragrafo 1, tale direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno dell'Unione.

102. Pertanto, l'articolo 15, paragrafo 1, della direttiva 2002/58 non potrebbe essere interpretato nel senso che esso offra agli Stati membri il potere di adottare una deroga al regime stabilito da detta direttiva di un'ampiezza tale da privare di ogni effetto utile siffatto sforzo di armonizzazione.

103. Stando al secondo argomento, il testo dell'articolo 15, paragrafo 1, della direttiva 2002/58 osterebbe parimenti a un'interpretazione così ampia del potere degli Stati membri di derogare al regime stabilito da tale direttiva. A termini di detta disposizione, infatti, «[g]li 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 [di tale] direttiva» (il corsivo è mio).

104. Orbene, un obbligo generale di conservazione di dati non si risolverebbe nel «limitare» i diritti e gli obblighi menzionati da detta disposizione, ma li eliminerebbe. Ciò avverrebbe:

— per l'obbligo di garantire la riservatezza dei dati sul traffico e per l'obbligo di subordinare l'archiviazione di informazioni al consenso dell'utente, rispettivamente previsti dall'articolo 5, paragrafi 1 e 3, della direttiva 2002/58;

— per l'obbligo di cancellare o di rendere anonimi i dati sul traffico, stabilito dall'articolo 6, paragrafo 1, di tale direttiva, e

19 — Sentenza del 10 febbraio 2009, Irlanda/Parlamento e Consiglio (C-301/06, EU:C:2009:68, punto 80).

— per l'obbligo di rendere anonimi i dati relativi all'ubicazione o di ottenere il consenso dell'utente per trattare tali dati, imposto dall'articolo 9, paragrafo 1, di detta direttiva.

105. Ritengo che questi due primi argomenti debbano essere respinti per i motivi seguenti.

106. Da una parte, il testo dell'articolo 15, paragrafo 1, della direttiva 2002/58 menziona la possibilità, per gli Stati membri, di adottare «misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato». Tale riferimento esplicito agli obblighi di conservazione di dati conferma che obblighi di tal genere non sono, di per sé, incompatibili con il regime stabilito dalla direttiva 2002/58/CE. Sebbene tale formulazione non preveda espressamente la possibilità di adottare un obbligo *generale* di conservazione di dati, occorre constatare che essa non vi osta neanche.

107. Dall'altra parte, il considerando 11 della direttiva 2002/58 precisa che quest'ultima lascia inalterato «l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, [di tale] direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale». Di conseguenza, «[detta] direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla [CEDU]».

108. Da tale considerando 11, a mio avviso, risulta che l'intenzione del legislatore dell'Unione era non già quella di pregiudicare la facoltà degli Stati membri di adottare le misure previste dall'articolo 15, paragrafo 1, della direttiva 2002/58, bensì quella di subordinare tale facoltà a taluni requisiti relativi, in particolare, agli scopi perseguiti e alla proporzionalità di dette misure. In altri termini, un obbligo generale di conservazione di dati non è, a mio avviso, incompatibile con il regime stabilito da tale direttiva, purché esso soddisfi determinate condizioni.

109. Secondo un terzo argomento, l'articolo 15, paragrafo 1, della direttiva 2002/58 dovrebbe, in quanto deroga al regime stabilito da tale direttiva, essere interpretato restrittivamente, in virtù di una regola di interpretazione che risulta da una costante giurisprudenza della Corte. Tale regola di interpretazione restrittiva impedirebbe di interpretare detta disposizione nel senso che essa offra la facoltà di imporre un obbligo generale di conservazione di dati.

110. A questo proposito, ritengo che la facoltà prevista dall'articolo 15, paragrafo 1, della direttiva 2002/58 non possa essere qualificata come deroga e non possa pertanto essere interpretata restrittivamente, come ha sostenuto a buon diritto la Commissione. Infatti, mi sembra difficile qualificare tale facoltà come deroga alla luce del considerando 11 sopra menzionato, secondo il quale detta direttiva non pregiudica la facoltà degli Stati membri di adottare le misure previste dalla summenzionata disposizione. Rilevo peraltro che l'articolo 15 di detta direttiva è intitolato «Applicazione di alcune disposizioni della direttiva 95/46», mentre l'articolo 10 della medesima direttiva è intitolato esplicitamente «Deroghe». Tali titoli rafforzano la mia convinzione che la facoltà prevista da detto articolo 15 non possa essere qualificata come «deroga».

111. Secondo un quarto e ultimo argomento, l'incompatibilità di un obbligo generale di conservazione di dati con il regime stabilito dalla direttiva 2002/58 sarebbe confermata dall'aggiunta dell'articolo 15, paragrafo 1 bis, di tale direttiva in occasione dell'adozione della direttiva 2006/24, invalidata dalla sentenza DRI. Stando a tale argomento, è detta incompatibilità che avrebbe indotto il legislatore dell'Unione a dichiarare l'articolo 15, paragrafo 1, della direttiva 2002/58 inapplicabile al regime di conservazione generale previsto dalla direttiva 2006/24.

112. Ritengo che detto argomento prenda le mosse da una comprensione erronea della portata dell'articolo 15, paragrafo 1 bis, della direttiva 2002/58. A termini di tale disposizione, «[l'articolo 15, paragrafo 1, della direttiva 2002/58] 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».

113. La mia lettura di questa disposizione è la seguente. Per quanto riguarda i dati la cui conservazione era prescritta dalla direttiva 2006/24 e ai fini stabiliti da quest'ultima, gli Stati membri perdevano la facoltà, prevista dall'articolo 15, paragrafo 1, della direttiva 2002/58, di limitare ulteriormente la portata dei diritti e degli obblighi previsti da tale disposizione, in particolare mediante obblighi complementari di conservazione di dati. In altri termini, l'articolo 15, paragrafo 1 bis, prevedeva un'armonizzazione esaustiva per quanto riguarda i dati la cui conservazione era prescritta dalla direttiva 2006/24 e ai fini stabiliti da quest'ultima.

114. Trovo conferma di tale interpretazione nel considerando 12 della direttiva 2006/24, a termini del quale «[l]'articolo 15, paragrafo 1, della direttiva [2002/58] *continua ad applicarsi* ai dati, compresi quelli connessi ai tentativi di chiamata non riusciti, di cui non è specificamente richiesta la conservazione a norma della presente direttiva e *che pertanto non rientrano nel campo di applicazione della stessa*, e alla conservazione dei dati *per scopi*, anche giudiziari, *diversi da quelli contemplati dalla presente direttiva*» (il corsivo è mio).

115. Pertanto, l'inserimento dell'articolo 15, paragrafo 1 bis, della direttiva 2002/58 attesta non già l'incompatibilità di un obbligo generale di conservazione di dati con il regime stabilito da tale direttiva, bensì la volontà del legislatore dell'Unione di realizzare un'armonizzazione esaustiva all'atto dell'adozione della direttiva 2006/24.

116. Alla luce di quanto precede, ritengo che un obbligo generale di conservazione di dati sia compatibile con il regime stabilito dalla direttiva 2002/58 e, pertanto, che sia possibile, per uno Stato membro, avvalersi della facoltà offerta dall'articolo 15, paragrafo 1, di tale direttiva per imporre un siffatto obbligo [20]. Il ricorso a tale facoltà è tuttavia subordinato al rispetto di requisiti rigorosi, derivanti non solo da tale disposizione, ma anche dalle pertinenti disposizioni della Carta, lette alla luce della sentenza DRI, che saranno esaminate in una sezione successiva [21].

C – *Sull'applicabilità della Carta a un obbligo generale di conservazione di dati*

117. Prima di esaminare il contenuto dei requisiti imposti dalla Carta, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58, qualora uno Stato scelga di istituire un obbligo generale di conservazione di dati, occorre verificare se la Carta si applichi effettivamente a un tale obbligo.

118. L'applicabilità della Carta ad un obbligo generale di conservazione di dati dipende essenzialmente dall'applicabilità della direttiva 2002/58 a un siffatto obbligo.

20 — Poiché la direttiva 2002/58 può essere qualificata come «lex specialis» rispetto alla direttiva 95/46 (v., a tale riguardo, articolo 1, paragrafo 2, della direttiva 2002/58), non ritengo necessario verificare la compatibilità di un obbligo generale di conservazione di dati con il regime stabilito dalla direttiva 95/46, che, peraltro, non è oggetto delle questioni sottoposte alla Corte. Per completezza, vorrei comunque precisare che il testo dell'articolo 13, paragrafo 1, della direttiva 95/46 offre agli Stati membri un margine di manovra più ampio rispetto a quello offerto dall'articolo 15, paragrafo 1, della direttiva 2002/58, che ne precisa la portata nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico. Poiché la facoltà prevista dall'articolo 15, paragrafo 1, della direttiva 2002/58 consente l'adozione, da parte di uno Stato membro, di un obbligo generale di conservazione di dati, ne desumo che l'articolo 13, paragrafo 1, della direttiva 95/46 la consente parimenti.

21 — V. paragrafi da 126 a 262 delle presenti conclusioni.

119. Infatti, a termini del suo articolo 51, paragrafo 1, prima frase, «le disposizioni della [Carta] si applicano (…) agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione». Le spiegazioni relative all'articolo 51 della Carta rinviano, a tale riguardo, alla giurisprudenza della Corte secondo la quale l'obbligo di rispettare i diritti fondamentali definiti nell'ambito dell'Unione vale per gli Stati membri soltanto quando agiscono nell'ambito di applicazione del diritto dell'Unione [22].

120. I governi ceco, francese, polacco e del Regno Unito, i quali hanno contestato l'applicabilità della direttiva 2002/58 a un obbligo generale di conservazione di dati [23], hanno parimenti sostenuto che la Carta non fosse applicabile a un tale obbligo.

121. Ho già chiarito i motivi per i quali ritengo che un obbligo generale di conservazione di dati costituisca un'attuazione della facoltà prevista dall'articolo 15, paragrafo 1, della direttiva 2002/58 [24].

122. Di conseguenza, ritengo che le disposizioni della Carta siano applicabili alle misure nazionali che istituiscono un tale obbligo, ai sensi dell'articolo 51, paragrafo 1, della Carta, come hanno sostenuto il sig. Watson, i sigg. Brice e Lewis, l'Open Rights Group e la Privacy International, i governi danese, tedesco e finlandese, nonché la Commissione [25].

123. Tale conclusione non è rimessa in discussione dal fatto che le disposizioni nazionali che disciplinano l'accesso ai dati conservati non rientrino, di per sé, nell'ambito di applicazione della Carta.

124. È pur vero che, nella misura in cui riguardino «attività dello Stato in settori che rientrano nel diritto penale», le disposizioni nazionali che disciplinano l'accesso ai dati conservati dalle autorità di polizia o giudiziarie al fine di contrastare i reati gravi rientrano, a mio avviso, nell'esclusione prevista dall'articolo 1, paragrafo 3, della direttiva 2002/58 [26]. Di conseguenza, tali disposizioni nazionali non attuano il diritto dell'Unione, cosicché la Carta non si applica loro.

125. Tuttavia, la ratio di un obbligo di conservazione di dati è quella di consentire alle autorità di contrasto di accedere ai dati conservati, cosicché le problematiche della conservazione e dell'accesso non possono essere completamente dissociate. Come ha sottolineato giustamente la Commissione, le disposizioni che disciplinano l'accesso rivestono un'importanza determinante al fine di decidere in ordine alla compatibilità con la Carta delle disposizioni che stabiliscono un obbligo generale di conservazione di dati, le quali attuano l'articolo 15, paragrafo 1, della direttiva 2002/58. Più precisamente, le disposizioni che disciplinano l'accesso devono essere prese in considerazione per valutare la necessità e la proporzionalità di un siffatto obbligo [27].

