COMMISSIONE EUROPEA

Bruxelles, 18.4.2011
COM(2011) 225 definitivo

RELAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE)

RELAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE)

1. INTRODUZIONE

Ai sensi della direttiva sulla conservazione dei dati[1] (di seguito «direttiva»), gli Stati membri devono imporre ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione (di seguito «operatori») l'obbligo di conservare i dati relativi al traffico e all'ubicazione per un periodo compreso tra sei mesi e due anni, a fini di indagine, accertamento e perseguimento di reati gravi.

Conformemente all'articolo 14 della direttiva, la presente relazione della Commissione fornisce una valutazione dell'applicazione della direttiva da parte degli Stati membri e del suo impatto sugli operatori economici e sui consumatori, tenendo conto degli ulteriori sviluppi delle tecnologie della comunicazione elettronica e delle statistiche fornite alla Commissione, allo scopo di determinare se sia necessario modificarne le disposizioni, in particolare per quanto riguarda i dati da conservare e i periodi di conservazione. La presente relazione esamina anche le implicazioni della direttiva per i diritti fondamentali, alla luce delle critiche formulate sulla conservazione dei dati in generale, e valuta se sia necessario adottare misure in risposta alle preoccupazioni associate all'uso delle carte SIM anonime a fini criminali[2].

Nel complesso la valutazione ha dimostrato che la conservazione dei dati è uno strumento prezioso per la giustizia penale e per l'attività di contrasto nell'UE. Il contributo della direttiva all'armonizzazione della conservazione dei dati è stato limitato, segnatamente per quanto riguarda la limitazione delle finalità, i periodi di conservazione e il rimborso delle spese sostenute dagli operatori, aspetto quest'ultimo che esula dal suo campo di applicazione. Considerate le implicazioni e i rischi per il mercato interno e per il diritto al rispetto della vita privata e alla protezione dei dati personali, l'UE dovrebbe continuare a garantire, tramite norme comuni, il mantenimento di standard elevati in materia di immagazzinamento, estrazione e uso dei dati relativi al traffico e all'ubicazione. Tenuto conto di queste conclusioni, la Commissione intende proporre modifiche alla direttiva, sulla base di una valutazione d'impatto.

---

1 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU L 105 del 13.4.2006, pagg. 54-63).

2 Conclusioni del Consiglio sulla lotta contro l'utilizzo delle comunicazioni elettroniche e del loro anonimato a fini criminali, 2908ª sessione del Consiglio «Giustizia e affari interni», Bruxelles, 27-28 novembre 2008.

2. CONTESTO DELLA VALUTAZIONE

La presente relazione di valutazione si basa sulle discussioni approfondite condotte con gli Stati membri, gli esperti e le parti interessate e sui rispettivi contributi.

Nel maggio 2009 la Commissione ha organizzato una conferenza intitolata *«Towards the Evaluation of the Data Retention Directive»*, alla quale hanno partecipato le autorità di protezione dei dati, il settore privato, la società civile e il mondo accademico. Nel settembre 2009 la Commissione ha inviato un questionario alle parti interessate appartenenti a tali gruppi e ha ricevuto circa 70 risposte[3]. La Commissione ha organizzato una seconda conferenza nel dicembre 2010, intitolata *«Taking on the Data Retention Directive»*, alla quale ha partecipato un insieme analogo di parti interessate, per scambiare valutazioni preliminari della direttiva e discutere le sfide future per il settore.

Tra ottobre 2009 e marzo 2010 la Commissione ha incontrato i rappresentanti degli Stati membri e dei paesi associati dello Spazio economico europeo per esaminare in modo più approfondito gli aspetti riguardanti l'applicazione della direttiva. Gli Stati membri hanno cominciato ad applicare la direttiva più tardi del previsto, soprattutto per quanto riguarda i dati relativi a Internet. A causa dei ritardi nel recepimento, soltanto nove Stati membri sono stati in grado di fornire alla Commissione, per il 2008 o 2009, le statistiche complete richieste dall'articolo 10 della direttiva, sebbene nell'insieme diciannove Stati membri abbiano fornito alcune statistiche (cfr. punto 4.7). Nel luglio 2010 la Commissione ha inviato una lettera agli Stati membri chiedendo maggiori informazioni quantitative e qualitative sulla necessità della conservazione dei dati a fini di contrasto. Dieci Stati membri hanno risposto fornendo informazioni su casi specifici in cui i dati si sono rivelati necessari[4].

La presente relazione si avvale dei documenti di sintesi adottati dal 2008, anno della sua istituzione, dalla «Piattaforma per la conservazione di dati elettronici a fini di indagine, accertamento e perseguimento di reati gravi»[5]. La Commissione ha tenuto conto delle relazioni del Gruppo di lavoro «articolo 29»[6], in particolare della relazione sulla seconda azione di controllo dell'applicazione, cioè la valutazione del rispetto delle disposizioni della direttiva relative alla protezione e alla sicurezza dei dati da parte degli Stati membri[7].

---

3 Le risposte sono pubblicate sul sito Internet della Commissione (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm).

4 Belgio, Repubblica ceca, Cipro, Lituania, Ungheria, Paesi Bassi, Polonia, Slovenia, Regno Unito. Anche la Svezia ha comunicato diversi casi di reati gravi specifici per i quali i dati storici relativi al traffico, disponibili nonostante l'assenza di un obbligo di conservazione dei dati, sono stati essenziali per assicurare la condanna.

5 Questo gruppo di esperti è stato istituito dalla decisione della Commissione 2008/324/CE (GU L 111 del 23.4.2008, pagg. 11-14). La Commissione ha mantenuto contatti regolari con il gruppo. I relativi documenti di sintesi sono pubblicati all'indirizzo Internet: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm.

6 Il Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali è stato istituito dall'articolo 29 della direttiva sulla protezione dei dati (direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31).

7 Relazione 01/2010 sulla seconda azione comune di controllo dell'applicazione della legislazione dell'UE: Rispetto a livello nazionale, da parte dei fornitori di servizi di telecomunicazione e di servizi Internet, degli obblighi imposti dalla legislazione nazionale in materia di conservazione dei dati relativi

3. CONSERVAZIONE DEI DATI NELL'UNIONE EUROPEA

3.1. Conservazione dei dati ai fini della giustizia penale e dell'attività di contrasto

Nell'ambito delle loro attività, i fornitori di reti e servizi (di seguito «operatori») trattano dati personali ai fini della trasmissione di una comunicazione, della fatturazione, dei pagamenti di interconnessione, della commercializzazione e della fornitura di altri servizi a valore aggiunto. Tale trattamento riguarda dati che indicano la fonte, la destinazione, la data, l'ora, la durata e il tipo di una comunicazione, nonché le attrezzature di comunicazione degli utenti e, nel caso della telefonia mobile, dati sull'ubicazione delle attrezzature. A norma della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche[8], in linea di principio tali dati relativi al traffico, generati dall'uso dei servizi di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, salvo i casi in cui risultino necessari per la fatturazione, e solo per il periodo necessario a tal fine, o in cui sia stato ottenuto il consenso dell'abbonato o utente. I dati relativi all'ubicazione possono essere trattati soltanto se sono resi anonimi o con il consenso dell'utente interessato, nella misura e per il periodo necessari alla fornitura di un servizio a valore aggiunto.

Prima dell'entrata in vigore della direttiva, fatte salve alcune condizioni specifiche, le autorità nazionali richiedevano agli operatori l'accesso a tali dati al fine, per esempio, di identificare gli abbonati che utilizzavano un indirizzo IP, analizzare comunicazioni e individuare l'ubicazione di un telefono cellulare.

A livello di Unione europea, la conservazione e l'uso di dati a fini di contrasto sono stati affrontati per la prima volta dalla direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. Detta direttiva ha stabilito, per la prima volta, che gli Stati membri possono adottare le disposizioni legislative che considerano necessarie per la salvaguardia della pubblica sicurezza, della difesa o dell'ordine pubblico (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato), e per l'applicazione del diritto penale[9].

Tale disposizione è stata ulteriormente elaborata nella direttiva relativa alla vita privata e alle comunicazioni elettroniche, in forza della quale gli Stati membri possono adottare disposizioni legislative in deroga al principio della riservatezza delle comunicazioni, tra cui, a talune condizioni, la conservazione, l'accesso e il ricorso ai dati a fini di contrasto. L'articolo 15, paragrafo 1, permette agli Stati membri di limitare i diritti e gli obblighi attinenti alla vita privata, anche mediante la conservazione di dati per un periodo di tempo

---

al traffico, sulla base giuridica degli articoli 6 e 9 della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche e della direttiva 2006/24/CE sulla conservazione dei dati che la modifica, WP 172, 13.7.2010 (cfr. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

[8] 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 L 201 del 31.7.2002, pagg. 37-47).

[9] Articolo 14, paragrafo 1, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (GU L 24 del 30.1.1998, pagg. 1-8).

limitato, qualora la misura sia «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».

Il ruolo dei dati conservati nell'ambito della giustizia penale e dell'attività di contrasto è approfondito nella sezione 5.

3.2. Finalità e base giuridica della direttiva sulla conservazione dei dati

In conseguenza delle disposizioni della direttiva 97/66/CE e della direttiva relativa alla vita privata e alle comunicazioni elettroniche, che permettono agli Stati membri di adottare disposizioni legislative in materia di conservazione dei dati, in alcuni Stati membri gli operatori hanno dovuto acquistare attrezzature per la conservazione dei dati e impiegare personale addetto all'estrazione dei dati per conto delle autorità di contrasto, mentre in altri Stati membri non hanno dovuto provvedervi, fatto che ha creato distorsioni sul mercato interno. Inoltre, le tendenze nei modelli commerciali e nelle offerte di servizi, quali la crescita dei servizi di comunicazione elettronica a tariffa forfettaria, prepagati e gratuiti, hanno gradualmente eliminato la necessità degli operatori di conservare i dati relativi al traffico e all'ubicazione a fini di fatturazione, riducendo così la disponibilità di tali dati per la giustizia penale e le attività di contrasto. Gli attentati terroristici di Madrid nel 2004 e di Londra nel 2005 hanno reso ancora più urgenti le discussioni a livello UE sul modo in cui affrontare tali problematiche.