22 — Da una costante giurisprudenza della Corte risulta, infatti, che i diritti fondamentali garantiti nell'ordinamento giuridico dell'Unione si applicano in tutte le situazioni disciplinate dal diritto dell'Unione, ma non al di fuori di esse. A tale riguardo, la Corte ha già ricordato che essa non può valutare alla luce della Carta una normativa nazionale che non si collochi nell'ambito del diritto dell'Unione. Per contro, una volta che una siffatta normativa rientri nell'ambito di applicazione di tale diritto, la Corte, adita in via pregiudiziale, deve fornire tutti gli elementi di interpretazione necessari per la valutazione, da parte del giudice nazionale, della conformità di tale normativa con i diritti fondamentali di cui essa garantisce il rispetto (v. sentenza del 26 febbraio 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punto 19 e giurisprudenza citata).

23 — V. supra, paragrafo 88.

24 — V. supra, paragrafi da 90 a 97.

25 — Più precisamente, l'articolo 51, paragrafo 1, seconda frase, della Carta dispone che gli Stati membri sono tenuti a rispettare i diritti garantiti da quest'ultima nell'attuazione del diritto dell'Unione.

26 — Sulla portata di tale esclusione, v. paragrafi da 90 a 97 delle presenti conclusioni.

27 — V. paragrafi da 185 a 262 delle presenti conclusioni.

D – *Sulla compatibilità di un obbligo generale di conservazione di dati con i requisiti stabiliti dall'articolo 15, paragrafo 1, della direttiva 2002/58 nonché dagli articoli 7, 8 e 52, paragrafo 1, della Carta*

126. Mi resta da trattare adesso la difficile questione della compatibilità di un obbligo generale di conservazione di dati con i requisiti stabiliti dall'articolo 15, paragrafo 1, della direttiva 2002/58 nonché dagli articoli 7, 8 e 52, paragrafo 1, della Carta. Tale questione riguarda, più in generale, il necessario adeguamento del quadro normativo che disciplina le capacità di sorveglianza degli Stati, le quali sono state potenziate dai recenti progressi della tecnologia [28].

127. La prima fase di qualsiasi analisi, in tale contesto, consiste nella constatazione dell'ingerenza nei diritti garantiti dalla direttiva 2002/58 e nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta.

128. Infatti, un siffatto obbligo costituisce una grave ingerenza nel diritto al rispetto della vita privata, sancito dall'articolo 7 della Carta, e nel diritto alla protezione dei dati di carattere personale, garantito dall'articolo 8 della Carta. Non ritengo utile soffermarmi su tale constatazione d'ingerenza, che è stata chiaramente effettuata dalla Corte ai punti da 32 a 37 della sentenza DRI [29]. Allo stesso modo, un obbligo generale di conservazione di dati costituisce un'ingerenza in diversi diritti sanciti dalla direttiva 2002/58 [30].

129. La seconda fase dell'analisi consiste nel determinare se, e a quali condizioni, detta grave ingerenza nei diritti garantiti dalla direttiva 2002/58, nonché nei dritti fondamentali sanciti dagli articoli 7 e 8 della Carta, possa essere giustificata.

130. Due disposizioni stabiliscono le condizioni che devono essere soddisfatte affinché tale doppia ingerenza sia giustificata: l'articolo 15, paragrafo 1, della direttiva 2002/58, che disciplina la facoltà, per gli Stati membri, di limitare la portata di taluni diritti stabiliti da detta direttiva, e l'articolo 52, paragrafo 1, della Carta, letto alla luce della sentenza DRI, il quale disciplina qualsiasi limitazione all'esercizio dei diritti sanciti dalla Carta.

131. Tengo a sottolineare che tali requisiti sono *cumulativi*. Infatti, il rispetto dei requisiti stabiliti dall'articolo 15, paragrafo 1, della direttiva 2002/58 non implica, di per sé, che i requisiti previsti dall'articolo 52, paragrafo 1, della Carta siano soddisfatti, e viceversa [31]. Di conseguenza, un obbligo generale di conservazione di dati può essere considerato compatibile con il diritto dell'Unione soltanto se soddisfi sia i requisiti stabiliti dall'articolo 15, paragrafo 1, della direttiva 2002/58, sia quelli previsti dall'articolo 52, paragrafo 1, della Carta, come ha sottolineato la Law Society of England and Wales [32].

28 — V. in particolare Consiglio per i diritti umani delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione del diritto di libertà di opinione ed espressione, 17 aprile 2013, A/HRC/23/40, n. 33: «I progressi tecnologici consentono allo Stato di compiere attività di sorveglianza che non sono più limitate da criteri di scala o di durata. (…) Di conseguenza, lo Stato dispone, oggi più che mai, di mezzi più potenti per svolgere attività di sorveglianza simultanee, pregiudizievoli per la riservatezza, mirate e su vasta scala. (…)». V. inoltre n. 50: «In generale, la legislazione non ha seguito il ritmo dei cambiamenti tecnologici. Nella maggior parte degli Stati, le norme giuridiche sono inesistenti o insufficienti a far fronte alle condizioni attuali di sorveglianza delle comunicazioni. (…)».

29 — Tornerò nondimeno sui rischi specifici posti dalla costituzione di banche dati di tale ampiezza nell'ambito del requisito di proporzionalità, in una società democratica, di un obbligo generale di conservazione di dati come quello di cui trattasi nei procedimenti principali: v. paragrafi da 252 a 261 delle presenti conclusioni.

30 — V., a tale riguardo, l'argomento addotto dall'Open Rights Group e dalla Privacy International, riassunto al paragrafo 104 delle presenti conclusioni.

31 — Trovo conferma di tale natura cumulativa nell'ultima frase dell'articolo 15, paragrafo 1, della direttiva 2002/58, secondo la quale «[t]utte le misure di cui a[tale] paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE]». Ai sensi dell'articolo 6, paragrafo 1, TUE, «[l]'Unione riconosce i diritti, le libertà e i principi sanciti nella [Carta], che ha lo stesso valore giuridico dei trattati».

32 — Da tale natura cumulativa consegue logicamente che, qualora i requisiti stabiliti dalle suddette due disposizioni si sovrappongano, occorre applicare il requisito più rigoroso ovvero, in altri termini, il requisito che protegge maggiormente i diritti in questione.

132. Congiuntamente, tali due disposizioni stabiliscono sei requisiti che devono essere soddisfatti affinché l'ingerenza causata da un obbligo generale di conservazione di dati sia giustificata:

— l'obbligo di conservazione deve avere una base giuridica;

— deve rispettare il contenuto essenziale dei diritti sanciti dalla Carta;

— deve perseguire un obiettivo di interesse generale;

— deve essere adeguato al perseguimento di tale obiettivo;

— deve essere necessario al perseguimento di detto obiettivo, e

— deve essere proporzionato, all'interno di una società democratica, al perseguimento del medesimo obiettivo.

133. Alcune di tali condizioni sono già state menzionate dalla Corte nella sentenza DRI. A fini di chiarezza e tenuto conto delle peculiarità delle presenti cause rispetto alla causa DRI, desidero nondimeno ritornare su ciascuna di esse, esaminando in modo più dettagliato i requisiti relativi alla base giuridica, al carattere necessario nonché al carattere proporzionato all'interno di una società democratica di un obbligo generale di conservazione di dati.

1. Sul requisito di una base giuridica nel diritto nazionale

134. Sia l'articolo 52, paragrafo 1, della Carta sia l'articolo 15, paragrafo 1, della direttiva 2002/58 stabiliscono i requisiti relativi alla base giuridica che dev'essere utilizzata da uno Stato membro per imporre un obbligo generale di conservazione di dati.

135. In primo luogo, le eventuali limitazioni all'esercizio dei diritti riconosciuti dalla Carta devono essere «previste dalla legge» ai sensi del suo articolo 52, paragrafo 1. Preciso che tale requisito non è stato formalmente esaminato dalla Corte nella sentenza DRI, che riguardava un'ingerenza prevista da una direttiva.

136. Fino alla recente sentenza WebMindLicenses [33], la Corte non si era mai pronunciata sull'esatta portata di tale requisito, anche quando essa aveva espressamente constatato che quest'ultimo era [34] o non era [35] soddisfatto. Al punto 81 di detta sentenza, la Terza Sezione della Corte si è pronunciata nei termini seguenti:

«A tale riguardo, si deve sottolineare che il requisito secondo cui eventuali limitazioni all'esercizio di tale diritto devono essere previste dalla legge implica che la base giuridica che permette l'utilizzo delle prove menzionate al punto precedente da parte dell'amministrazione tributaria deve essere sufficientemente chiara e precisa e che, nel definire essa stessa la portata della limitazione all'esercizio

33 — Sentenza del 17 dicembre 2015 (C-419/14, EU:C:2015:832).

34 — V., in particolare, sentenze del 17 ottobre 2013, Schwarz (C-291/12, EU:C:2013:670, punto 35) (ingerenza prevista da un regolamento europeo); del 27 maggio 2014, Spasic (C-129/14 PPU, EU:C:2014:586, punto 57) (ingerenza prevista dalla Convenzione di applicazione dell'accordo di Schengen, del 14 giugno 1985, tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni,, firmata a Schengen il 19 giugno 1990 ed entrata in vigore il 26 marzo 1995); del 6 ottobre 2015, Delvigne (C-650/13, EU:C:2015:648, punto 47) (ingerenza prevista dal codice elettorale e dal codice penale francese); e del 17 dicembre 2015, Neptune Distribution (C-157/14, EU:C:2015:823, punto 69) (ingerenza prevista da un regolamento e una direttiva europei).

35 — Sentenza del 1º luglio 2010, Knauf Gips/Commissione (C-407/08 P, EU:C:2010:389, punti da 87 a 92) (ingerenza priva di base giuridica).

del diritto garantito dall'articolo 7 della Carta, essa offre una certa tutela contro eventuali violazioni arbitrarie di tale amministrazione (v., in particolare, Corte EDU, Malone c. Regno Unito, 2 agosto 1984, serie A n. 82, § 67, nonché Gillan e Quinton c. Regno Unito, 12 gennaio 2010, n. 4158/05, § 77, CEDU 2010)».

137. Invito la Grande Sezione della Corte a confermare tale interpretazione nelle presenti cause per i seguenti motivi.

138. Come ha rilevato giustamente l'avvocato generale Cruz Villalón nelle sue conclusioni nella causa Scarlet Extended [36], la Corte EDU ha elaborato una copiosa giurisprudenza relativa a tale requisito nel contesto della CEDU, la quale si caratterizza per un'accezione materiale e non formale del termine «legge» [37].

139. Secondo tale giurisprudenza, l'espressione «previste dalla legge» implica che la base giuridica sia sufficientemente accessibile e prevedibile, vale a dire enunciata con una precisione sufficiente a consentire all'individuo, ricorrendo se del caso a consulenti esperti, di regolare la propria condotta. Detta base giuridica deve inoltre fornire una tutela adeguata nei confronti dell'arbitrio e, di conseguenza, definire in modo sufficientemente netto la portata e le modalità di esercizio del potere conferito alle autorità competenti (principio della preminenza del diritto) [38].

140. Orbene, a mio avviso occorre attribuire all'espressione «previste dalla legge», utilizzata all'articolo 52, paragrafo 1, della Carta, una portata simile a quella che tale espressione riveste nel contesto della CEDU, per le seguenti ragioni.

141. Da una parte, ai sensi dell'articolo 53 della Carta e delle spiegazioni relative a tale articolo, il livello di protezione offerto dalla Carta non può mai essere inferiore a quello garantito dalla CEDU. Tale divieto di oltrepassare la «soglia CEDU» implica che l'interpretazione, da parte della Corte, dell'espressione «previste dalla legge», utilizzata all'articolo 52, paragrafo 1, della Carta, debba essere almeno altrettanto rigorosa di quella della Corte EDU nel contesto della CEDU [39].