In tale contesto, la direttiva sulla conservazione dei dati ha imposto agli Stati membri di prevedere l'obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, di conservare i dati relativi alle comunicazioni a fini di «indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale», e ha tentato di armonizzare alcune questioni correlate a livello UE.

La direttiva ha modificato l'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche, inserendo un paragrafo in forza del quale l'articolo 15, paragrafo 1, non si applica ai dati conservati in base alla direttiva sulla conservazione dei dati[10]. Gli Stati membri (come indicato al considerando 12 della direttiva) possono quindi continuare a derogare al principio della riservatezza delle comunicazioni. La direttiva (sulla conservazione dei dati) disciplina soltanto la conservazione dei dati ai fini più limitati dell'indagine, dell'accertamento e del perseguimento di reati gravi.

Questo complesso rapporto giuridico tra la direttiva e la direttiva relativa alla vita privata e alle comunicazioni elettroniche, associato all'assenza di una definizione di «reato grave» in

---

[10] L'articolo 11 della direttiva dispone: «All'articolo 15 della direttiva 2002/58/CE è inserito il seguente paragrafo: '1 *bis*. Il paragrafo 1 non si applica ai dati la cui conservazione è specificamente prevista dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, ai fini di cui all'articolo 1, paragrafo 1, di tale direttiva'».

entrambi gli strumenti, rende difficile distinguere, da un lato, le misure adottate dagli Stati membri per attuare gli obblighi in materia di conservazione dei dati previsti dalla direttiva e, dall'altro lato, la prassi più generale di conservazione dei dati negli Stati membri, consentita dall'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche[11]. Questo aspetto è approfondito nella sezione 4.

La direttiva si basa sull'articolo 95 del trattato che istituisce la Comunità europea (sostituito dall'articolo 114 del trattato sul funzionamento dell'Unione europea), relativo all'instaurazione e al funzionamento del mercato interno. Dopo l'adozione della direttiva, la sua base giuridica è stata contestata dinanzi alla Corte di giustizia per il fatto che il suo scopo principale è l'indagine, l'accertamento e il perseguimento di reati gravi. La Corte ha statuito che la direttiva disciplina operazioni che sono indipendenti dall'attuazione di qualsiasi eventuale azione di cooperazione di polizia e giudiziaria in materia penale e che non armonizza né l'accesso ai dati da parte delle autorità nazionali competenti, né il ricorso ai medesimi e il loro scambio fra tali autorità. Ha pertanto concluso che la direttiva ha essenzialmente come oggetto le attività degli operatori nel settore interessato del mercato interno e di conseguenza ne ha confermato la base giuridica[12].

3.3. Conservazione dei dati

La conservazione dei dati è diversa dalla conservazione per ordine giudiziario (il cosiddetto «congelamento rapido»), in base al quale gli operatori sono tenuti a conservare soltanto i dati riguardanti specifici indiziati a partire dalla data dell'ordine. Questo tipo di conservazione dei dati è uno strumento investigativo previsto e utilizzato dagli Stati firmatari della convenzione del Consiglio d'Europa sulla criminalità informatica[13]. Quasi tutti gli Stati firmatari hanno istituito un punto di contatto, il cui ruolo è garantire assistenza immediata nelle indagini o nei procedimenti riguardanti la criminalità informatica. Tuttavia non tutte le parti della convenzione sembrano aver previsto questo tipo di conservazione, e finora non è ancora stata valutata l'efficacia di tale strumento nell'affrontare la criminalità informatica[14]. Di recente è stato messo a punto un tipo di preservazione dei dati, il cosiddetto «congelamento rapido plus», che va al di là della conservazione per ordine giudiziario, in quanto un giudice può autorizzare anche l'accesso ai dati che non sono ancora stati cancellati dagli operatori. Sarebbe inoltre prevista per legge un'esenzione molto limitata dall'obbligo di cancellare, per un breve periodo, alcuni dati relativi alle comunicazioni che di norma non vengono immagazzinati, come ad esempio i dati relativi all'ubicazione, alla connessione a Internet e gli indirizzi IP dinamici, per gli utenti che hanno sottoscritto un abbonamento a tariffa forfettaria e nei casi in cui non sia necessario immagazzinare dati a fini di fatturazione.

I sostenitori della conservazione per ordine giudiziario ritengono che questo strumento comporti una minore ingerenza nella vita privata rispetto alla conservazione dei dati. Tuttavia,

---

11 Il Gruppo di lavoro «articolo 29» si chiede se «l'intento della direttiva [sulla conservazione dei dati] sia quello di derogare all'obbligo generale di cancellare i dati relativi al traffico una volta conclusa la comunicazione elettronica, o di rendere obbligatoria la conservazione di tutti i dati che i fornitori sono già autorizzati a memorizzare ai fini delle loro attività commerciali».

12 Causa C-301/06, *Irlanda/Parlamento europeo e Consiglio dell'Unione europea*, Racc. 2009, pag. I-00593.

13 Articolo 16 della convenzione sulla criminalità informatica (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Fonte: Consiglio d'Europa.

secondo la maggior parte degli Stati membri, qualsiasi modalità di conservazione per ordine giudiziario non può sostituire adeguatamente la conservazione dei dati, in quanto quest'ultima rende disponibili dati storici, mentre la conservazione per ordine giudiziario non garantisce la possibilità di individuare tracce anteriormente all'ordine di conservazione, né consente di condurre indagini quando un soggetto è ignoto o di raccogliere prove, per esempio, sugli spostamenti delle vittime o dei testimoni di reato[15].

4. RECEPIMENTO DELLA DIRETTIVA SULLA CONSERVAZIONE DEI DATI

Gli Stati membri erano tenuti a recepire la direttiva entro il 15 settembre 2007, con la facoltà di differire, fino al 15 marzo 2009, l'attuazione degli obblighi di conservazione concernenti l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet.

L'analisi che segue si basa sulle comunicazioni relative al recepimento trasmesse alla Commissione da venticinque Stati membri, tra cui il Belgio, che ha attuato la direttiva solo in parte[16]. In Austria e in Svezia il progetto di legge è in corso di esame. In questi due Stati membri non è previsto l'obbligo di conservare dati, ma le autorità di contrasto possono richiedere (ed effettivamente lo fanno) e ottenere dagli operatori i dati relativi al traffico eventualmente disponibili. Successivamente alla notifica iniziale del recepimento da parte della Repubblica ceca, della Germania e della Romania, le rispettive corti costituzionali hanno dichiarato incostituzionali le leggi nazionali di attuazione della direttiva[17] e stanno esaminando come procedere al nuovo recepimento.

Nella presente sezione si analizza il modo in cui gli Stati membri hanno attuato le pertinenti disposizioni della direttiva. Si esamina inoltre se gli Stati membri abbiano scelto di rimborsare agli operatori le spese sostenute per conservare e consentire l'estrazione dei dati, aspetto non disciplinato dalle disposizioni della direttiva, e se le sentenze delle corti costituzionali tedesca, romena e ceca siano rilevanti ai fini della direttiva.

4.1. Finalità della conservazione dei dati (articolo 1)

La direttiva impone agli Stati membri di adottare misure allo scopo di garantire la conservazione e la disponibilità dei dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale.

---

15 Ciò è stato riconosciuto anche dalla corte costituzionale tedesca nella sentenza con la quale ha dichiarato incostituzionale la legge tedesca di attuazione della direttiva (cfr. punto 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 del 2 marzo 2010, punto 208).

16 I venticinque Stati membri che hanno notificato alla Commissione il recepimento della direttiva sono: Belgio, Bulgaria, Repubblica ceca, Danimarca, Germania, Grecia, Estonia, Irlanda, Spagna, Francia, Italia, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia e Regno Unito. Il Belgio ha comunicato alla Commissione che il progetto di legge che completa l'attuazione è ancora all'esame del Parlamento.

17 Decisione n. 1258 della corte costituzionale romena, dell'8 ottobre 2009, Gazzetta ufficiale romena n. 789, 23 novembre 2009; sentenza 1 BvR 256/08 del Bundesverfassungsgericht, del 2 marzo 2010; Gazzetta ufficiale del 1° aprile 2011, sentenza della corte costituzionale del 22 marzo sulle disposizioni della sezione 97, paragrafi 3 e 4, della legge n. 127/2005 Coll. sulle comunicazioni elettroniche, che modifica alcune leggi correlate e relative modifiche, e decreto n. 485/2005 Coll. sulla conservazione dei dati e la relativa trasmissione alle autorità competenti.

Tuttavia le finalità della conservazione dei dati e/o dell'accesso ai medesimi indicate nelle legislazioni nazionali continuano a variare nell'UE. Dieci Stati membri (Bulgaria, Estonia, Irlanda, Grecia, Spagna, Lituania, Lussemburgo, Ungheria, Paesi Bassi, Finlandia) hanno definito i «reati gravi» in termini di condanna a un periodo minimo di reclusione, di possibilità di infliggere una pena privativa della libertà o facendo riferimento a un elenco di reati definiti in altre leggi nazionali. Otto Stati membri (Belgio, Danimarca, Francia, Italia, Lettonia, Polonia, Slovacchia, Slovenia) impongono la conservazione dei dati non solo a fini di indagine, accertamento e perseguimento di reati gravi, ma per quanto riguarda tutti i reati e la prevenzione dei reati, oppure per motivi generali di sicurezza nazionale, sicurezza dello Stato e/o sicurezza pubblica. La legislazione di quattro Stati membri (Cipro, Malta, Portogallo, Regno Unito) fa riferimento ai «reati gravi» senza fornirne una definizione. Per i particolari si rimanda alla tabella 1.