142. Dall'altra, tenuto conto della natura orizzontale di tale requisito, che può essere applicato a numerosi tipi di ingerenza, sia nel contesto della Carta che in quello della CEDU [40], sarebbe inopportuno sottoporre gli Stati membri a criteri diversi a seconda che l'ingerenza sia esaminata alla luce dell'uno o dell'altro di tali strumenti [41].

36 — C-70/10, EU:C:2011:255 (paragrafi da 94 a 100).

37 — V., in particolare, Corte EDU, 14 settembre 2010, Sanoma Uitgevers B.V. c. Paesi Bassi, CE:ECHR:2010:0914JUD003822403, § 83.

38 — V., in particolare, Corte EDU, 26 marzo 1987, Leander c. Svezia, CE:ECHR:1987:0326JUD000924881, §§ 50-51; Corte EDU, 26 ottobre 2000, Hassan e Tchaouch c. Bulgaria, CE:ECHR:2000:1026JUD003098596, § 84; Corte EDU, 4 dicembre 2008, S. e Marper c. Regno Unito, CE:ECHR:2008:1204JUD003056204, § 95; Corte EDU, 14 settembre 2010, Sanoma Uitgevers B.V. c. Paesi Bassi, CE:ECHR:2010:0914JUD003822403, §§ 81-83; Corte EDU, 31 marzo 2016, Stoyanov e altri c. Bulgaria, CE:ECHR:2016:0331JUD005538810, §§ 124-126.

39 — Più precisamente, la Corte non può, a mio avviso, adottare un'interpretazione di tale requisito più permissiva di quella della Corte EDU, il che avrebbe la conseguenza di consentire un numero di ingerenze più elevato di quello che risulterebbe dall'interpretazione del medesimo requisito da parte della Corte EDU.

40 — Tale espressione «previste dalla legge» è utilizzata all'articolo 8, paragrafo 2 (diritto al rispetto della vita privata e familiare), all'articolo 9, paragrafo 2 (libertà di pensiero, di coscienza e di religione), all'articolo 10, paragrafo 2 (libertà di espressione), e all'articolo 11, paragrafo 2 (libertà di riunione e di associazione), della CEDU. Nel contesto della Carta, l'articolo 52, paragrafo 1, si applica a eventuali limitazioni all'esercizio dei diritti riconosciuti da quest'ultima, ammesso che siffatte limitazioni siano consentite.

41 — V., in tal senso, Peers, S., «Article 52 – Scope of guaranteed rights», in Peers, S., et al, *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, n. 52.39.

143. Ritengo pertanto che, come hanno affermato il governo estone e la Commissione, l'espressione «previste dalla legge», presente nell'articolo 52, paragrafo 1, della Carta, debba essere interpretata, alla luce della giurisprudenza della Corte EDU riassunta al paragrafo 139 delle presenti conclusioni, nel senso che un obbligo generale di conservazione di dati, come quello di cui trattasi nei procedimenti principali, deve essere previsto da una base giuridica sufficientemente accessibile e prevedibile, da una parte, e che offra una tutela adeguata nei confronti dell'arbitrio, dall'altra.

144. In secondo luogo, occorre determinare il contenuto dei requisiti imposti dall'articolo 15, paragrafo 1, della direttiva 2002/58 per quanto riguarda la base giuridica che deve essere utilizzata da uno Stato membro che intenda avvalersi della facoltà offerta da tale disposizione.

145. Devo rilevare, a questo proposito, l'esistenza di una divergenza tra le versioni linguistiche della prima frase di detta disposizione.

146. Nelle versioni inglese («*legislative measures*»), francese («*mesures législatives*»), italiana («disposizioni legislative»), portoghese («*medidas legislativas*»), rumena («*măsuri legislative*») e svedese («*genom lagstiftning vidta åtgärder*»), l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 impone, a mio avviso, l'adozione di misure emanate dal potere legislativo.

147. Per contro, le versioni danese («*retsforskrifter*»), tedesca («*Rechtsvorschriften*»), neerlandese («*wettelijke maatregele*») e spagnola («*medidas legales*») di tale frase possono essere interpretate nel senso che essa impone l'adozione di misure emanate dal potere legislativo oppure di misure regolamentari emanate dal potere esecutivo.

148. Secondo costante giurisprudenza, la necessità di un'applicazione e quindi di un'interpretazione uniformi di un atto dell'Unione esclude che questo sia considerato isolatamente in una delle sue versioni, e rende al contrario necessaria l'interpretazione basata sulla reale volontà del suo autore e sullo scopo da questo perseguito, alla luce, segnatamente, di tutte le altre versioni linguistiche ufficiali. In caso di divergenza tra queste ultime, la disposizione in questione deve essere interpretata in funzione dell'economia generale e della finalità della normativa di cui essa fa parte [42].

149. Nella fattispecie, l'articolo 15, paragrafo 1, della direttiva 2002/58 disciplina la facoltà degli Stati membri di derogare ai diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, la cui protezione è realizzata da tale direttiva. Ritengo pertanto opportuno interpretare il requisito di una base giuridica, imposto dall'articolo 15, paragrafo 1, della direttiva 2002/58, alla luce della Carta, e in particolare dell'articolo 52, paragrafo 1, di quest'ultima.

150. Di conseguenza, le «disposizioni» richieste dall'articolo 15, paragrafo 1, della direttiva 2002/58 devono obbligatoriamente possedere le qualità della accessibilità, della prevedibilità e della tutela adeguata nei confronti dell'arbitrio, menzionate al paragrafo 143 delle presenti conclusioni. Da tali qualità, e in particolare dal requisito della tutela adeguata nei confronti dell'arbitrio, consegue segnatamente che dette disposizioni debbano essere *vincolanti* per le autorità nazionali alle quali è concesso il potere di accedere ai dati conservati. Non sarebbe sufficiente, in particolare, che le garanzie che accompagnano l'accesso a tali dati fossero previste in codici o in orientamenti interni privi di un siffatto carattere vincolante, come ha sottolineato giustamente la Law Society of England and Wales.

42 — V., in particolare, sentenza del 30 maggio 2013, Asbeek Brusse e de Man Garabito (C-488/11, EU:C:2013:341, punto 26); del 24 giugno 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414, punto 26), e del 26 febbraio 2015, Christie's France (C-41/14, EU:C:2015:119, punto 26).

151. Inoltre, ritengo che l'espressione «[g]li Stati membri possono adottare disposizioni», comune a tutte le versioni linguistiche dell'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58, escluda la possibilità che una giurisprudenza nazionale, ancorché costante, possa costituire una base giuridica sufficiente per attuare tale disposizione. Sottolineo che, sotto tale aspetto, detta disposizione va al di là dei requisiti derivanti dalla giurisprudenza della Corte EDU [43].

152. Aggiungo che mi sembra auspicabile, tenuto conto della gravità delle ingerenze che implica un obbligo generale di conservazione di dati nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, che il contenuto essenziale del regime in questione, e in particolare quello delle garanzie che accompagnano tale obbligo, siano stabiliti in una disposizione adottata dal potere legislativo, lasciando al potere esecutivo il compito di precisarne le modalità di applicazione.

153. Alla luce di quanto precede, ritengo che l'articolo 15, paragrafo 1, della direttiva 2002/58 e l'articolo 52, paragrafo 1, della Carta debbano essere interpretati nel senso che il regime che stabilisce un obbligo generale di conservazione di dati, come quello di cui trattasi nei procedimenti principali, deve essere istituito da disposizioni legislative o regolamentari che possiedano le qualità dell'accessibilità, della prevedibilità e della tutela adeguata nei confronti dell'arbitrio.

154. Spetta ai giudici del rinvio verificare il rispetto di tale requisito, tenuto conto della loro posizione privilegiata ai fini della valutazione dei loro rispettivi regimi nazionali.

2. Sul rispetto del contenuto essenziale dei diritti riconosciuti dagli articoli 7 e 8 della Carta

155. Ai sensi del suo articolo 52, paragrafo 1, le eventuali limitazioni all'esercizio dei diritti riconosciuti dalla Carta devono «rispettare il contenuto essenziale di detti diritti» [44]. Tale aspetto, che è stato esaminato dalla Corte ai punti 39 e 40 della sentenza DRI nel contesto della direttiva 2006/24, non pone, a mio avviso, problemi particolari nell'ambito delle presenti cause, come hanno osservato i governi spagnolo e irlandese, nonché la Commissione.

156. Al punto 39 della sentenza DRI, la Corte ha dichiarato che detta direttiva non pregiudicava il contenuto essenziale del diritto al rispetto della vita privata e degli altri diritti sanciti dall'articolo 7 della Carta, in quanto essa non permetteva di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale.

157. A mio avviso, detta valutazione è trasponibile ai regimi nazionali di cui trattasi nei procedimenti principali, poiché neanche siffatti regimi permettono di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale [45].

158. Al punto 40 della sentenza DRI, la Corte ha considerato che la direttiva 2006/24 non pregiudicava il contenuto essenziale del diritto fondamentale alla protezione dei dati di carattere personale, sancito dall'articolo 8 della Carta, tenuto conto dei principi di protezione e di sicurezza dei dati che dovevano essere rispettati dai fornitori ai sensi dell'articolo 7 di tale direttiva, mentre agli Stati membri spettava il compito di assicurare l'adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l'alterazione accidentale dei dati.

43 — V., in particolare, Corte EDU, 14 settembre 2010, Sanoma Uitgevers B.V. c. Paesi Bassi, CE:ECHR:2010:0914JUD003822403, § 83: «[il termine "legge", contenuto negli articoli da 8 a 11 della CEDU, include] tanto il "diritto scritto", comprendente sia testi di rango infralegislativo sia atti regolamentari adottati da un ordine professionale, su delega del legislatore, nell'ambito del proprio potere normativo autonomo, quanto il "diritto non scritto". La "legge" deve intendersi nel senso che comprende sia il testo scritto, sia il "diritto elaborato" dai giudici».

44 — Tale requisito non risulta dal testo dell'articolo 15, paragrafo 1, della direttiva 2002/58, né dall'economia della medesima direttiva, per i motivi esposti ai paragrafi da 99 a 116 delle presenti conclusioni.

45 — V. la descrizione dei regimi nazionali in questione nei procedimenti principali, segnatamente ai paragrafi 13 e 36 delle presenti conclusioni.

159. Anche in questo caso, ritengo che tale valutazione sia trasponibile ai regimi nazionali di cui trattasi nei procedimenti principali, poiché siffatti regimi prevedono, a mio avviso, garanzie paragonabili quanto alla protezione e alla sicurezza dei dati conservati dai fornitori, garanzie che devono consentire di proteggere efficacemente i dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati [46].

160. Spetta tuttavia ai giudici del rinvio verificare che i regimi nazionali di cui trattasi nei procedimenti principali rispettino effettivamente il contenuto essenziale dei diritti riconosciuti dagli articoli 7 e 8 della Carta, alla luce delle considerazioni che precedono.

3. Sull'esistenza di un obiettivo di interesse generale riconosciuto dall'Unione che possa giustificare un obbligo generale di conservazione di dati

161. Sia l'articolo 15, paragrafo 1, della direttiva 2002/58 sia l'articolo 52, paragrafo 1, della Carta prescrivono che qualsiasi ingerenza nei diritti sanciti da tali strumenti persegua un obiettivo di interesse generale.

162. Ai punti da 41 a 44 della sentenza DRI, la Corte ha dichiarato, da una parte, che l'obbligo generale di conservazione di dati imposto dalla direttiva 2006/24 contribuiva «alla lotta contro la criminalità grave e, di conseguenza, in ultima analisi, alla sicurezza pubblica» e, dall'altra, che tale lotta costituiva un obiettivo di interesse generale dell'Unione.