Tabella 1: Limitazione delle finalità della conservazione dei dati indicate nelle legislazioni nazionali

Belgio	A fini di indagine e perseguimento dei reati, perseguimento dell'uso improprio del numero di telefono dei servizi di emergenza, indagini relative all'uso improprio intenzionale della rete o servizio di comunicazione elettronica, nonché ai fini delle attività di raccolta di intelligence svolte dai servizi di intelligence e di sicurezza[18].
Bulgaria	A fini di «indagine e accertamento dei reati gravi e dei reati di cui agli articoli 319a-319f del codice penale, nonché di ricerca di persone»[19].
Repubblica ceca	Non recepita.
Danimarca	A fini di indagine e perseguimento di attività criminali[20].
Germania	Non recepita.
Estonia	Vi si può fare ricorso se la raccolta di prove mediante altre procedure è preclusa o particolarmente complicata e se l'oggetto di un procedimento penale è un reato [di primo grado o, un reato di secondo grado commesso intenzionalmente e punibile con una pena detentiva non inferiore a tre anni][21].
Irlanda	Per la prevenzione dei reati gravi [cioè i reati punibili con reclusione non inferiore a cinque anni, o quelli previsti dalla legge di attuazione], la salvaguardia della sicurezza dello Stato e per salvare vite umane.[22]
Grecia	A fini di accertamento dei reati particolarmente gravi[23].
Spagna	A fini di accertamento, indagine e perseguimento dei reati gravi previsti dal codice penale o da leggi penali speciali[24].

18 Articolo 126, paragrafo 1, della legge 13 giugno 2005 sulle comunicazioni elettroniche.
19 Articolo 250a, paragrafo 2, della legge sulle comunicazioni elettroniche (modificata) 2010.
20 Articolo 1 dell'ordinanza relativa alla conservazione dei dati.
21 Sottosezione 110, paragrafo 1, codice di procedura penale.
22 Articolo 6 della legge sulle comunicazioni (conservazione dei dati) 2011.
23 Tali reati sono definiti all'articolo 4 della legge 2225/1994; articolo 1 della legge 3917/2011.
24 Articolo 1, paragrafo1, della legge 25/2007.

Tabella 1: Limitazione delle finalità della conservazione dei dati indicate nelle legislazioni nazionali	
Francia	A fini di accertamento, indagine e perseguimento dei reati, e al solo scopo di fornire alle autorità giudiziarie le informazioni necessarie, nonché per la prevenzione dei reati di terrorismo e la tutela della proprietà intellettuale[25].
Italia	Per finalità di accertamento e repressione dei reati[26].
Cipro	A fini di indagine su reati gravi[27].
Lettonia	Per proteggere la sicurezza dello Stato e la sicurezza pubblica o per agevolare le indagini su reati, l'azione penale e i procedimenti penali[28].
Lituania	A fini di indagine, accertamento e perseguimento di reati gravi e molto gravi, quali definiti nel codice penale nazionale[29].
Lussemburgo	A fini di accertamento, indagine e perseguimento dei reati punibili con una pena detentiva non inferiore, nel massimo, a un anno[30].
Ungheria	Per permettere agli organismi investigativi, al pubblico ministero, ai giudici e alle agenzie responsabili della sicurezza nazionale di svolgere le loro funzioni e consentire alle forze di polizia e all'ufficio fiscale e doganale nazionale di condurre indagini sui reati intenzionali punibili con reclusione non inferiore a due anni[31].
Malta	A fini di indagine, accertamento e perseguimento dei reati gravi[32].
Paesi Bassi	A fini di indagine e perseguimento dei reati gravi per i quali possa essere inflitta una pena privativa della libertà[33].
Austria	Non recepita.
Polonia	Per la prevenzione e l'accertamento dei reati, per la prevenzione e l'accertamento dei reati fiscali, per l'uso da parte dei pubblici ministeri e dei giudici se pertinente con il procedimento giudiziario pendente, per permettere all'agenzia per la sicurezza interna, all'agenzia di intelligence estera, all'ufficio centrale anticorruzione, ai servizi di controspionaggio militare e ai servizi di intelligence militare di svolgere le loro funzioni[34].

25 Le disposizioni che disciplinano il ricorso ai dati conservati per i reati, per la prevenzione degli atti di terrorismo e per la tutela della proprietà intellettuale sono rispettivamente l'articolo L.34-1(II) del CPCE, la legge n. 2006-64 del 23 gennaio 2006 e la legge n. 2009-669 del 12 giugno 2009.

26 Articolo 132, paragrafo 1, del codice in materia di protezione dei dati personali.

27 Articolo 4, paragrafo 1, della legge 183(I)/2007.

28 Articolo 71, paragrafo 1, della legge sulle comunicazioni elettroniche.

29 Articolo 65 della legge X-1835.

30 Articolo 1, paragrafo 1, della legge 24 luglio 2010.

31 A fini generali di conservazione dei dati, articolo 159/A della legge C/2003, modificata dalla legge CLXXIV/2007; a fini di accesso da parte delle forze di polizia, articolo 68 della legge XXXIV/1994; a fini di accesso da parte dell'ufficio fiscale e doganale nazionale, articolo 59 della legge CXXII/2010.

32 Articolo 20, paragrafo 1, del decreto 198/2008.

33 Articolo 126 del codice di procedura penale.

34 Articolo 180a della legge sulle telecomunicazioni del 16 luglio 2004, modificata dall'articolo 1 della legge 24 aprile 2009.

Tabella 1: Limitazione delle finalità della conservazione dei dati indicate nelle legislazioni nazionali	
Portogallo	A fini di indagine, accertamento e perseguimento dei reati gravi[35].
Romania	Non recepita.
Slovenia	Per garantire la sicurezza nazionale, l'ordine costituzionale e la sicurezza, gli interessi politici ed economici dello Stato … e a fini di difesa nazionale[36].
Slovacchia	A fini di prevenzione, indagine, accertamento e perseguimento dei reati[37].
Finlandia	A fini di indagine, accertamento e perseguimento dei reati gravi, come previsto al capitolo 5a, articolo 3, paragrafo 1, della legge sulle misure coercitive[38].
Svezia	Non recepita.
Regno Unito	A fini di indagine, accertamento e perseguimento dei reati gravi[39].

La maggior parte degli Stati membri che hanno recepito la direttiva consente, a norma della rispettiva legislazione, l'accesso e il ricorso ai dati conservati per fini che vanno oltre quelli previsti dalla direttiva stessa, tra cui la prevenzione e il contrasto della criminalità in generale e i rischi per la vita e l'incolumità delle persone. Sebbene ciò sia ammesso ai sensi della direttiva relativa alla vita privata e alle comunicazioni elettroniche, il livello di armonizzazione raggiunto dalla legislazione dell'UE in questo ambito è ancora limitato. Le differenze nelle finalità della conservazione dei dati verosimilmente influiscono sul volume e sulla frequenza delle richieste e quindi sui costi da sostenere per ottemperare agli obblighi imposti dalla direttiva. Questa situazione può inoltre comportare una mancanza di prevedibilità, la quale deve essere garantita da qualsiasi disposizione legislativa che limiti il diritto al rispetto della vita privata[40]. La Commissione valuterà la necessità di una maggiore armonizzazione in questo ambito e le soluzioni per conseguirla[41].

35 Articolo 1 e articolo 3, paragrafo 1, della legge 32/2008.

36 Articolo 170a, paragrafo 1, della legge sulle comunicazioni elettroniche.

37 Articolo 59a, paragrafo 6, della legge sulle comunicazioni elettroniche.

38 Articolo 14a, paragrafo 1, della legge sulle comunicazioni elettroniche.

39 Regolamenti sulla conservazione dei dati (direttiva CE) del 2009 (2009 n. 859).

40 Sentenza della Corte di giustizia del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01 (domande di pronuncia pregiudiziale del Verfassungsgerichtshof e dell'Oberster Gerichtshof): Rechnungshof (C-465/00)/Österreichischer Rundfunk e altri e tra Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) e Österreichischer Rundfunk (tutela delle persone fisiche con riguardo al trattamento dei dati personali – direttiva 95/46/CE – tutela della vita privata – divulgazione di dati sui redditi di dipendenti di enti giuridici soggetti al controllo del Rechnungshof).

41 Al momento dell'adozione della direttiva, la Commissione ha adottato una dichiarazione nella quale propone di prendere in considerazione l'elenco dei reati previsti per il mandato d'arresto europeo (decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri).

4.2. Operatori tenuti a conformarsi alla conservazione dei dati (articolo 1)

La direttiva si applica ai «fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione» (articolo 1, paragrafo 1). Due Stati membri (Finlandia, Regno Unito) non impongono agli operatori di piccole dimensioni l'obbligo di conservare i dati perché, a loro parere, i costi da sostenere per rispettare tale obbligo, a carico sia del fornitore sia dello Stato, sono superiori ai benefici per la giustizia penale e l'attività di contrasto. Quattro Stati membri (Lettonia, Lussemburgo, Paesi Bassi, Polonia) comunicano di avere introdotto disposizioni amministrative alternative. Mentre i grandi operatori presenti in più Stati membri beneficiano di economie di scala in termini di costi, gli operatori più piccoli in alcuni Stati membri tendono a creare imprese comuni oppure «appaltano» l'attività a imprese specializzate in servizi di conservazione e di estrazione dei dati al fine di ridurre i costi. Tale esternalizzazione delle funzioni tecniche lascia impregiudicato l'obbligo dei fornitori di garantire un controllo adeguato delle operazioni di trattamento e l'esistenza delle misure di sicurezza richieste, il che può essere problematico, soprattutto per gli operatori di piccole dimensioni. La Commissione esaminerà le questioni connesse alla sicurezza dei dati e l'impatto sulle piccole e medie imprese, nell'ambito delle soluzioni intese a modificare il quadro giuridico in materia di conservazione dei dati.

4.3. Accesso ai dati: autorità, procedure e condizioni (articolo 4)

Gli Stati membri sono tenuti a «garantire che i dati conservati […] siano trasmessi solo alle autorità nazionali competenti, in casi specifici e conformemente alle normative nazionali». Spetta agli Stati membri definire nella legislazione nazionale «le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della Convenzione europea dei diritti dell'uomo, secondo l'interpretazione della Corte europea dei diritti dell'uomo».

In tutti gli Stati membri le forze di polizia nazionali e, fatta eccezione per gli ordinamenti di *common law* (Irlanda e Regno Unito), i pubblici ministeri possono accedere ai dati conservati. Quattordici Stati membri elencano tra le autorità competenti i servizi di sicurezza o di intelligence o le forze militari, sei Stati membri le autorità fiscali e/o doganali e tre Stati membri le autorità di frontiera. Uno Stato membro consente ad altre autorità pubbliche di consultare i dati, previa autorizzazione per finalità specifiche previste dalla legislazione secondaria. In undici Stati membri è necessaria l'autorizzazione giudiziaria per ogni richiesta di accesso ai dati conservati. In tre Stati membri l'autorizzazione giudiziaria è necessaria nella maggior parte dei casi. Quattro altri Stati membri richiedono l'autorizzazione di un'autorità di alto livello, ma non di un giudice. In due Stati membri l'unica condizione prevista sembra essere la necessità di presentare la richiesta per iscritto.

Tabella 2: Accesso ai dati conservati relativi alle telecomunicazioni

	Autorità nazionali competenti	*Procedure e condizioni*
Belgio	Unità di coordinamento giudiziario, giudici istruttori, pubblico ministero, polizia criminale.	L'accesso deve essere autorizzato da un magistrato o un pubblico ministero. Su richiesta, gli operatori devono fornire in «tempo reale» i dati relativi agli abbonati e i dati sul traffico e sull'ubicazione relativi alle chiamate effettuate nell'ultimo mese. I dati relativi a chiamate anteriori devono essere messi a disposizione il più presto possibile.

Tabella 2: Accesso ai dati conservati relativi alle telecomunicazioni		
	Autorità nazionali competenti	*Procedure e condizioni*
Bulgaria[42]	Direzioni e dipartimenti specifici dell'agenzia statale per la sicurezza nazionale e del ministero dell'Interno, servizio di informazione militare, servizio di polizia militare, ministero della Difesa, agenzia investigativa nazionale; giudici e autorità incaricate delle indagini preliminari, secondo le condizioni prescritte.	L'accesso è possibile soltanto con mandato del presidente di un tribunale regionale.
Repubblica ceca	Non recepita.	
Danimarca[43]	Forze di polizia.	L'accesso richiede l'autorizzazione giudiziaria; il mandato giudiziario è concesso se la domanda soddisfa criteri rigorosi in termini di sospetto, necessità e proporzionalità.
Germania	Non recepita.	
Estonia[44]	Direzione della polizia e delle guardie di frontiera, direzione della polizia di sicurezza e, per gli oggetti e le comunicazioni elettroniche, direzione dell'ente fiscale e doganale.	L'accesso richiede l'autorizzazione di un giudice per le indagini preliminari. Gli operatori devono «fornire [i dati conservati] nei casi urgenti entro dieci ore e in altri casi entro dieci giorni lavorativi [dal ricevimento della richiesta]».
Irlanda[45]	Membri della *Garda Síochána* (polizia) con il grado di *Chief Superintendant* o superiore; ufficiali della *Permanent Defence Force* (forza della difesa permanente) con il grado di colonnello o superiore; funzionari dei *Revenue Commissioners* (amministrazione fiscale) a livello di funzionario principale o superiore.	La richiesta deve essere presentata per iscritto.
Grecia[46]	Autorità giudiziarie, militari o autorità pubbliche di polizia.	L'accesso richiede la decisione di un giudice che dichiari impossibile o estremamente difficile condurre indagini con altri mezzi.
Spagna[47]	Forze di polizia responsabili dell'accertamento, dell'indagine e del perseguimento di reati gravi, centro di intelligence nazionale ed ente delle dogane.	L'accesso ai dati da parte delle autorità nazionali competenti richiede la previa autorizzazione giudiziaria.
Francia[48]	Pubblico ministero, ufficiali di polizia designati e gendarmi.	La polizia deve fornire una motivazione per ogni richiesta di accesso ai dati conservati e ottenere l'autorizzazione dal funzionario del ministero dell'Interno designato dalla *Commission nationale de contrôle des interceptions de sécurité*. Le richieste di accesso sono gestite da un funzionario designato che lavora per

42 Articolo 250b, paragrafo 1, della legge sulle comunicazioni elettroniche (modificata) 2010 (autorità); articolo 250b, paragrafo 2, articolo 250c, paragrafo 1, della legge sulle comunicazioni elettroniche (modificata) 2010 (accesso).

43 Capitolo 71 della legge sull'amministrazione della giustizia.

44 Sottosezione 112, paragrafi 2 e 3, del codice di procedura penale (autorità e procedura); sottosezione 111, paragrafo 9, (condizioni) della legge sulle comunicazioni elettroniche.

45 Articolo 6 della legge sulle comunicazioni (conservazione dei dati) 2009.

46 Articoli 3 e 4 della legge 2225/94.

47 Articoli 6-7 della legge 25/2007.

Tabella 2: Accesso ai dati conservati relativi alle telecomunicazioni		
	Autorità nazionali competenti	*Procedure e condizioni*
		l'operatore.
Italia[49]	Pubblico ministero; forze di polizia; difensore dell'imputato o della persona sottoposta alle indagini.	L'accesso richiede un «decreto motivato» del pubblico ministero.
Cipro[50]	Giudici, pubblico ministero, forze di polizia.	L'accesso deve essere approvato da un pubblico ministero, qualora ritenga che possa fornire prove di un reato grave. Un giudice può emettere tale mandato se sussiste un ragionevole sospetto di reato grave e se è probabile che i dati siano associati allo stesso.
Lettonia[51]	Funzionari autorizzati delle istituzioni responsabili delle indagini preliminari; persone che svolgono attività investigative; funzionari autorizzati delle istituzioni responsabili della sicurezza dello Stato, ufficio del pubblico ministero; giudici.	I funzionari autorizzati, l'ufficio del pubblico ministero e i giudici sono tenuti a valutare «l'adeguatezza e la pertinenza» della richiesta, registrarla e garantire la protezione dei dati personali ottenuti. Gli organismi autorizzati possono concludere un accordo con un operatore, per es. per la cifratura dei dati forniti.
Lituania[52]	Organismi incaricati delle indagini preliminari, pubblico ministero, giudici e funzionari di intelligence.	Le autorità pubbliche autorizzate devono richiedere i dati per iscritto. Per l'accesso a fini di indagini preliminari è necessario un mandato giudiziario.
Lussemburgo[53]	Autorità giudiziarie (giudici istruttori, pubblico ministero), autorità responsabili della salvaguardia della sicurezza dello Stato, della difesa, della sicurezza pubblica e della prevenzione, indagine, accertamento e perseguimento dei reati.	L'accesso richiede l'autorizzazione giudiziaria.
Ungheria[54]	Forze di polizia, ufficio fiscale e doganale nazionale, servizi responsabili della sicurezza nazionale, pubblico ministero, giudici.	Le forze di polizia e l'ufficio fiscale e doganale nazionale devono ottenere l'autorizzazione del pubblico ministero. Il pubblico ministero e le agenzie responsabili della sicurezza nazionale possono consultare i dati senza mandato giudiziario.
Malta[55]	Polizia nazionale; servizio di sicurezza.	La richiesta deve essere presentata per iscritto.
Paesi Bassi[56]	Ufficiali della polizia investigativa.	L'accesso è possibile con mandato di un pubblico ministero o di un giudice istruttore.
Austria	Non recepita.	
Polonia[57]	Forze di polizia, guardie di frontiera, ispettori fiscali, agenzia per la sicurezza	Le richieste devono essere presentate per iscritto e, nel caso della polizia, delle guardie

48 Articoli 60-1 e 60-2 del codice di procedura penale (autorità); articolo L.31-1-1 (condizioni).

49 Articolo 132, paragrafo 3, del codice in materia di protezione dei dati personali.

50 Articolo 4, paragrafi 2 e 4, della legge 183(I)/2007.

51 Articolo 71, paragrafo 1, della legge sulle comunicazioni elettroniche (autorità); regolamento del governo n. 820 (procedure).

52 Articolo 77, paragrafi 1 e 2, della legge X-1835; relazione verbale alla Commissione.

53 Articolo 5-2, paragrafo 1, e articolo 9, paragrafo 2, della legge 24 luglio 2010 (autorità); articolo 67-1 del codice di istruzione penale (condizioni).

54 Articolo 68, paragrato 1, e articolo 69, paragrafo 1, lettere c) e d), della legge XXXIV 1994; articolo 9/A, paragrafo 1, della legge V 1972; articoli 71, paragrafi 1, 3 e 4, 178/A, paragrafo 4, 200, 201, 268, paragrafo 2, della legge XIX 1998; articoli 40, paragrafi 1 e 2, 53, paragrafo 1, 54, paragrafo 1, lettera j), della legge CXXV 1995.

55 Articolo 20, paragrafi 1 e 3, del decreto 198/2008.

56 Articolo 126ni del codice di procedura penale.

Tabella 2: Accesso ai dati conservati relativi alle telecomunicazioni		
	Autorità nazionali competenti	*Procedure e condizioni*
	interna, agenzia di intelligence estera, ufficio centrale anticorruzione, servizi di controspionaggio militare, servizi di intelligence militare, giudici e pubblico ministero.	di frontiera, degli ispettori fiscali, devono essere autorizzate dal funzionario di alto livello dell'organizzazione.
Portogallo[58]	Polizia giudiziaria, guardia repubblicana nazionale, ufficio per la sicurezza pubblica, polizia giudiziaria militare, servizio immigrazione e frontiere, polizia marittima.	La trasmissione dei dati richiede l'autorizzazione giudiziaria fondata sul motivo che l'accesso è indispensabile per accertare la verità o che il reperimento di prove sarebbe impossibile o molto difficile in qualsiasi altro modo. L'autorizzazione giudiziaria è concessa in base ai criteri di necessità e proporzionalità.
Romania	Non recepita.	
Slovenia[59]	Forze di polizia, agenzie di intelligence e di sicurezza, agenzie della difesa responsabili delle attività di intelligence e controspionaggio e delle missioni di sicurezza.	L'accesso richiede l'autorizzazione giudiziaria.
Slovacchia[60]	Autorità di contrasto, giudici.	La richiesta deve essere presentata per iscritto.
Finlandia[61]	Forze di polizia, guardie di frontiera, autorità doganali (per i dati conservati relativi agli abbonati, al traffico e all'ubicazione). Centro di pronto intervento, operazioni di soccorso marittimo, centro secondario di soccorso marittimo (per i dati relativi all'identificazione e all'ubicazione in situazioni di emergenza).	Tutte le autorità competenti possono accedere ai dati relativi agli abbonati senza autorizzazione giudiziaria. Per gli altri dati è necessario un mandato giudiziario.
Svezia	Non recepita.	
Regno Unito[62]	Forze di polizia, servizi di intelligence, autorità fiscali e doganali, altre autorità pubbliche designate nella legislazione secondaria.	L'accesso è permesso, con l'autorizzazione di una «persona designata» e se sono soddisfatti i criteri di necessità e proporzionalità, in casi specifici e nelle circostanze in cui la comunicazione dei dati è permessa o imposta dalla legge. Sono state definite procedure specifiche con gli operatori.