163. Infatti, dalla giurisprudenza della Corte risulta che la lotta contro il terrorismo internazionale finalizzata al mantenimento della pace e della sicurezza internazionali costituisce un obiettivo di interesse generale dell'Unione. Lo stesso vale per la lotta contro la criminalità grave al fine di garantire la sicurezza pubblica. Inoltre, va rilevato, a tale riguardo, che l'articolo 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma altresì alla sicurezza [47].

164. Tale valutazione è trasponibile agli obblighi generali di conservazione di dati di cui trattasi nei procedimenti principali, i quali possono essere giustificati dall'obiettivo della lotta contro i reati gravi.

165. Tuttavia, tenuto conto di taluni argomenti presentati alla Corte, occorre determinare se un siffatto obbligo possa essere giustificato da un obiettivo di interesse generale diverso da quello della lotta contro i reati gravi.

166. A questo proposito, il testo dell'articolo 52, paragrafo 1, della Carta menziona, in generale, le «finalità di interesse generale riconosciute dall'Unione» e l'«esigenza di proteggere i diritti e le libertà altrui».

167. Il testo dell'articolo 15, paragrafo 1, della direttiva 2002/58 è più preciso quanto agli obiettivi che possono giustificare un'ingerenza nei diritti stabiliti da tale direttiva. Infatti, secondo detta disposizione, le misure in questione devono contribuire, «ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46(…)», alla «salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e [al]la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica».

46 — Sentenza DRI, punto 54. V. descrizione dei regimi nazionali in questione nei procedimenti principali ai paragrafi da 29 a 33 nonché 45 e 46 delle presenti conclusioni.

47 — Sentenza DRI, punto 42 e giurisprudenza citata.

168. Inoltre, nella sentenza Promusicae [48], la Corte ha dichiarato che detta disposizione doveva essere interpretata alla luce dell'articolo 13, paragrafo 1, della direttiva 95/46, il quale autorizza le deroghe ai diritti previsti da tale direttiva qualora esse siano giustificate dalla «protezione (…) dei diritti e delle libertà altrui». Di conseguenza, la Corte ha statuito che l'articolo 15, paragrafo 1, della direttiva 2002/58 offre agli Stati membri la facoltà di prevedere l'obbligo, per un fornitore, di divulgare dati personali al fine di determinare, nell'ambito di un procedimento civile, l'esistenza di una violazione dei diritti d'autore relativi a registrazioni musicali e audiovisive.

169. Il governo del Regno Unito ha argomentato da tale sentenza per sostenere che un obbligo generale di conservazione di dati può essere giustificato da qualsiasi obiettivo menzionato nell'articolo 15, paragrafo 1, della direttiva 2002/58 oppure nell'articolo 13, paragrafo 1, della direttiva 95/46. Secondo tale governo, un siffatto obbligo può essere giustificato dall'utilità che presentano i dati conservati nella lotta contro i reati «minori» (in contrapposizione a quelli «gravi») o anche nel contesto di procedimenti non penali in relazione agli obiettivi menzionati da tali disposizioni.

170. Tale argomento non mi convince per le ragioni seguenti.

171. In primo luogo, come hanno sostenuto giustamente il sig. Watson nonché l'Open Rights Group e la Privacy International, l'orientamento adottato dalla Corte nella sentenza Promusicae [49] non è trasponibile alle presenti cause, poiché tale sentenza riguardava una domanda di accesso, da parte di un'associazione di titolari di diritti d'autore, a dati conservati spontaneamente da un fornitore, vale a dire la Telefónica de España. In altri termini, detta decisione non riguardava gli obiettivi in grado di giustificare le gravi ingerenze nei diritti fondamentali che implica un obbligo generale di conservazione di dati come quello di cui trattasi nei procedimenti principali.

172. In secondo luogo, ritengo che il requisito di proporzionalità in una società democratica escluda che la lotta contro i reati minori o il corretto svolgimento di procedimenti non penali possa giustificare un obbligo generale di conservazione di dati. In effetti, i notevoli rischi causati da un siffatto obbligo sono sproporzionati rispetto ai vantaggi che esso offrirebbe nella lotta contro i reati minori o nel contesto di procedimenti non penali [50].

173. Alla luce di quanto precede, ritengo che l'articolo 15, paragrafo 1, della direttiva 2002/58 e l'articolo 52, paragrafo 1, della Carta debbano essere interpretati nel senso che la lotta contro i reati gravi costituisce un obiettivo di interesse generale tale da giustificare un obbligo generale di conservazione di dati, a differenza della lotta contro i reati minori o del corretto svolgimento di procedimenti non penali.

174. Di conseguenza, occorre esaminare il carattere adeguato, necessario e proporzionato di un siffatto obbligo alla luce dell'obiettivo della lotta contro i reati gravi.

4. Sul carattere adeguato di un obbligo generale di conservazione di dati alla luce della lotta contro i reati gravi

175. I requisiti relativi al carattere adeguato, necessario [51] e proporzionato [52] derivano sia dall'articolo 15, paragrafo 1, della direttiva 2002/58, sia dall'articolo 52, paragrafo 1, della Carta.

48 — Sentenza del 29 gennaio 2008 (C-275/06, EU:C:2008:54, punti da 50 a 54).

49 — Sentenza del 29 gennaio 2008 (C-275/06, EU:C:2008:54).

50 — V. paragrafi da 252 a 261 delle presenti conclusioni.

51 — Sul carattere necessario, v. paragrafi da 185 a 245 delle presenti conclusioni.

52 — Sul carattere proporzionato stricto sensu, v. paragrafi da 246 a 262 delle presenti conclusioni.

176. In virtù del primo di tali requisiti, un obbligo generale di conservazione di dati come quello di cui trattasi nei procedimenti principali deve essere idoneo a contribuire all'obiettivo di interesse generale sopra individuato, vale a dire la lotta contro i reati gravi.

177. Tale requisito non pone particolari difficoltà nel contesto delle presenti cause. Come la Corte ha rilevato, in sostanza, nel punto 49 della sentenza DRI, i dati conservati permettono alle autorità nazionali competenti in materia penale di disporre di uno strumento investigativo supplementare per prevenire o accertare i reati gravi. Di conseguenza, un siffatto obbligo contribuisce alla lotta contro i reati gravi.

178. Tengo comunque a precisare l'utilità che può rivestire un obbligo generale di conservazione di dati ai fini della lotta contro i reati gravi. Come ha correttamente sostenuto il governo francese, un tale obbligo consente, in una certa misura, alle autorità di contrasto di «leggere il passato» consultando i dati conservati, a differenza delle misure di sorveglianza mirate.

179. Una misura di sorveglianza mirata riguarda persone che sono state precedentemente individuate come aventi potenzialmente un collegamento, anche indiretto o lontano, con un reato grave. Siffatte misure mirate consentono alle autorità competenti di avere accesso ai dati relativi alle comunicazioni effettuate da dette persone, e persino al contenuto di tali comunicazioni. Tuttavia, tale accesso può riguardare soltanto le comunicazioni effettuate da dette persone *successivamente* alla loro individuazione.

180. Al contrario, un obbligo generale di conservazione di dati riguarda l'insieme delle comunicazioni effettuate da tutti gli utenti, senza che sia richiesto un qualsiasi collegamento con un reato grave. Tale obbligo consente alle autorità competenti di avere accesso alla cronologia delle comunicazioni effettuate da una persona prima di essere stata individuata come avente un siffatto collegamento. È in questo senso che siffatto obbligo conferisce alle autorità di contrasto una capacità limitata di leggere il passato, offrendo loro un accesso alle comunicazioni effettuate da dette persone *precedentemente* alla loro individuazione [53].

181. In altri termini, l'utilità offerta da un obbligo generale di conservazione di dati ai fini della lotta contro i reati gravi consiste in tale capacità limitata di leggere il passato attraverso dati che mostrano la cronologia delle comunicazioni effettuate da una persona prima ancora di essere sospettata di avere un collegamento con un reato grave [54].

182. In sede di presentazione della proposta di direttiva che ha portato all'adozione della direttiva 2006/24, la Commissione ha illustrato tale utilità mediante diversi esempi concreti di indagini vertenti in particolare su atti di terrorismo, di omicidio, di sequestro di persona e di pedopornografia [55].

53 — La Commissione ha parimenti sottolineato che il valore aggiunto di un obbligo generale di conservazione di dati, rispetto a una conservazione mirata di dati, consiste in tale capacità limitata di leggere il passato: v. Commission Staff Working Document presentato in allegato alla proposta di direttiva che ha portato all'adozione della direttiva 2006/24, SEC(2005) 1131, 21 settembre 2005, n. 3.6, «Data Preservation versus Data Retention»: «[W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects».

54 — Il governo francese ha citato, a questo proposito, la relazione del Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, pagg. 209 e 210. Il Conseil d'État (Francia) sottolinea che un meccanismo di misure di sorveglianza mirate «sarebbe nettamente meno efficace della conservazione sistematica dal punto di vista della sicurezza nazionale e della ricerca degli autori di reati. Infatti, esso non consentirebbe un accesso retrospettivo agli scambi che hanno avuto luogo prima che l'autorità individuasse una minaccia o un reato: il suo carattere operativo dipenderebbe quindi dalla capacità delle autorità di conoscere in anticipo l'identità delle persone i cui dati di connessione possano essere utili, il che è impossibile nell'ambito della polizia giudiziaria. Ad esempio, nel caso di un reato, l'autorità giudiziaria non potrebbe avere accesso alle comunicazioni precedenti a quest'ultimo, elementi tuttavia preziosi e talvolta persino indispensabili per l'identificazione del suo autore e dei suoi complici, come hanno dimostrato casi recenti di attentati terroristici. Nel campo della prevenzione degli attentati alla sicurezza nazionale, i nuovi programmi tecnici si basano su una capacità di rilevamento dei segnali deboli, incompatibile con l'idea dell'individuazione preventiva delle persone pericolose».

55 — Commission Staff Working Document presentato in allegato alla proposta di direttiva che ha portato all'adozione della direttiva 2006/24, SEC(2005) 1131, 21 settembre 2005, n. 1.2, «The importance of traffic data for law enforcement».

183. Vari esempi simili sono stati esposti alla Corte nell'ambito delle presenti cause, segnatamente dal governo francese, il quale ha sottolineato l'obbligo positivo che incombe agli Stati membri di garantire la sicurezza delle persone presenti sul loro territorio. Secondo tale governo, nell'ambito delle indagini relative allo smantellamento delle reti che organizzano la partenza di residenti francesi verso zone di conflitto in Iraq o in Siria, l'accesso ai dati conservati gioca un ruolo determinante ai fini dell'identificazione delle persone che hanno facilitato tale partenza. Detto governo aggiunge che l'accesso ai dati relativi alle comunicazioni delle persone coinvolte nei recenti attentati terroristici del gennaio e del novembre 2015 in Francia è stata estremamente utile agli inquirenti per scoprire i complici degli autori di tali attentati. Parimenti, nell'ambito della ricerca di una persona scomparsa, i dati relativi all'ubicazione di tale persona durante comunicazioni effettuate prima della sua scomparsa potrebbero svolgere un ruolo determinante ai fini dell'indagine.

184. Alla luce delle considerazioni che precedono, ritengo che un obbligo generale di conservazione di dati sia idoneo a contribuire alla lotta contro i reati gravi. Resta tuttavia da verificare se un siffatto obbligo sia necessario e proporzionato a tale obiettivo.

5. Sul carattere necessario di un obbligo generale di conservazione di dati alla luce della lotta contro i reati gravi

185. Secondo giurisprudenza costante, una misura può essere considerata necessaria soltanto in assenza di qualsiasi altra misura che sia altrettanto adeguata pur essendo meno restrittiva [56].

186. Il requisito relativo al carattere adeguato si risolve nel valutare l'efficacia «assoluta» – indipendentemente da qualsiasi altra misura ipotizzabile – di un obbligo generale di conservazione di dati alla luce della lotta contro i reati gravi. Il requisito della necessità porta, dal canto suo, a valutare l'efficienza – o efficacia «relativa», vale a dire in confronto a qualsiasi altra misura ipotizzabile – di un tale obbligo [57].