Per quanto riguarda le autorità che hanno accesso ai dati conservati e le procedure per ottenere l'accesso, la Commissione valuterà la necessità di una maggiore armonizzazione e le soluzioni per conseguirla. Si potrebbero prevedere, tra l'altro, elenchi più precisi delle autorità competenti, il controllo indipendente e/o giurisdizionale delle richieste di dati e norme

---

57 Articolo 179, paragrafo 3, della legge sulle telecomunicazioni del 16 luglio 2004, modificata dall'articolo 1 della legge 24 aprile 2009.

58 Articoli 2, paragrafo 1, 3, paragrafo 2, e 9 della legge 32/2008.

59 Articolo 107c della legge sulle comunicazioni elettroniche; articolo 149b del codice di procedura penale; articolo 24, lettera b), della legge sull'intelligence e la sicurezza; articolo 32 della legge sulla difesa.

60 Articolo 59a, paragrafo 8, della legge sulle comunicazioni elettroniche.

61 Articoli 35, paragrafo 1, e 36 della legge sulle comunicazioni elettroniche; articoli 31-33 della legge sulle forze di polizia; articolo 41 della legge sulle guardie di confine.

62 Articolo 25, tabella 1, della legge che disciplina i poteri di indagine (RIPA) del 2000; articolo 7 del regolamento sulla conservazione dei dati. L'articolo 22, paragrafo 2, della RIPA stabilisce le finalità per le quali tali autorità possono acquisire i dati.

minime procedurali per consentire alle autorità competenti l'acceso ai dati conservati dagli operatori.

4.4. Campo d'applicazione della conservazione dei dati e categorie di dati da conservare (articolo 1, paragrafo 2, articolo 3, paragrafo 2, e articolo 5)

La direttiva si applica ai settori della telefonia di rete fissa, della telefonia mobile, dell'accesso Internet, della posta elettronica su Internet e della telefonia via Internet. Essa specifica (all'articolo 5) le categorie di dati da conservare, cioè i dati necessari per identificare:

(a) la fonte di una comunicazione;

(b) la destinazione di una comunicazione;

(c) la data, l'ora e la durata di una comunicazione;

(d) il tipo di comunicazione;

(e) le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature;

(f) l'ubicazione delle apparecchiature di comunicazione mobile.

Comprende inoltre (articolo 3, paragrafo 2) i tentativi di chiamata non riusciti, cioè le chiamate telefoniche che sono state collegate con successo ma non hanno ottenuto risposta, oppure in cui vi è stato un intervento del gestore della rete, ove i dati relativi a tali tentativi siano generati o trattati e immagazzinati oppure trasmessi dagli operatori. A norma della direttiva non può essere conservato alcun dato relativo al contenuto della comunicazione. Successivamente è stato anche chiarito che le *query* di ricerca, cioè i *log server* generati dall'offerta di un servizio di ricerca, non rientrano nel campo di applicazione della direttiva, in quanto sono considerate come contenuto piuttosto che come dati relativi al traffico[63].

Ventuno Stati membri prevedono la conservazione di ciascuna delle suddette categorie di dati nella legge di attuazione. Il Belgio non ha stabilito i tipi di dati di telefonia da conservare, né ha previsto disposizioni per i dati relativi a Internet. Gli Stati membri che hanno risposto al questionario della Commissione non ritengono necessario modificare le categorie di dati da conservare, sebbene il Parlamento europeo abbia trasmesso alla Commissione una dichiarazione scritta nella quale chiede di estendere la direttiva ai motori di ricerca «per contrastare in maniera rapida ed efficace la pedopornografia e le molestie sessuali online»[64]. Nella sua relazione sulla seconda azione di controllo dell'applicazione, il Gruppo di lavoro «articolo 29» ha affermato che le categorie previste dalla direttiva dovrebbero essere considerate esaustive e che non dovrebbero essere imposti agli operatori ulteriori obblighi di conservazione di dati. La Commissione valuterà la necessità di tutte queste categorie di dati.

---

63 Parere del Gruppo di lavoro «articolo 29» sugli aspetti della protezione dei dati connessi ai motori di ricerca, 4 aprile 2008.

64 Dichiarazione scritta presentata il 19.4.2010 a norma dell'articolo 123 del regolamento sulla creazione di un sistema di allerta rapida europeo (S.EA.R.) contro pedofili e molestatori sessuali (0029/2010).

4.5. Periodi di conservazione (articolo 6 e articolo 12)

Gli Stati membri sono tenuti a garantire che le categorie di dati di cui all'articolo 5 siano conservate per periodi non inferiori a sei mesi e non superiori a due anni. Il periodo massimo di conservazione può essere prolungato da uno Stato membro che «si trovi ad affrontare circostanze particolari che giustificano una proroga per un periodo limitato»; tale proroga deve essere notificata alla Commissione, la quale decide, entro sei mesi dalla notifica, se approvarla o respingerla. Mentre il periodo massimo di conservazione può essere prolungato, non esistono disposizioni che consentano di ridurre la conservazione a meno di sei mesi. Tutti gli Stati membri che hanno recepito la direttiva, tranne uno, applicano un periodo o periodi di conservazione compresi entro tali limiti e non hanno notificato proroghe alla Commissione. Tuttavia non è stato adottato un approccio coerente a livello UE.

Quindici Stati membri specificano un solo periodo per tutte le categorie di dati: uno Stato membro (Polonia) indica un periodo di conservazione di due anni, uno indica 1,5 anni (Lettonia), dieci indicano un anno (Bulgaria, Danimarca, Estonia, Grecia, Spagna, Francia, Paesi Bassi, Portogallo, Finlandia, Regno Unito) e tre indicano sei mesi (Cipro, Lussemburgo, Lituania). Cinque Stati membri hanno definito periodi di conservazione diversi per le varie categorie di dati: due Stati membri (Irlanda, Italia) indicano due anni per i dati relativi alla telefonia fissa e mobile e 1 anno per i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet; uno Stato membro (Slovenia) indica 14 mesi per i dati relativi alla telefonia e otto mesi per i dati relativi a Internet; uno Stato membro (Slovacchia) indica un anno per la telefonia fissa e mobile e sei mesi per i dati relativi a Internet; uno Stato membro (Malta) indica un anno per i dati relativi alla telefonia fissa, mobile e via Internet e sei mesi per l'accesso Internet e la posta elettronica su Internet. Uno Stato membro (Ungheria) conserva tutti i dati per un anno, eccetto i dati sui tentativi di chiamata non riusciti, che sono conservati per sei mesi. Uno Stato membro (Belgio) non ha previsto un periodo di conservazione specifico per le categorie di dati stabilite dalla direttiva. Per i particolari si rimanda alla tabella 3.

Tabella 3: Periodi di conservazione previsti dalla legislazione nazionale	
Belgio[65]	Tra 1 anno e 36 mesi per i servizi telefonici «accessibili al pubblico». Non sono previste disposizioni per i dati relativi a Internet.
Bulgaria	1 anno. Su richiesta, i dati che sono stati consultati possono essere conservati per un ulteriore periodo di 6 mesi.
Repubblica ceca	Non recepita.
Danimarca	1 anno.
Germania	Non recepita.
Estonia	1 anno.
Irlanda	2 anni per i dati relativi alla telefonia fissa e mobile, 1 anno per i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet.
Grecia	1 anno.
Spagna	1 anno.
Francia	1 anno.
Italia	2 anni per i dati relativi alla telefonia fissa e mobile, 1 anno per i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet.

[65] Articolo 126, paragrafo 2, della legge 13 giugno 2005 concernente le comunicazioni elettroniche.

Tabella 3: Periodi di conservazione previsti dalla legislazione nazionale	
Cipro	6 mesi.
Lettonia	18 mesi.
Lituania	6 mesi.
Lussemburgo	6 mesi.
Ungheria	6 mesi per i tentativi di chiamata non riusciti e 1 anno per tutti gli altri dati.
Malta	1 anno per i dati relativi alla telefonia fissa, mobile e via Internet, 6 mesi per i dati relativi all'accesso Internet e alla posta elettronica su Internet.
Paesi Bassi	1 anno.
Austria	Non recepita.
Polonia	2 anni.
Portogallo	1 anno.
Romania	Non recepita (6 mesi a norma della precedente legge di attuazione, poi dichiarata incostituzionale).
Slovenia	14 mesi per i dati relativi alla telefonia e 8 mesi per i dati relativi a Internet.
Slovacchia	1 anno per i dati relativi alla telefonia fissa e mobile, 6 mesi per i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet.
Finlandia	1 anno.
Svezia	Non recepita.
Regno Unito	1 anno.

Questa diversità di approccio è permessa dalla direttiva, ma è inevitabile che lo strumento non garantisca la piena certezza del diritto e la prevedibilità in tutta l'UE per gli operatori attivi in più di uno Stato membro e per i cittadini i cui dati sulle comunicazioni possono essere conservati in Stati membri diversi. Tenendo conto della crescente internazionalizzazione del trattamento dei dati e dell'esternalizzazione dell'immagazzinamento dei dati, si dovrebbe esaminare la possibilità di conseguire una maggiore armonizzazione dei periodi di conservazione a livello UE. Al fine di rispettare il principio di proporzionalità, e alla luce delle informazioni quantitative e qualitative sull'utilità dei dati conservati negli Stati membri, nonché delle tendenze in atto, da un lato, nelle comunicazioni e nelle tecnologie e, dall'altro, nella criminalità e nel terrorismo, la Commissione valuterà se applicare periodi diversi per le varie categorie di dati, per le varie categorie di reati gravi, o una combinazione delle due soluzioni[66]. Le informazioni quantitative fornite finora dagli Stati membri riguardo all'età dei dati conservati indicano che, al momento della richiesta (iniziale) di accesso da parte delle autorità di contrasto, circa il 90% dei dati è conservato da sei mesi o meno e circa il 70% da tre mesi o meno (cfr. punto 5.2).

4.6. Protezione e sicurezza dei dati e autorità di controllo (articoli 7 e 9)

La direttiva impone agli Stati membri di provvedere a che gli operatori rispettino, come minimo, quattro principi di sicurezza dei dati, cioè che i dati conservati siano:

(a) della stessa qualità e soggetti alla stessa sicurezza e tutela dei dati in rete [pubblica di comunicazione];

[66] La proposta di direttiva sulla conservazione dei dati, presentata dalla Commissione nel 2005, prevedeva un periodo di conservazione di un anno per i dati relativi alla telefonia e di sei mesi per i dati relativi a Internet.

(b) soggetti ad adeguate misure tecniche e organizzative intese a tutelarli da una distruzione accidentale o illecita, da un'alterazione o perdita accidentale, da immagazzinamento, trattamento, accesso o divulgazione non autorizzati o illeciti;

(c) soggetti ad adeguate misure tecniche e organizzative intese a garantire che gli stessi possono essere consultati soltanto da persone appositamente autorizzate; e

(d) distrutti alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati [ai fini previsti dalla direttiva].

Conformemente alla direttiva sulla protezione dei dati e alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, gli operatori non possono trattare i dati conservati a norma della direttiva per scopi diversi da quelli per cui sono stati raccolti, purché i dati non siano stati conservati per altri fini[67]. Gli Stati membri devono designare un'autorità pubblica responsabile di esercitare, «in totale indipendenza», il controllo dell'applicazione dei suddetti principi. Tale autorità può essere la stessa autorità prevista dalla direttiva sulla protezione dei dati[68].

Quindici Stati membri hanno recepito tutti e quattro i principi nella rispettiva legislazione. Quattro Stati membri (Belgio, Estonia, Spagna, Lettonia) hanno recepito due o tre di tali principi, ma non prevedono espressamente la distruzione dei dati alla fine del periodo di conservazione. Due Stati membri (Italia, Finlandia) prevedono la distruzione dei dati. Non è chiaro quali misure di sicurezza tecniche e organizzative specifiche siano state adottate, per esempio l'autenticazione forte o la gestione dettagliata delle informazioni relative all'accesso[69]. Ventidue Stati membri hanno designato un'autorità di controllo responsabile di vigilare sull'applicazione dei principi. Nella maggior parte dei casi l'autorità di controllo è l'autorità di protezione dei dati. Per i particolari si rimanda alla tabella 4.

Tabella 4: Protezione e sicurezza dei dati e autorità di controllo

Stato membro	*Disposizioni in materia di protezione e sicurezza dei dati previste dalla legislazione nazionale*	*Autorità di controllo*
Belgio	Gli operatori sono tenuti a garantire che la trasmissione dei dati non possa essere intercettata da terzi e a rispettare le norme ETSI in materia di sicurezza e legittima intercettazione delle telecomunicazioni[70]. Il principio della distruzione obbligatoria dei dati alla fine del periodo di conservazione non sembra essere previsto.	Istituto per i servizi postali e le telecomunicazioni.

67 Direttiva 95/46/CE, articolo 13, paragrafo 1.

68 Direttiva 95/46/CE, articolo 28.

69 L'autenticazione forte si basa su due diversi meccanismi di autenticazione, per esempio una *password* associata a dati biometrici oppure una *password* associata a un *token*, intesi a garantire la presenza fisica della persona incaricata del trattamento dei dati relativi al traffico. La gestione dettagliata delle informazioni relative all'accesso consiste nel tracciamento preciso delle operazioni di accesso e di trattamento dei dati mediante la conservazione di informazioni che registrano l'identificativo dell'utente, l'ora di accesso e i dati consultati.

70 Articolo 6, decreto reale 9 gennaio 2003.

Tabella 4: Protezione e sicurezza dei dati e autorità di controllo		
Stato membro	*Disposizioni in materia di protezione e sicurezza dei dati previste dalla legislazione nazionale*	*Autorità di controllo*
Bulgaria	La legge di attuazione prescrive l'obbligo di attuare i quattro principi[71].	La commissione per la protezione dei dati personali controlla il trattamento e l'immagazzinamento dei dati per garantire il rispetto degli obblighi; la commissione parlamentare in seno all'Assemblea nazionale controlla le procedure di autorizzazione e accesso ai dati.
Repubblica ceca[72]	Non recepita.	
Danimarca	Sono previsti i quattro principi[73].	L'agenzia nazionale per le tecnologie informatiche e le telecomunicazioni controlla che i fornitori di reti e servizi di comunicazione elettronica rispettino l'obbligo di assicurare che i sistemi e le attrezzature tecniche consentano alle forze di polizia di accedere alle informazioni relative al traffico.
Germania	Non recepita.	
Estonia	La legge di attuazione prevede tre dei quattro principi. Non esiste una disposizione specifica sul quarto principio, ma chiunque abbia subito una violazione del diritto al rispetto della vita privata a causa di attività di sorveglianza può richiedere la distruzione dei dati, previa sentenza di un tribunale[74].	Autorità di vigilanza tecnica.
Irlanda[75]	La legge di attuazione prevede l'obbligo di attuare i quattro principi.	Il giudice designato ha la facoltà di verificare e riferire se le autorità nazionali competenti rispettano le disposizioni della legge di attuazione.
Grecia[76]	La legge di attuazione prescrive l'obbligo di attuare i quattro principi e impone inoltre agli operatori l'obbligo di preparare e applicare un programma inteso a garantirne il rispetto, sotto la responsabilità di un garante designato per la sicurezza dei dati.	Autorità di protezione dei dati personali e autorità garante della riservatezza delle comunicazioni.
Spagna[77]	Le disposizioni in materia di sicurezza dei dati prevedono tre dei quattro principi (qualità e sicurezza dei dati conservati, accesso da parte di persone autorizzate e tutela contro il trattamento non autorizzato).	Agenzia per la protezione dei dati.

71 Articolo 4, paragrafo 1, della legge sulle comunicazioni elettroniche (modificata) del 2010.

72 Sezioni 87, paragrafo 3, e 88 della legge 127/2005, modificata dalla legge 247/2008; Sezione 2 della legge 336/2005; sezione 3, paragrafo 4, della legge 485/2005; sezione 28, paragrafo 1, della legge 101/2000.

73 Legge sul trattamento dei dati personali; ordinanza esecutiva n. 714, del 26 giugno 2008, sulla fornitura di reti e servizi di comunicazione elettronica.

74 Sottosezione 111, paragrafo 9, della legge sulle comunicazioni elettroniche; sottosezione 122, paragrafo 2, del codice di procedura penale.

75 Sezioni 4, 11 e 12 della legge sulle comunicazioni (conservazione dei dati) del 2009.

76 Articolo 6 della legge 3917/2011.

Tabella 4: Protezione e sicurezza dei dati e autorità di controllo		
Stato membro	*Disposizioni in materia di protezione e sicurezza dei dati previste dalla legislazione nazionale*	*Autorità di controllo*
Francia[78]	La legge di attuazione comprende l'obbligo di attuare i quattro principi.	La commissione nazionale per le tecnologie informatiche e la libertà controlla il rispetto degli obblighi.
Italia	Non sono previste disposizioni specifiche in materia di sicurezza dei dati conservati, ma vige un obbligo generale di cancellare o rendere anonimi i dati relativi al traffico e di trattare i dati relativi all'ubicazione solo previo consenso dell'interessato[79].	Il garante per la protezione dei dati controlla il rispetto della direttiva da parte degli operatori.
Cipro[80]	La legge di attuazione prevede ciascuno dei quattro principi.	Il commissario per la protezione dei dati personali controlla l'applicazione della legge di attuazione.
Lettonia[81]	La legge di attuazione prevede due principi: riservatezza dei dati e accesso autorizzato agli stessi e distruzione dei dati alla fine del periodo di conservazione.	L'ispettorato statale per i dati controlla la protezione dei dati personali nel settore delle comunicazioni elettroniche, ma non l'accesso ai dati conservati e il relativo trattamento.
Lituania[82]	La legge di attuazione prevede i quattro principi.	L'ispettorato statale per la protezione dei dati controlla l'applicazione della legge di attuazione ed è responsabile della comunicazione delle statistiche alla Commissione europea.
Lussemburgo[83]	La legge di attuazione prevede i quattro principi.	Autorità di protezione dei dati.
Ungheria[84]	La legge di attuazione prevede i quattro principi.	Commissario parlamentare per la protezione dei dati e la libertà dell'informazione.
Malta[85]	La legge di attuazione prevede i quattro principi.	Commissario per la protezione dei dati.
Paesi Bassi[86]	La legge di attuazione prevede i quattro principi.	L'agenzia per le radiocomunicazioni controlla il rispetto degli obblighi imposti ai fornitori di servizi di accesso Internet e telecomunicazione; l'autorità di protezione dei dati controlla il trattamento generale dei dati personali; un protocollo specifica le modalità di cooperazione tra le due autorità.
Austria	Non recepita.	

77 Articolo 8 della legge 25/2007, articolo 38, paragrafo 3, della legge generale sulle telecomunicazioni. La legge (articolo 9) fa riferimento all'eccezione ai diritti di accesso e cancellazione prescritti dalla legge organica 15/1999 sulla protezione dei dati personali (articoli 22 e 23).

78 Articolo D.98-5 del CPCE; articolo L-34-1(V) del CPCE; articolo 34 della legge n. 78-17; articolo 34-1 del CPCE; articolo 11 della legge n. 78-17 del 6 gennaio 1978.

79 Articoli 123 e 126 del codice in materia di protezione dei dati personali.

80 Articoli 14 e 15 della legge 183(I)/2007.

81 Articolo 4, paragrafo 4, e articolo 71, paragrafi 6-8, della legge sulle comunicazioni elettroniche.

82 Articolo 12, paragrafo 5, e articolo 66, paragrafi 8 e 9, della legge sulle comunicazioni elettroniche, modificata il 14 novembre 2009.

83 Articolo 1, paragrafo 5, della legge 24 luglio 2010.

84 Articolo 157 della legge C/2003, modificata dalla legge CLXXIV/2007; articolo 2 del decreto 226/2003; e legge LXIII/1992 sulla protezione dei dati.

85 Articoli 24 e 25 del decreto 198/2008; articolo 40, lettera b), della legge sulla protezione dei dati (Cap. 440).

86 Articolo 13, paragrafo 5, della legge sulle telecomunicazioni; il lungo titolo del protocollo relativo alla cooperazione è: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens*.