187. Nel contesto delle presenti cause, il test di necessità impone di verificare, da una parte, se altre misure possano essere altrettanto efficaci di un obbligo generale di conservazione di dati nella lotta contro i reati gravi e, dall'altra, se tali eventuali misure siano meno lesive dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta [58].

188. Ricordo inoltre la giurisprudenza costante, richiamata al punto 52 della sentenza DRI, secondo la quale la protezione del diritto fondamentale alla vita privata richiede che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello «stretto necessario» [59].

56 — V., in particolare, sentenze del 22 gennaio 2013, Sky Österreich (C-283/11, EU:C:2013:28, punti da 54 a 57); del 13 novembre 2014, Reindl (C-443/13, EU:C:2014:2370, punto 39), e del 16 luglio 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punti da 120 a 122). Nella dottrina, v. in particolare Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, pag. 29: «Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value».

57 — V. Rivers, J., «Proportionality and variable intensity of review», 65(1) *Cambridge Law Journal* (2006) 174, pag. 198: «The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest».

58 — Sull'esistenza di tali due componenti nel test di necessità, v. Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pagg. da 323 a 331.

59 — V., in particolare, sentenze del 9 novembre 2010, Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662, punti 77 e 86), e del 7 novembre 2013, IPI (C-473/12, EU:C:2013:715, punto 39).

189. Le parti che hanno presentato osservazioni alla Corte hanno discusso ampiamente due problematiche relative al requisito di stretta necessità nel contesto delle presenti cause, che corrispondono in sostanza alle due questioni sollevate dal giudice del rinvio nella causa C-203/15:

— da una parte, se, alla luce dei punti da 56 a 59 della sentenza DRI, debba considerarsi che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario ai fini della lotta contro i reati gravi, indipendentemente da eventuali garanzie che accompagnino tale obbligo;

— dall'altra, nell'ipotesi in cui possa considerarsi che un tale obbligo non ecceda, di per sé, i limiti dello stretto necessario, se esso debba essere accompagnato dall'insieme delle garanzie menzionate dalla Corte ai punti da 60 a 68 della sentenza DRI al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta.

190. Prima di trattare tali questioni, ritengo opportuno respingere un argomento addotto dal governo del Regno Unito, secondo cui i criteri stabiliti nella sentenza DRI sarebbero irrilevanti nel contesto delle presenti cause, in quanto detta sentenza riguardava non già un regime nazionale, bensì un regime stabilito dal legislatore dell'Unione.

191. A questo proposito, sottolineo che la sentenza DRI ha interpretato gli articoli 7, 8 e 52, paragrafo 1, della Carta e che tali disposizioni sono parimenti oggetto delle questioni sollevate nei procedimenti principali. Orbene, è impossibile, a mio avviso, interpretare le disposizioni della Carta in modo diverso a seconda che il regime in questione sia stato stabilito a livello dell'Unione o a livello nazionale, come hanno sottolineato giustamente i sigg. Brice e Lewis nonché la Law Society of England and Wales. Laddove si sia constatato che la Carta è applicabile, come avviene nelle presenti cause [60], quest'ultima deve essere applicata nello stesso modo, indipendentemente dal regime in questione. Pertanto, i criteri stabiliti dalla Corte nella sentenza DRI sono rilevanti ai fini della valutazione dei regimi nazionali di cui trattasi nelle presenti cause, come hanno sostenuto segnatamente i governi danese e irlandese nonché la Commissione.

a) Sul carattere strettamente necessario di un obbligo generale di conservazione di dati

192. Secondo un primo orientamento, sostenuto dalla Tele2 Sverige nonché dall'Open Rights Group e dalla Privacy International, deve considerarsi, alla luce della sentenza DRI, che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario ai fini della lotta contro i reati gravi, indipendentemente da eventuali garanzie che accompagnino tale obbligo.

193. Stando a un secondo orientamento, sostenuto dalla maggioranza delle altre parti che hanno presentato osservazioni alla Corte, un siffatto obbligo non eccede i limiti dello stretto necessario qualora sia accompagnato da talune garanzie riguardanti l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati.

194. I seguenti motivi mi inducono ad adottare questo secondo orientamento.

195. In primo luogo, secondo la mia lettura della sentenza DRI, la Corte ha dichiarato che un obbligo generale di conservazione di dati eccede i limiti dello stretto necessario qualora esso *non sia accompagnato* da garanzie rigorose riguardanti l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati. Per contro, la Corte non si è pronunciata sulla compatibilità con il diritto dell'Unione di un obbligo generale di conservazione di dati che sia *accompagnato* da tali garanzie, in quanto un siffatto regime non formava oggetto delle questioni sottoposte alla Corte in detta causa.

60 — V. paragrafi da 117 a 125 delle presenti conclusioni.

196. A questo proposito, sottolineo che i punti da 56 a 59 della sentenza DRI non contengono alcuna dichiarazione della Corte nel senso che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario.

197. Ai punti 56 e 57 di tale sentenza, la Corte constata che l'obbligo di conservazione previsto dalla direttiva 2006/24 riguarda qualsiasi mezzo di comunicazione elettronica, tutti gli utenti nonché l'insieme dei dati relativi al traffico, senza alcuna distinzione, limitazione o eccezione basata sull'obiettivo della lotta contro i reati gravi.

198. Ai punti 58 e 59 di detta sentenza, la Corte espone in modo più dettagliato le conseguenze pratiche di tale assenza di distinzione. Da una parte, detto obbligo di conservazione riguarda anche 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. Dall'altra, detta 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.

199. In tal modo, la Corte constata che un obbligo generale di conservazione di dati si caratterizza per la sua assenza di distinzione sulla base dell'obiettivo della lotta contro i reati gravi. Tuttavia, essa non ha dichiarato che tale assenza di distinzione significava che un siffatto obbligo eccedeva, di per sé, i limiti dello stretto necessario.

200. In realtà, è soltanto al termine dell'esame del regime previsto dalla direttiva 2006/24, e dopo aver constatato l'assenza di talune garanzie che esaminerò in seguito [61], che la Corte dichiara, al punto 69 della sentenza DRI, quanto segue:

«*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» (il corsivo è mio).

201. Come hanno sostenuto i governi tedesco e neerlandese, se la mera conservazione generalizzata dei dati fosse stata sufficiente a causare l'invalidità della direttiva 2006/24, la Corte non avrebbe avuto bisogno di esaminare, per di più in maniera dettagliata, l'assenza delle garanzie menzionate ai punti da 60 a 68 di detta sentenza.

202. Pertanto, l'obbligo generale di conservazione di dati previsto dalla direttiva 2006/24 non eccedeva, di per sé, i limiti dello stretto necessario. Tale direttiva eccedeva i limiti dello stretto necessario a causa dell'*effetto combinato* della conservazione generalizzata dei dati e dell'assenza di garanzie volte a limitare allo stretto necessario la lesione dei diritti sanciti dagli articoli 7 e 8 della Carta. A causa di tale effetto combinato, la direttiva doveva essere dichiarata invalida nella sua interezza [62].

61 — V. paragrafi da 216 a 245 delle presenti conclusioni.

62 — V. sentenza DRI, punto 65: «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» (il corsivo è mio).

203. In secondo luogo, trovo conferma di tale interpretazione al punto 93 della sentenza Schrems [63], che riproduco di seguito:

«In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti *senza* alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito *e senza che* sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta [v., in tal senso, per quanto riguarda la direttiva 2006/24, sentenza DRI, punti da 57 a 61]» (il corsivo è mio).

204. Anche in questo caso, la Corte non ha dichiarato che il regime in questione in tale causa eccedeva i limiti dello stretto necessario per il solo fatto che esso autorizzava una conservazione generalizzata di dati personali. Nella specie, i limiti dello stretto necessario erano superati a causa dell'effetto combinato della possibilità di una tale conservazione generalizzata e dell'assenza di garanzie riguardanti l'accesso al fine di limitare l'ingerenza allo stretto necessario.

205. Da quanto precede, deduco che non si deve sempre considerare che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario ai fini della lotta contro i reati gravi. Per contro, un siffatto obbligo eccede sempre i limiti dello stretto necessario qualora non sia accompagnato da garanzie riguardanti l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati.

206. Inoltre, la mia opinione a tale riguardo è confermata dalla necessità di verificare in concreto il rispetto del requisito di stretta necessità nel contesto dei regimi nazionali di cui trattasi nei procedimenti principali.

207. Come ho già esposto al paragrafo 187 delle presenti conclusioni, il requisito di stretta necessità impone di esaminare se altre misure possano essere altrettanto efficaci quanto un obbligo generale di conservazione di dati nella lotta contro i reati gravi, pur essendo meno lesive dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta.

208. Orbene, una tale valutazione deve essere effettuata nel contesto specifico di ciascun regime nazionale che preveda un obbligo generale di conservazione di dati. Da una parte, siffatta valutazione richiede un confronto tra l'efficacia di tale obbligo e quella di qualsiasi altra misura ipotizzabile nel contesto nazionale, tenendo conto del fatto che detto obbligo offre alle autorità competenti una capacità limitata di leggere il passato attraverso i dati conservati [64].

209. Alla luce del requisito di stretta necessità, è imperativo che detti giudici non si limitino a verificare la mera utilità di un obbligo generale di conservazione di dati, bensì verifichino rigorosamente che nessun'altra misura o combinazione di misure, e segnatamente un obbligo mirato di conservazione di dati accompagnato da altri strumenti investigativi, possa offrire la medesima efficacia nella lotta contro i reati gravi. A questo proposito, sottolineo che diversi studi portati all'attenzione della Corte rimettono in discussione la necessità di tale tipo di obbligo ai fini della lotta contro i reati gravi [65].

63 — Sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650).

64 — V. paragrafi da 178 a 183 delle presenti conclusioni.

65 — V. commissario per i diritti umani del Consiglio d'Europa, «Issue paper on the rule of law on the Internet and in the wider digital world», dicembre 2014, CommDH/IssuePaper(2014)1, pag. 115; Consiglio per i diritti umani delle Nazioni unite, Relazione dell'Alto Commissariato delle Nazioni unite per i diritti umani sul diritto alla privacy nell'era digitale, 30 giugno 2014, A/HRC/27/37, n. 26; Assemblea generale delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta al terrorismo, 23 settembre 2014, A/69/397, nn. 18 e 19.

210. Dall'altra parte, ammesso che altre misure possano essere altrettanto efficaci nella lotta contro i reati gravi, ai giudici del rinvio spetterà l'ulteriore compito di determinare se queste ultime siano meno lesive dei diritti fondamentali in questione rispetto a un obbligo generale di conservazione di dati, ai sensi della giurisprudenza costante richiamata al paragrafo 185 delle presenti conclusioni.

211. Alla luce del punto 59 della sentenza DRI, ai giudici nazionali spetterà verificare, in particolare, la possibilità di limitare la portata materiale dell'obbligo di conservazione preservando nel contempo l'efficacia di tale misura nella lotta contro i reati gravi [66]. Obblighi di tal genere possono avere, infatti, una portata materiale più o meno ampia, a seconda degli utenti, delle aree geografiche e dei mezzi di comunicazione interessati [67].

212. A mio avviso, sarebbe auspicabile soprattutto, qualora la tecnologia lo consentisse, escludere dall'obbligo di conservazione i dati particolarmente sensibili in relazione ai diritti fondamentali di cui trattasi nelle presenti cause, quali i dati coperti dal segreto professionale e i dati che consentono di individuare le fonti dei giornalisti.