Tabella 4: Protezione e sicurezza dei dati e autorità di controllo		
Stato membro	*Disposizioni in materia di protezione e sicurezza dei dati previste dalla legislazione nazionale*	*Autorità di controllo*
Polonia	La legge di attuazione prevede i quattro principi [87].	Autorità di protezione dei dati.
Portogallo	La legge di attuazione prevede i quattro principi [88].	Autorità portoghese di protezione dei dati.
Romania	Non recepita.	
Slovenia[89]	La legge di attuazione prevede i quattro principi.	Commissario per l'informazione.
Slovacchia[90]	La legge di attuazione prevede i quattro principi.	L'autorità nazionale di regolamentazione e determinazione dei prezzi nel settore delle comunicazioni elettroniche controlla la protezione dei dati personali.
Finlandia	La legge di attuazione prevede espressamente soltanto l'obbligo di distruggere i dati alla fine del periodo di conservazione [91].	L'autorità nazionale di regolamentazione delle comunicazioni controlla il rispetto delle norme in materia di conservazione dei dati da parte degli operatori. Il mediatore per la protezione dei dati controlla la legittimità generale del trattamento dei dati personali.
Svezia	Non recepita.	
Regno Unito	La legge di attuazione prevede i quattro principi [92].	L'*Information Commissioner* vigila sulla conservazione e/o sul trattamento dei dati relativi alle comunicazioni (e di qualsiasi altro dato personale) e sugli opportuni controlli concernenti la protezione dei dati. L'*Interception Commissioner* (un giudice incaricato o in quiescenza) vigila sull'acquisizione di dati relativi alle comunicazioni a norma della RIPA da parte delle autorità pubbliche. L'*Investigatory Powers Tribunal* indaga sulle denunce relative all'uso improprio dei dati acquisiti a norma della legge di attuazione (RIPA).

L'articolo 7 non è stato recepito in modo omogeneo. I dati conservati possono essere di natura estremamente personale e sensibile ed è necessario applicare, in modo coerente e visibile, criteri rigorosi di protezione e sicurezza dei dati durante l'intero processo, per l'immagazzinamento, l'estrazione e l'uso dei dati, al fine di ridurre al minimo il rischio di violazioni del diritto al rispetto della vita privata e preservare la fiducia dei cittadini. La Commissione esaminerà la possibilità di rafforzare le norme in materia di sicurezza e protezione dei dati, compresa l'introduzione di soluzioni basate sul principio della «*privacy by design*» (protezione della vita privata fin dalla progettazione), per assicurare che tali norme siano rispettate nell'ambito sia dell'immagazzinamento sia della trasmissione dei dati. Terrà altresì conto delle raccomandazioni riguardanti le salvaguardie minime e le misure di

87 Articoli 180a e 180e della legge sulle telecomunicazioni.

88 Articolo 7, paragrafi 1 e 5, e articolo 11 della legge 32/2008; articoli 53 e 54 della legge sulla protezione dei dati personali.

89 Articolo 107a, paragrafo 6, e articolo 107c della legge sulle comunicazioni elettroniche.

90 Articolo 59a della legge sulle comunicazioni elettroniche; articolo S33 della legge n. 428/2002 sulla protezione dei dati personali.

91 Articolo 16, paragrafo 3, della legge sulle comunicazioni elettroniche.

92 Articolo 6 del regolamento sulla protezione dei dati.

sicurezza di natura tecnica e organizzativa formulate dal Gruppo di lavoro «articolo 29» nella relazione sulla seconda azione di controllo dell'applicazione[93].

4.7. Statistiche (Articolo 10)

Gli Stati membri sono tenuti a fornire annualmente alla Commissione statistiche sulla conservazione dei dati, riguardanti:

– i casi in cui sono state trasmesse informazioni alle autorità competenti conformemente alla legislazione nazionale applicabile;

– il tempo trascorso fra la data in cui le informazioni sono state conservate e la data in cui le autorità competenti ne hanno richiesto la trasmissione (cioè l'età dei dati);

– i casi in cui non è stato possibile soddisfare le richieste di dati.

Nel richiedere statistiche a norma di detta disposizione, la Commissione ha chiesto agli Stati membri di fornire informazioni dettagliate sui casi di «richieste» individuali di dati. Tuttavia le statistiche fornite presentano differenze in termini di ampiezza e di dettaglio: alcuni Stati membri nelle loro risposte distinguono i diversi tipi di comunicazioni, alcuni indicano l'età dei dati al momento della richiesta, altri invece forniscono soltanto statistiche annuali senza ripartizioni dettagliate. Diciannove Stati membri[94] hanno fornito statistiche sul numero di richieste di dati per il 2009 e/o il 2008, tra cui l'Irlanda, la Grecia e l'Austria, dove i dati sono richiesti nonostante l'assenza all'epoca di una legge di attuazione, e la Repubblica ceca e la Germania, le cui leggi in materia di conservazione dei dati sono state dichiarate incostituzionali. Sette Stati membri che hanno recepito la direttiva non hanno fornito statistiche, sebbene il Belgio abbia fornito una stima del volume di richieste annue di dati relativi alla telefonia (300 000).

È indispensabile disporre di dati quantitativi e qualitativi attendibili per dimostrare la necessità e l'utilità di misure di sicurezza quali la conservazione di dati. Ciò è stato riconosciuto nel piano d'azione del 2006 per la misurazione della criminalità e della giustizia penale[95], che prevedeva l'elaborazione di una metodologia per la regolare raccolta dei dati in linea con la direttiva e l'inclusione delle statistiche nella banca dati dell'Eurostat (purché soddisfino i criteri di qualità). Non è stato possibile realizzare tale obiettivo, in quanto la maggior parte degli Stati membri ha dato piena attuazione alla direttiva soltanto negli ultimi due anni e ha adottato interpretazioni diverse per la fonte delle statistiche. Nell'ambito della futura proposta di revisione del quadro giuridico in materia di conservazione dei dati, parallelamente alla revisione del piano d'azione sulle statistiche, la Commissione intende elaborare procedure di quantificazione e di notifica che permettano un controllo trasparente e significativo della conservazione dei dati, senza imporre oneri eccessivi a carico del sistema giudiziario penale e delle autorità di contrasto.

---

93 Parere 3/2006 del Gruppo di lavoro «articolo 29» per la protezione dei dati personali (WP 119); relazione 01/2010.

94 Repubblica ceca, Danimarca, Germania, Estonia, Irlanda, Grecia, Spagna, Francia, Cipro, Lettonia, Lituania, Malta, Paesi Bassi, Austria, Polonia, Slovenia, Slovacchia, Finlandia, Regno Unito.

95 Comunicazione della Commissione «Elaborazione di una coerente strategia globale per la misurazione della criminalità e della giustizia penale: piano d'azione dell'UE per il 2006-2010» (COM (2006) 437).

4.8. Recepimento nei paesi del SEE

La legislazione in materia di conservazione dei dati è in vigore in Islanda, Liechtenstein e Norvegia[96].

4.9. Decisioni delle corti costituzionali concernenti le leggi di attuazione

La corte costituzionale romena nell'ottobre 2009, la corte costituzionale federale tedesca nel marzo 2010 e la corte costituzionale ceca nel marzo 2011 hanno dichiarato incostituzionali le leggi di attuazione della direttiva nei rispettivi ordinamenti giuridici. La corte romena[97] ha riconosciuto che una limitazione dei diritti fondamentali può essere autorizzata purché rispetti determinate norme e preveda adeguate e sufficienti salvaguardie contro eventuali azioni arbitrarie da parte delle autorità statali. Tuttavia, alla luce della giurisprudenza della Corte europea dei diritti dell'uomo[98], la corte ha constatato che la legge di attuazione era troppo vaga quanto al campo di applicazione e alle finalità e non prevedeva sufficienti salvaguardie e ha stabilito che un «obbligo giuridico permanente» di conservare tutti i dati relativi al traffico per sei mesi era incompatibile con il diritto al rispetto della vita privata e alla libertà di espressione di cui all'articolo 8 della convenzione europea dei diritti dell'uomo.

La corte costituzionale tedesca[99] ha affermato che la conservazione dei dati crea una sensazione di controllo che potrebbe compromettere il libero esercizio dei diritti fondamentali. Ha riconosciuto esplicitamente che la conservazione dei dati per usi strettamente limitati, associata a un livello di sicurezza dei dati sufficientemente elevato, non viola necessariamente la legge fondamentale tedesca. La corte ha tuttavia sottolineato che la conservazione di tali dati costituisce una grave limitazione del diritto al rispetto della vita privata e dovrebbe quindi essere ammessa soltanto in circostanze particolarmente limitate, e che un periodo di conservazione di sei mesi costituisce il limite massimo («*an der Obergrenze*») che possa considerarsi proporzionato (punto 215). I dati dovrebbero essere richiesti soltanto se sussiste già il sospetto di un reato grave o la prova di un pericolo per la sicurezza pubblica, e l'estrazione dei dati dovrebbe essere vietata per alcune comunicazioni privilegiate (cioè quelle legate a esigenze psicologiche e sociali), che si basano sulla riservatezza. Si dovrebbe inoltre prevedere la cifratura dei dati e un controllo trasparente del loro uso.

La corte costituzionale ceca[100] ha dichiarato incostituzionale la legge di attuazione per il motivo che, quale provvedimento comportante un'ingerenza nell'esercizio dei diritti fondamentali, non era formulata con sufficiente chiarezza e precisione. La corte ha censurato la limitazione delle finalità in quanto inadeguata, alla luce della portata e dell'ambito di applicazione dell'obbligo di conservazione dei dati. Ha affermato che la definizione delle autorità competenti in materia di accesso e uso dei dati conservati e le relative procedure non erano sufficientemente chiare per garantire l'integrità e la riservatezza dei dati. Il singolo

---

96 La legge di attuazione in Islanda è la legge sulle telecomunicazioni 81/2003 (modificata nell'aprile 2005); in Liechtenstein è la legge sulle telecomunicazioni del 2006. In Norvegia la legge di attuazione è stata approvata il 5 aprile 2011 ed è attualmente in attesa di sanzione regia.