213. Occorre, tuttavia, tenere presente che una limitazione sostanziale della portata di un obbligo generale di conservazione di dati rischia di ridurre considerevolmente l'utilità offerta da tale regime nella lotta contro i reati gravi. Da una parte, diversi governi hanno sottolineato la difficoltà o addirittura l'impossibilità di determinare in anticipo i dati che possano presentare un collegamento con un reato grave. Pertanto, una siffatta limitazione rischia di escludere la conservazione di dati che potrebbero rivelarsi rilevanti ai fini della lotta contro i reati gravi.

214. Dall'altra, come ha sostenuto il governo estone, la criminalità grave è un fenomeno dinamico, capace di adattarsi agli strumenti investigativi di cui dispongono le autorità di contrasto. Pertanto, una limitazione a un'area geografica o a un mezzo di comunicazione determinati rischierebbe di provocare un trasferimento delle attività legate ai reati gravi verso un'area geografica e/o un mezzo di comunicazione non coperti da detto regime.

215. In quanto richiede un'analisi complessa dei regimi nazionali in questione nei procedimenti principali, ritengo che tale valutazione debba essere effettuata dai giudici nazionali, come hanno sottolineato i governi ceco, estone, irlandese, francese e neerlandese, nonché la Commissione.

b) Sul carattere imperativo delle garanzie enunciate dalla Corte ai punti dai 60 a 68 della sentenza DRI alla luce del requisito di stretta necessità

216. Ammesso che un obbligo generale di conservazione di dati possa essere considerato strettamente necessario nel contesto del regime nazionale in questione, ciò che dovrà essere valutato dal giudice nazionale, occorre inoltre determinare se un siffatto obbligo debba essere accompagnato dall'insieme delle garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta.

217. Tali garanzie riguardano le norme che disciplinano l'accesso e l'utilizzo dei dati conservati da parte delle autorità competenti (punti da 60 a 62 della sentenza DRI), la durata di conservazione dei dati (punti 63 e 64 di tale sentenza) nonché la sicurezza e la protezione dei dati conservati dai fornitori (punti da 66 a 68 di detta sentenza).

66 — Tale osservazione riguarda unicamente gli obblighi generali di conservazione di dati (che possono riguardare qualsiasi persona, indipendentemente da un qualunque collegamento con un reato grave) e non le misure di sorveglianza mirate (le quali riguardano persone che sono state precedentemente individuate come aventi un collegamento con un reato grave): su questa distinzione, v. paragrafi da 178 a 183 delle presenti conclusioni.

67 — Il governo tedesco ha in particolare precisato, all'udienza, che il Parlamento tedesco ha escluso i messaggi di posta elettronica dall'obbligo di conservazione imposto dalla legislazione tedesca, ma che tale regime riguarda tutti gli utenti e l'intero territorio nazionale.

218. Nell'ambito delle osservazioni presentate alla Corte, si sono contrapposte due tesi in merito alla natura di dette garanzie.

219. Secondo una prima tesi, sostenuta dal sig. Watson, dai sigg. Brice e Lewis nonché dall'Open Rights Group e dalla Privacy International, le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI sono imperative. Secondo detta tesi, la Corte ha stabilito garanzie minime che devono essere *tutte* soddisfatte dal regime nazionale in questione al fine di limitare allo stretto necessario la lesione dei diritti fondamentali.

220. Stando a una seconda tesi, sostenuta dai governi tedesco, estone, irlandese, francese e del Regno Unito, le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI sono meramente indicative. La Corte avrebbe proceduto ad una «valutazione complessiva» delle garanzie assenti nel regime previsto dalla direttiva 2006/24, senza che una qualsiasi di tali garanzie possa, in maniera isolata, essere considerata imperativa alla luce del requisito di stretta necessità. Per illustrare tale tesi, il governo tedesco ha evocato l'immagine dei «vasi comunicanti», in virtù della quale un approccio meno rigoroso su uno dei tre aspetti individuati dalla Corte (ad esempio, l'accesso ai dati conservati) potrebbe essere compensato da un approccio più rigoroso per quanto riguarda gli altri due aspetti (la durata di conservazione nonché la sicurezza e la protezione dei dati).

221. Sono convinto che detta tesi dei «vasi comunicanti» debba essere respinta e che *tutte* le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI debbano essere considerate imperative, per i motivi seguenti.

222. In primo luogo, le espressioni utilizzate dalla Corte nel suo esame della stretta necessità del regime stabilito dalla direttiva 2006/24 non si prestano a una tale interpretazione. In particolare, la Corte non fa mai riferimento, ai punti da 60 a 68 di detta sentenza, a una qualsiasi possibilità di «compensare» un approccio meno rigoroso su uno dei tre aspetti da essa individuati con un approccio più rigoroso per quanto riguarda gli altri due aspetti.

223. In realtà, mi sembra che la tesi dei «vasi comunicanti» prenda le mosse da una confusione tra il requisito di necessità e quello di proporzionalità stricto sensu, il quale non è stato esaminato dalla Corte nella sentenza DRI. Infatti, come ho affermato al paragrafo 186 delle presenti conclusioni, il requisito di necessità consiste nel respingere qualsiasi misura inefficiente. Non possono aver luogo, in tale contesto, «valutazioni complessive», «compensazioni» o «bilanciamenti», i quali intervengono soltanto nella fase della proporzionalità stricto sensu [68].

224. In secondo luogo, detta tesi dei «vasi comunicanti» priverebbe di ogni effetto utile le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI, cosicché le persone i cui dati sono stati conservati non disporrebbero più di garanzie sufficienti che consentano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti di tali dati, come prescrive il punto 54 di detta sentenza.

225. L'effetto distruttivo di siffatta tesi può essere facilmente illustrato mediante i seguenti esempi. Un regime nazionale che limitasse rigorosamente l'accesso ai soli fini della lotta al terrorismo e che limitasse la durata di conservazione a tre mesi (approccio rigoroso quanto all'accesso e alla durata di conservazione), ma che non obbligasse i fornitori a conservare i dati sul proprio territorio nazionale e in forma criptata (approccio permissivo quanto alla sicurezza), esporrebbe tutta la propria popolazione a un rischio elevato di accesso illegale ai dati conservati. Analogamente, un regime nazionale che

68 — V. Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pag. 344: «The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose. (…) Accordingly, those tests are referred to as means-end analysis.*They are not based on balancing*. The test of proportionality stricto sensu is different. (…) It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. *It is based on balancing*» (il corsivo è mio).

prevedesse una durata di conservazione di tre mesi nonché una conservazione dei dati sul proprio territorio nazionale e in forma criptata (approcci rigorosi quanto alla durata e alla sicurezza), ma che consentisse a tutti i dipendenti di tutte le autorità pubbliche di accedere ai dati conservati (approccio permissivo quanto all'accesso), esporrebbe tutta la propria popolazione a un rischio elevato di abusi da parte delle autorità nazionali.

226. A mio avviso, da tali esempi emerge che la preservazione dell'effetto utile delle garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI impone di considerare imperativa *ciascuna* di queste ultime. La Corte EDU ha parimenti sottolineato l'importanza fondamentale di dette garanzie nella recente sentenza Szabó e Vissy c. Ungheria, citando espressamente la sentenza DRI [69].

227. Inoltre, non mi sembra che l'attuazione di tali garanzie, da parte degli Stati membri che desiderano imporre un obbligo generale di conservazione di dati, ponga notevoli difficoltà pratiche. In realtà, dette garanzie mi sembrano, sotto molti aspetti, «minime», come ha affermato il sig. Watson.

228. Alcune di queste garanzie sono state discusse dinanzi alla Corte a causa della loro possibile assenza nell'ambito dei regimi nazionali di cui trattasi nei procedimenti principali.

229. In primo luogo, dai punti 61 e 62 della sentenza DRI risulta che l'accesso e l'utilizzo ulteriore dei dati conservati devono essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative.

230. Secondo la Tele2 Sverige e la Commissione, tale requisito non è rispettato dal regime svedese di cui trattasi nella causa C-203/15, il quale consentirebbe l'accesso ai dati conservati a fini di lotta contro reati minori. Una censura simile è espressa dai sigg. Brice e Lewis nonché dal sig. Watson nei confronti del regime del Regno Unito in questione nella causa C-698/15, il quale autorizzerebbe l'accesso a fini di lotta contro reati minori e anche in assenza di reati.

231. Se, da un lato, non spetta alla Corte pronunciarsi sul contenuto di tali regimi nazionali, dall'altro, essa è competente ad individuare gli obiettivi di interesse generale che possano giustificare un'ingerenza grave nei diritti sanciti dalla direttiva e dagli articoli 7 e 8 della Carta. Nel caso di specie, ho già esposto le ragioni per le quali ritengo che *soltanto* la lotta contro i reati gravi possa giustificare una siffatta ingerenza [70].

232. In secondo luogo, ai sensi del punto 62 della sentenza DRI, l'accesso ai dati conservati deve essere 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. Tale previo controllo deve inoltre intervenire a seguito di una richiesta motivata delle suddette autorità presentata nell'ambito di procedure di prevenzione, di accertamento o di indagini penali.

233. Secondo le osservazioni della Tele2 Sverige e della Commissione, detta garanzia di controllo indipendente e precedente all'accesso sarebbe parzialmente assente nel regime svedese in questione nella causa C-203/15. La stessa constatazione, la cui veridicità non è contestata dal governo del Regno Unito, è effettuata dai sigg. Brice e Lewis, dal sig. Watson, nonché dall'Open Rights Group e dalla Privacy International per quanto riguarda il regime del Regno Unito in questione nella causa C-698/15.

69 — Corte EDU, 12 gennaio 2016, Szabó e Vissy c. Ungheria, CE:ECHR:2016:0112JUD003713814, § 68: «Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information».

70 — V. paragrafi da 170 a 173 delle presenti conclusioni.

234. Non vedo alcun motivo per rendere meno rigoroso detto requisito di previo controllo da parte di un'entità indipendente, che risulta incontestabilmente dal linguaggio utilizzato dalla Corte al punto 62 della sentenza DRI [71]. In primo luogo, tale requisito è imposto dalla gravità dell'ingerenza e dei rischi causati dalla costituzione di banche dati che coprono la quasi totalità della popolazione interessata [72]. Sottolineo che diversi esperti in materia di tutela dei diritti umani nella lotta al terrorismo hanno criticato l'attuale tendenza consistente nel sostituire le tradizionali procedure di autorizzazione indipendente e di controllo effettivo con sistemi di «auto-autorizzazione» all'accesso ai dati da parte dei servizi di intelligence e di polizia [73].

235. Inoltre, un controllo indipendente e precedente all'accesso ai dati è necessario al fine di consentire un trattamento caso per caso dei dati particolarmente sensibili in relazione ai diritti fondamentali di cui trattasi nelle presenti cause, quali i dati coperti dal segreto professionale e i dati che consentono di individuare le fonti dei giornalisti, come hanno sottolineato la Law Society of England and Wales nonché i governi francese e tedesco. Tale controllo precedente all'accesso è ancora più necessario nell'ipotesi in cui sia tecnicamente difficile escludere l'insieme dei suddetti dati nella fase della conservazione [74].

236. Infine, aggiungo che, da un punto di vista pratico, nessuna delle tre parti interessate da una richiesta di accesso è in grado di esercitare un controllo effettivo sull'accesso ai dati conservati. Le autorità competenti in materia di repressione hanno tutto l'interesse a chiedere un accesso quanto più ampio possibile a tali dati. I fornitori, che non conoscono il fascicolo di indagine, non possono verificare se la richiesta di accesso sia limitata allo stretto necessario. Quanto alle persone i cui dati sono consultati, esse non hanno modo di sapere di essere oggetto di una tale misura di indagine, e ciò anche in caso di utilizzo abusivo o illecito, come hanno evidenziato il sig. Watson e i sigg. Brice e Lewis. Siffatta configurazione degli interessi in gioco richiede, a mio avviso, l'intervento di un'entità indipendente prima della consultazione dei dati conservati, al fine di proteggere le persone i cui dati sono conservati da qualsiasi accesso abusivo da parte delle autorità competenti.

237. Ciò premesso, mi sembra ragionevole considerare che situazioni specifiche di estrema urgenza, evocate dal governo del Regno Unito, possono giustificare un accesso immediato ai dati conservati da parte delle autorità di contrasto, senza previo controllo, al fine di prevenire la commissione di reati gravi o di perseguire gli autori di tali reati [75]. Per quanto possibile, è imperativo mantenere il requisito di un'autorizzazione preventiva istituendo una procedura d'urgenza all'interno dell'entità indipendente per il trattamento di tale tipo di richiesta di accesso. Tuttavia, nei casi in cui il semplice fatto di adire tale entità con una richiesta di accesso appaia incompatibile con l'estrema urgenza della situazione, l'accesso e l'utilizzo dei dati dovranno essere oggetto, nel più breve termine, di un controllo a posteriori da parte di detta entità.

71 — Preciso nondimeno che tale requisito di controllo previo e indipendente non può, a mio avviso, trovare la propria fonte nell'articolo 8, paragrafo 3, della Carta, poiché quest'ultima non è applicabile, di per sé, alle disposizioni nazionali che disciplinano l'accesso ai dati conservati: v. paragrafi da 123 a 125 delle presenti conclusioni.

72 — V. paragrafi da 252 a 261 delle presenti conclusioni.

73 — Consiglio per i diritti umani delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta al terrorismo, 28 dicembre 2009, A/HRC/13/37, n. 62: «[N]on deve esistere alcun sistema segreto di sorveglianza che non sia sottoposto alla supervisione di un'autorità di controllo efficace, né alcuna ingerenza che non sia autorizzata da un organismo indipendente» (v. anche n. 51). V. inoltre Assemblea generale delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta al terrorismo, 23 settembre 2014, A/69/397, n. 61.

74 — V. paragrafo 212 delle presenti conclusioni. Per quanto riguarda le fonti dei giornalisti, la Corte EDU ha sottolineato la necessità di un'autorizzazione preventiva da parte di un'entità indipendente, in quanto un controllo a posteriori non consente di ripristinare la riservatezza di tali fonti: v. Corte EDU, 22 novembre 2012, Telegraaf Media Nederland Landelijke Media B.V. e altri c. Paesi Bassi, CE:ECHR:2012:1122JUD003931506, § 101 e Corte EDU, 12 gennaio 2016, Szabó e Vissy c. Ungheria, CE:ECHR:2016:0112JUD003713814, § 77. Nella sentenza Kopp c. Svizzera, che riguardava la sorveglianza di linee telefoniche di un avvocato, la Corte EDU ha censurato il fatto che un funzionario appartenente all'amministrazione fosse incaricato, senza controllo da parte di un magistrato indipendente, di filtrare le informazioni coperte dal segreto professionale: v. Corte EDU, 25 marzo 1998, Kopp c. Svizzera, CE:ECHR:1998:0325JUD002322494, § 74.

75 — V., a questo proposito, il meccanismo descritto al paragrafo 22 delle presenti conclusioni. Sottolineo che tale problematica non è stata affrontata dalla Corte nella sentenza DRI.

238. Inoltre, il punto 68 della sentenza DRI stabilisce l'obbligo, a carico dei fornitori, di conservare i dati sul territorio dell'Unione, al fine di garantire il controllo da parte di un'autorità indipendente, richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza enunciati ai punti 66 e 67 di tale sentenza.

239. La Tele2 Sverige e la Commissione hanno sostenuto che la conservazione dei dati sul territorio nazionale non è garantita nell'ambito del regime svedese in questione nella causa C-203/15. La medesima censura è sollevata dai sigg. Brice e Lewis nonché dal sig. Watson nei confronti del regime del Regno Unito in questione nella causa C-698/15.

240. A questo proposito, da una parte, non vedo alcuna ragione per indebolire detto requisito stabilito al punto 68 della sentenza DRI, poiché una conservazione dei dati al di fuori del territorio dell'Unione non consentirebbe di garantire alle persone i cui dati sono conservati il livello di protezione offerto dalla direttiva 2002/58 e dagli articoli 7, 8 e 52, paragrafo 1, della Carta [76].

241. Mi sembra ragionevole, dall'altra, adattare tale requisito, sancito dalla Corte nel contesto della direttiva 2006/24, al contesto dei regimi nazionali, prevedendo la conservazione dei dati sul territorio nazionale, come sostenuto dai governi tedesco e francese nonché dalla Commissione. Infatti, ai sensi dell'articolo 8, paragrafo 3, della Carta, spetta a ciascuno Stato membro garantire il controllo, da parte di un'autorità indipendente, del rispetto degli obblighi di protezione e di sicurezza previsti dal proprio regime nazionale da parte dei fornitori. Orbene, in assenza di un coordinamento a livello dell'Unione, una siffatta autorità nazionale potrebbe trovarsi nell'impossibilità di svolgere i propri compiti di controllo sul territorio di un altro Stato membro.

242. Infine, per quanto riguarda la durata di conservazione, i giudici del rinvio dovranno applicare i criteri definiti dalla Corte ai punti 63 e 64 della sentenza DRI. Da una parte, tali giudici devono determinare se i dati conservati possano essere distinti sulla base della loro utilità e, in questo caso, se la durata di conservazione sia stata adeguata in funzione di tale criterio. Dall'altra, detti giudici devono verificare che la durata di conservazione sia basata su criteri obiettivi in grado di garantire che quest'ultima sia limitata allo stretto necessario.

243. Sottolineo che la Corte EDU, nella recente sentenza Roman Zakharov c. Russia, ha giudicato ragionevole una durata massima di conservazione di sei mesi, pur deplorando l'assenza di un obbligo di distruggere immediatamente i dati che non hanno alcuna relazione con lo scopo per il quale sono stati raccolti [77]. A questo proposito, aggiungo che i regimi nazionali di cui trattasi nei procedimenti principali devono prevedere un obbligo di distruggere irreversibilmente qualsiasi dato conservato non appena esso non sia più strettamente necessario alla lotta contro i reati gravi. Tale obbligo deve essere rispettato non solo dai fornitori che procedono alla conservazione dei dati, ma anche dalle autorità che hanno avuto accesso ai dati conservati.

244. Alla luce delle considerazioni che precedono, ritengo che tutte le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI abbiano carattere imperativo e debbano, pertanto, accompagnare un obbligo generale di conservazione di dati al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta.

245. Spetta ai giudici del rinvio verificare che i regimi nazionali di cui trattasi nei procedimenti principali contengano ciascuna di tali garanzie.

76 — V., a tale riguardo, sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650).

77 — V., a tale riguardo, Corte EDU, 4 dicembre 2015, Roman Zakharov c. Russia, CE:ECHR:2015:1204JUD004714306, §§ 254 e 255. Secondo il diritto russo, la distruzione degli elementi intercettati doveva avvenire al termine di un periodo di conservazione di sei mesi qualora la persona interessata non fosse stata accusata di un reato. La Corte EDU ha giudicato ragionevole la durata massima di conservazione, precisamente sei mesi, fissata dal diritto russo per tali dati. Essa ha tuttavia deplorato l'assenza di un obbligo di distruggere immediatamente i dati che non hanno alcuna relazione con lo scopo per il quale sono stati raccolti, precisando che la conservazione automatica, per la durata di sei mesi, di dati manifestamente privi di interesse non può ritenersi giustificata alla luce dell'articolo 8 della CEDU.

6. Sul carattere proporzionato, in una società democratica, di un obbligo generale di conservazione di dati alla luce dell'obiettivo della lotta contro i reati gravi

246. Dopo aver verificato il carattere necessario dei regimi nazionali di cui trattasi nei procedimenti principali, ai giudici del rinvio spetta inoltre verificarne il carattere proporzionato, in una società democratica, alla luce dell'obiettivo della lotta contro i reati gravi. Tale aspetto non è stato esaminato dalla Corte nella sentenza DRI, poiché il regime stabilito dalla direttiva 2006/24 eccedeva i limiti dello stretto necessario ai fini della lotta contro i reati gravi.

247. Detto requisito di proporzionalità in una società democratica – o proporzionalità «stricto sensu» – deriva dall'articolo 15, paragrafo 1, della direttiva 2002/58, dall'articolo 52, paragrafo 1, della Carta e da una giurisprudenza costante. Secondo tale giurisprudenza costante, una misura che leda diritti fondamentali può considerarsi proporzionata soltanto se gli inconvenienti provocati non siano sproporzionati rispetto agli scopi perseguiti [78].

248. A differenza dei requisiti relativi al carattere adeguato e necessario della misura in questione, i quali valutano la sua efficacia alla luce dell'obiettivo perseguito, il requisito di proporzionalità stricto sensu consiste nel bilanciare i vantaggi risultanti da tale misura alla luce dell'obiettivo legittimo perseguito con gli inconvenienti che ne derivano alla luce dei diritti fondamentali garantiti in una società democratica [79]. Tale requisito dà luogo, pertanto, a un dibattito sui valori che devono prevalere in una società democratica e, in definitiva, sul tipo di società in cui vogliamo vivere [80].

249. Di conseguenza, come ho affermato al paragrafo 223 delle presenti conclusioni, è nella fase dell'esame della proporzionalità in senso stretto che occorre procedere a una valutazione complessiva del regime in questione, e non nella fase dell'esame di necessità come hanno affermato i sostenitori della tesi dei «vasi comunicanti» [81].

250. Ai sensi della giurisprudenza richiamata al paragrafo 247 delle presenti conclusioni, occorre bilanciare i vantaggi con gli inconvenienti, in una società democratica, di un obbligo generale di conservazione di dati. Tali vantaggi e inconvenienti sono intimamente connessi alla caratteristica essenziale di un siffatto obbligo, di cui essi costituiscono in qualche modo le due facce della medaglia, vale a dire il fatto che esso riguardi tutte le comunicazioni effettuate da tutti gli utenti senza che sia richiesto un qualsiasi collegamento con un reato grave.

251. Da una parte, ho già esposto ai paragrafi da 178 a 183 delle presenti conclusioni i vantaggi offerti, nella lotta contro i reati gravi, dalla conservazione dei dati relativi a tutte le comunicazioni effettuate sul territorio nazionale.

78 — V., in particolare, sentenze del 15 febbraio 2016, N. (C-601/15 PPU, EU:C:2016:84, punto 54; il carattere necessario è esaminato ai punti da 56 a 67, il carattere proporzionato ai punti 68 e 69); del 16 luglio 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punto 123; il carattere necessario è esaminato ai punti da 120 a 122, il carattere proporzionato ai punti da 123 a 127), e del 22 gennaio 2013, Sky Österreich (C-283/11, EU:C:2013:28, punto 50; il carattere necessario è esaminato ai punti da 54 a 57, il carattere proporzionato ai punti da 58 a 67).

79 — V. Rivers, J., «Proportionality and variable intensity of review», 65(1) *Cambridge Law Journal* (2006) 174, pag. 198: «It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable».

80 — V. Pirker B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, pag. 30: «In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail».

81 — La specificità del requisito di proporzionalità stricto sensu, rispetto ai requisiti del carattere adeguato e necessario, può essere illustrata dal seguente esempio. Immaginiamo che uno Stato membro imponga a tutte le persone residenti nel proprio territorio l'iniezione di un microchip di geolocalizzazione che consenta alle autorità di ricostruire i movimenti del suo portatore nel corso dell'ultimo anno. Una tale misura potrebbe essere considerata «necessaria» qualora nessun'altra misura consentisse di ottenere il medesimo livello di efficacia nella lotta contro i reati gravi. Tuttavia, a mio avviso, detta misura sarebbe sproporzionata in una società democratica, poiché gli inconvenienti risultanti dalla lesione dei diritti all'integrità fisica, al rispetto della vita privata e alla protezione dei dati di carattere personale sarebbero sproporzionati rispetto ai vantaggi che ne deriverebbero nella lotta contro i reati gravi.

252. Dall'altra, gli inconvenienti di un obbligo generale di conservazione dei dati derivano dal fatto che la stragrande maggioranza dei dati conservati riguardano persone che non avranno mai alcun collegamento con un reato grave. A questo proposito, è importante precisare la natura degli inconvenienti che subiranno tali persone. Orbene, detti inconvenienti sono di natura diversa a seconda del livello di ingerenza nei loro diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale.

253. Nell'ambito di un'ingerenza «individuale», che colpisce un determinato individuo, gli inconvenienti risultanti da un obbligo generale di conservazione di dati sono stati descritti con grande acume dall'avvocato generale Cruz Villalón ai paragrafi da 72 a 74 delle sue conclusioni nella causa DRI [82]. Per riprendere i termini utilizzati da quest'ultimo, l'impiego di tali dati può consentire di «creare una mappatura tanto fedele quanto esaustiva di una parte importante dei comportamenti di una persona facenti strettamente parte della sua vita privata, se non addirittura un ritratto completo e preciso della sua identità privata».

254. In altri termini, in un contesto individuale, un obbligo generale di conservazione di dati consente ingerenze tanto gravi quanto quelle permesse da misure di sorveglianza mirate, comprese quelle che intercettano il contenuto delle comunicazioni effettuate.

255. Sebbene la gravità di tali ingerenze individuali non possa essere sottovalutata, ritengo nondimeno che i rischi specifici derivanti da un obbligo generale di conservazione di dati si rivelino nel contesto di ingerenze «di massa».

256. Infatti, a differenza delle misure di sorveglianza mirate, un tale obbligo può facilitare notevolmente le ingerenze di massa, vale a dire le ingerenze che colpiscono una parte sostanziale o addirittura l'insieme della popolazione rilevante, come dimostrano i seguenti esempi.

257. Supponiamo, in primo luogo, che una persona che ha accesso ai dati conservati abbia intenzione di identificare, nell'ambito della popolazione di uno Stato membro, tutti gli individui che soffrono di disturbi psicologici. L'analisi a tal fine del contenuto di tutte le comunicazioni effettuate sul territorio nazionale richiederebbe risorse considerevoli. Invece, l'utilizzo delle banche dati relative alle comunicazioni consentirebbe di identificare istantaneamente tutti gli individui che hanno contattato uno psicologo durante il periodo di conservazione dei dati [83]. Aggiungo che tale tecnica potrebbe essere estesa a ciascuna delle specializzazioni mediche registrate in uno Stato membro [84].

82 — C-293/12 e C-594/12, EU:C:2013:845. V. inoltre sentenza DRI, punti 27 e 37.

83 — I dati conservati includono infatti l'identità della fonte e del destinatario di una comunicazione, dati che basterebbe incrociare con l'elenco dei numeri di telefono degli psicologi operanti sul territorio nazionale.

84 — V., a tale riguardo, Consiglio per i diritti umani delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta al terrorismo, 28 dicembre 2009, A/HRC/13/37, n. 42: «[I]n Germania, alcuni studi hanno evidenziato una conseguenza inquietante delle politiche di conservazione dei dati: il 52% delle persone intervistate ha dichiarato che era poco probabile che avrebbe utilizzato le telecomunicazioni per contattare un tossicologo, uno psicoterapeuta o un consulente matrimoniale a causa delle leggi sulla conservazione dei dati».

258. Supponiamo, in secondo luogo, che la medesima persona desideri identificare gli individui contrari alla politica del governo in carica. Anche in questo caso, l'analisi a tal fine del contenuto delle comunicazioni richiederebbe risorse considerevoli. Invece, l'utilizzo dei dati relativi alle comunicazioni consentirebbe di identificare tutti gli individui iscritti in elenchi di distribuzione di email che criticano la politica del governo. Inoltre, tali dati consentirebbero altresì di identificare gli individui che partecipano a una qualsiasi manifestazione pubblica di opposizione al governo [85].

259. Tengo a sottolineare che i rischi legati all'accesso ai dati relativi alle comunicazioni (o «metadati») possono essere equivalenti, se non addirittura superiori a quelli risultanti dall'accesso al contenuto di tali comunicazioni, come hanno evidenziato l'Open Rights Group e la Privacy International, la Law Society of England and Wales nonché una recente relazione dell'Alto Commissariato delle Nazioni unite per i diritti umani [86]. In particolare, come dimostrano gli esempi sopra citati, i «metadati» consentono una classificazione quasi istantanea di un'intera popolazione, ciò che invece non consente il contenuto delle comunicazioni.

260. Aggiungo che i rischi di accesso abusivo o illegale ai dati conservati non sono affatto teorici. Da un lato, il rischio di accesso abusivo da parte delle autorità competenti deve essere rapportato al numero estremamente elevato di richieste di accesso indicato nelle osservazioni presentate alla Corte. Nel contesto del regime svedese, la Tele2 Sverige ha dichiarato che riceveva circa 10 000 richieste di accesso al mese, cifra che non include le richieste ricevute da altri fornitori attivi sul territorio svedese. Per quanto riguarda il regime del Regno Unito, il sig. Watson ha riprodotto alcune cifre estratte da una relazione ufficiale da cui risultano 517 236 autorizzazioni e 55 346 autorizzazioni orali urgenti per il solo 2014. Dall'altro lato, il rischio di accesso illegale, da parte di qualsiasi persona, è connaturato all'esistenza stessa di banche dati archiviate su supporti informatici [87].

261. A mio avviso, spetta ai giudici del rinvio valutare se gli inconvenienti causati dagli obblighi generali di conservazione di dati di cui trattasi nei procedimenti principali non siano sproporzionati, in una società democratica, rispetto agli scopi perseguiti, ai sensi della giurisprudenza richiamata al paragrafo 247 delle presenti conclusioni. Nell'ambito di tale valutazione, detti giudici dovranno bilanciare i rischi e i vantaggi connessi ad un obbligo di tal genere, e precisamente:

— da una parte, i vantaggi connessi alla concessione di una capacità limitata di leggere il passato alle autorità preposte alla lotta contro i reati gravi [88] e,

— dall'altra, i gravi rischi derivanti, in una società democratica, dal potere di mappatura della vita privata di un individuo e dal potere di classificazione di un'intera popolazione.

85 — Poiché i dati conservati includono l'ubicazione della fonte e del destinatario di una comunicazione, qualsiasi persona che inizia o riceve una comunicazione durante una manifestazione può essere facilmente identificata grazie ai dati conservati. A tale riguardo, Marc Goodman, esperto dell'FBI e dell'Interpol nel campo dei rischi connessi alle nuove tecnologie, riferisce che, in un passato recente, il governo ucraino ha proceduto, durante una manifestazione dell'opposizione, all'identificazione di tutti i telefoni cellulari localizzati in prossimità di scontri di strada tra le forze dell'ordine e gli oppositori del governo. Tutti questi telefoni hanno quindi ricevuto un messaggio che l'autore descrive come il messaggio possibilmente più «orwelliano» mai inviato da un governo: «Gentile abbonato, Lei è stato registrato come partecipante a una grave turbativa dell'ordine pubblico» (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, pag. 153, traduzione libera). V. inoltre Consiglio per i diritti umani delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione del diritto di libertà di opinione ed espressione, 17 aprile 2013, A/HRC/23/40, n. 75, e Consiglio per i diritti umani delle Nazioni unite, relazione dell'Alto Commissariato delle Nazioni unite per i diritti umani sul diritto alla privacy nell'era digitale, 30 giugno 2014, A/HRC/27/37, n. 3.

86 — V., a tale riguardo, Consiglio per i diritti umani delle Nazioni unite, relazione dell'Alto Commissariato delle Nazioni unite per i diritti umani sul diritto alla privacy nell'era digitale, 30 giugno 2014, A/HRC/27/37, n. 19: «Nello stesso ordine di idee, alcuni sostengono che l'intercettazione – o la raccolta – di dati su una comunicazione, e non anche del contenuto della comunicazione, non costituisce di per sé un'ingerenza nella vita privata. Orbene, dal punto di vista del diritto alla vita privata, tale distinzione non convince. Le aggregazioni di informazioni comunemente denominate "metadati" possono fornire indicazioni sulla condotta di un individuo, sulle sue relazioni sociali, sulle sue preferenze personali e sulla sua identità *che vanno ben al di là di ciò che si ottiene accedendo al contenuto* di una comunicazione privata» (il corsivo è mio). V. inoltre Assemblea generale delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta al terrorismo, 23 settembre 2014, A/69/397, n. 53.

87 — V. in particolare Consiglio per i diritti umani delle Nazioni unite, rapporto del relatore speciale sulla promozione e la protezione del diritto di libertà di opinione ed espressione, 17 aprile 2013, A/HRC/23/40, n. 67: «Le banche dati di comunicazioni diventano vulnerabili al furto, alla frode e alla divulgazione accidentale».

88 — V. paragrafi da 178 a 183 delle presenti conclusioni.

262. Detta valutazione deve essere effettuata alla luce di tutte le caratteristiche rilevanti dei regimi nazionali di cui trattasi nei procedimenti principali. A tale riguardo, sottolineo che le garanzie imperative enunciate dalla Corte ai punti da 60 a 68 della sentenza DRI costituiscono soltanto garanzie minime al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla direttiva 2002/58 e degli articoli 7 e 8 della Carta. Di conseguenza, non è escluso che un regime nazionale che contenga tutte le suddette garanzie debba nondimeno essere considerato sproporzionato all'interno di una società democratica, a motivo della sproporzione tra i gravi rischi causati da detto obbligo in una società democratica e i vantaggi che ne derivano nella lotta contro i reati gravi.

VI – **Conclusione**

263. Alla luce di quanto precede, propongo alla Corte di rispondere nei seguenti termini alle questioni pregiudiziali sollevate dal Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla Court of Appeal (England & Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (sezione civile), Regno Unito]:

L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), quale modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, nonché gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea devono essere interpretate nel senso che esse non ostano a che uno Stato membro imponga ai fornitori di servizi di comunicazione elettronica un obbligo di conservare tutti i dati relativi alle comunicazioni effettuate dagli utenti dei loro servizi, qualora siano soddisfatte tutte le condizioni seguenti, circostanza che spetta ai giudici del rinvio verificare alla luce di tutte le caratteristiche rilevanti dei regimi nazionali di cui trattasi nei procedimenti principali:

— tale obbligo e le garanzie che lo accompagnano devono essere previsti da disposizioni legislative o regolamentari che possiedano le qualità dell'accessibilità, della prevedibilità e della tutela adeguata nei confronti dell'arbitrio;

— tale obbligo e le garanzie che lo accompagnano devono rispettare il contenuto essenziale dei diritti riconosciuti dagli articoli 7 e 8 della Carta dei diritti fondamentali;

— tale obbligo deve essere strettamente necessario alla lotta contro i reati gravi, il che implica che nessun'altra misura o combinazione di misure possa essere altrettanto efficace nella lotta contro i reati gravi pur essendo meno lesiva dei diritti sanciti dalla direttiva 2002/58 e dagli articoli 7 e 8 della Carta dei diritti fondamentali;

— tale obbligo deve essere accompagnato da tutte le garanzie enunciate dalla Corte ai punti da 60 a 68 della sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238) per quanto riguarda l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati, al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla direttiva 2002/58 e degli articoli 7 e 8 della Carta dei diritti fondamentali, e

— tale obbligo deve essere proporzionato, in una società democratica, all'obiettivo della lotta contro i reati gravi, il che implica che i gravi rischi causati da detto obbligo in una società democratica non debbano essere sproporzionati rispetto ai vantaggi che ne derivano nella lotta contro i reati gravi.