97 Decisione n. 1258 della corte costituzionale romena, dell'8 ottobre 2009.

98 Corte europea dei diritti dell'uomo, *Rotaru/Romania* 2000, *Sunday Times/Regno Unito* 1979 e *Principe Hans-Adam del Liechtenstein/Romania* 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, punti 1-345.

100 Sentenza della corte costituzionale ceca del 22 marzo riguardante la legge n. 127/2005 e il decreto n. 485/2005; cfr. in particolare i punti 45-48, 50-51 e 56.

cittadino non disponeva quindi di adeguate garanzie e salvaguardie contro eventuali abusi di potere da parte delle autorità pubbliche. Non ha criticato la direttiva di per sé e ha affermato che offre margini sufficienti per poter essere attuata nella Repubblica ceca nel rispetto della costituzione. Tuttavia la corte, in un *obiter dictum*, ha espresso dubbi in merito alla necessità, all'efficienza e all'adeguatezza della conservazione dei dati relativi al traffico, considerata la comparsa di nuove pratiche nella criminalità, per esempio l'uso di carte SIM anonime.

Questi tre Stati membri stanno ora esaminando nuove norme di attuazione della direttiva. Sono stati presentati ricorsi riguardanti la conservazione dei dati anche dinanzi alla corte costituzionale della Bulgaria, dove hanno determinato una revisione della legge di attuazione, di Cipro, dove alcuni mandati giudiziari emanati ai sensi della legge di attuazione sono stati dichiarati incostituzionali, e dell'Ungheria, dove è pendente una ricorso riguardante l'omissione delle finalità giuridiche del trattamento dei dati nella legge di attuazione[101].

La Commissione esaminerà le questioni sollevate dalla giurisprudenza nazionale nella futura proposta di revisione del quadro giuridico in materia di conservazione dei dati.

4.10. Controllo dell'applicazione della direttiva

La Commissione si attende che gli Stati membri che non hanno ancora pienamente recepito la direttiva, o che non hanno ancora adottato una legislazione che sostituisca la legge di attuazione dichiarata incostituzionale dalle corti nazionali, vi provvedano quanto prima. In caso contrario, la Commissione si riserva il diritto di esercitare i poteri conferitile dai trattati. A tutt'oggi la Corte di giustizia ha accertato che due Stati membri che non hanno recepito la direttiva (Austria e Svezia) sono venuti meno agli obblighi ad essi incombenti in forza del diritto dell'Unione[102]. Nell'aprile 2011 la Commissione ha deciso di deferire per la seconda volta la Svezia alla Corte per il mancato adempimento della sentenza di cui alla causa C-185/09, chiedendo l'irrogazione di sanzioni pecuniarie ai sensi dell'articolo 260 del trattato sul funzionamento dell'Unione europea, in seguito alla decisione del parlamento svedese di rinviare di dodici mesi l'adozione della legge di attuazione. La Commissione continua a seguire da vicino la situazione in Austria, le cui autorità hanno presentato un calendario per l'imminente adozione della legge di attuazione.

5. IL RUOLO DEI DATI CONSERVATI AI FINI DELLA GIUSTIZIA PENALE E DEL CONTRASTO

Questa sezione presenta un riepilogo delle funzioni dei dati conservati descritte dagli Stati membri nei loro contributi alla valutazione.

5.1. Volume dei dati conservati consultati dalle autorità nazionali competenti

Il volume del traffico delle telecomunicazioni e delle richieste di accesso ai dati relativi al traffico è in crescita. Le statistiche fornite da diciannove Stati membri per il 2008 e/o il 2009 indicano che, nell'insieme dell'UE, sono stati presentati più di due milioni di richieste di dati

---

101 Tribunale amministrativo supremo della Bulgaria, decisione n. 13627, 11 dicembre 2008; corte suprema di Cipro, ricorsi nn. 65/2009, 78/2009, 82/2009 e 15/2010-22/2010, 1° febbraio 2011; in Ungheria il ricorso costituzionale è stato proposto dall'associazione ungherese per le libertà civili il 2 giugno 2008.

102 Rispettivamente causa C-189/09 e causa C-185/09.

l'anno, con variazioni significative tra gli Stati membri, da meno di cento (Cipro) a più di un milione l'anno (Polonia). Secondo le informazioni sul tipo di dati richiesti fornite da dodici Stati membri per il 2008 o il 2009, il tipo di dati richiesto con maggiore frequenza riguarda la telefonia mobile (cfr. tabelle 5, 8 e 12). Le statistiche non indicano la finalità precisa per la quale è stata presentata ciascuna richiesta. La Repubblica ceca, la Lettonia e la Polonia hanno indicato che, nel caso dei dati relativi alla telefonia mobile, le autorità competenti hanno dovuto presentare la medesima richiesta a tutti i principali operatori di telefonia mobile e il numero effettivo di richieste per ciascun caso era quindi notevolmente inferiore a quello risultante dalle statistiche.

Non esiste una spiegazione ovvia per tali variazioni, sebbene le dimensioni della popolazione, le tendenze prevalenti nella criminalità, la limitazione delle finalità, le condizioni di accesso e i costi di acquisizione dei dati siano tutti fattori significativi.

5.2. Età dei dati conservati consultati

Secondo la ripartizione statistica fornita da nove Stati membri[103] per il 2008 (cfr. tabella 5 per una sintesi e l'allegato per maggiori informazioni), al momento della richiesta (iniziale) di accesso circa il 90% dei dati consultati dalle autorità competenti in detto anno era conservato da sei mesi o meno e circa il 70% da tre mesi o meno.

Tabella 5: Età dei dati conservati consultati nei nove Stati membri che hanno fornito una ripartizione per tipo di dati nel 2008

Età	*Telefonia fissa*	*Telefonia mobile*	*Dati relativi a Internet*	*Dati aggregati*
Meno di 3 mesi	61%	70%	56%	67%
Da 3 a 6 mesi	28%	18%	19%	19%
Da 6 a 12 mesi	8%	11%	18%	12%
Più di 12 mesi	3%	1%	7%	2%

Secondo la maggior parte degli Stati membri, il ricorso ai dati conservati da più di tre e anche da più di sei mesi è meno frequente ma può essere decisivo, e tendenzialmente rientra in tre categorie. In primo luogo, i dati relativi a Internet tendono a essere richiesti più tardi rispetto ad altri elementi di prova nel corso di un'indagine penale. Dall'analisi dei dati relativi alla telefonia di rete fissa e alla telefonia mobile spesso emergono potenziali indizi che determinano richieste successive di dati più vecchi. Per esempio, se durante un'indagine viene individuato un nome in base ai dati relativi alla telefonia fissa o mobile, gli inquirenti potrebbero voler identificare l'indirizzo del protocollo Internet (IP) utilizzato da tale persona e le persone con le quali è stata in contatto durante un determinato periodo di tempo utilizzando tale indirizzo IP. In una situazione di questo tipo, è probabile che gli inquirenti richiedano dati che consentano di rintracciare anche le comunicazioni con altri indirizzi IP e di identificare le persone che li hanno utilizzati.

In secondo luogo, le indagini concernenti reati particolarmente gravi, una serie di reati, la criminalità organizzata e gli atti di terrorismo tendenzialmente si basano su dati conservati per periodi più lunghi, che rispecchino il tempo necessario per la pianificazione di tali reati, per

[103] Repubblica ceca, Danimarca, Estonia, Irlanda, Spagna, Cipro, Lettonia, Malta, Regno Unito.

individuare i modelli di comportamento criminale e le relazioni tra i complici in un reato e per accertare la premeditazione. Le attività legate a reati finanziari complessi spesso vengono individuate soltanto dopo diversi mesi. In terzo luogo, e in via eccezionale, gli Stati membri hanno richiesto dati relativi al traffico conservati in altri Stati membri, i quali di norma possono comunicare tali dati soltanto previa autorizzazione giudiziaria in risposta a una rogatoria trasmessa da un giudice dello Stato membro richiedente. Questa forma di assistenza giudiziaria reciproca può comportare una procedura piuttosto lunga, motivo per cui alcuni dati richiesti in questi casi erano conservati da più di sei mesi.

5.3. Richieste transnazionali di dati conservati

Le indagini e le azioni penali possono riguardare prove o testimoni provenienti da un altro Stato membro o fatti avvenuti in un altro Stato membro. Secondo le statistiche fornite dagli Stati membri, meno dell'1% delle richieste ha riguardato dati conservati in un altro Stato membro. Le autorità di contrasto hanno indicato che preferiscono richiedere i dati agli operatori nazionali, i quali potrebbero aver conservato i dati pertinenti, anziché avviare una procedura di assistenza giudiziaria reciproca, che potrebbe richiedere tempi lunghi senza alcuna garanzia di ottenere l'accesso ai dati. La decisione quadro 2006/960/GAI relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri incaricate dell'applicazione della legge[104], che stabilisce i termini per la comunicazione di informazioni in risposta alla richiesta di un altro Stato membro, non è applicabile perché i dati conservati sono considerati informazioni ottenute con mezzi coercitivi, escluse dal campo di applicazione dello strumento. Nessuno Stato membro o autorità di contrasto ha tuttavia sollecitato misure atte ad agevolare tali scambi transnazionali.

5.4. Utilità dei dati conservati ai fini delle indagini e delle azioni penali

Sebbene il numero assoluto di richieste di dati indicato non rifletta necessariamente l'utilità dei dati nelle singole indagini penali, gli Stati membri in generale hanno affermato che la conservazione dei dati è quanto meno utile, e in alcuni casi indispensabile[105], per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti. Una condanna efficace si basa sull'ammissione di colpevolezza, sulle dichiarazioni di testimoni o su prove forensi. È stato riferito che il ricorso ai dati conservati relativi al traffico si è rivelato necessario per contattare i testimoni di un fatto che in assenza di tali dati non sarebbero stati identificati e per raccogliere prove o indizi nell'accertare la complicità in un reato. Alcuni Stati membri[106] hanno inoltre sostenuto che il ricorso ai dati conservati ha contribuito a scagionare indiziati, senza dover ricorrere ad altri metodi di controllo, quali le intercettazioni e le perquisizioni domiciliari, che si potrebbero considerare più intrusivi.

---

104 Decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (GU L 386 del 29.12.2006, pagg. 89-100 e GU L 200 dell'1.8.2007, pagg. 637-648).

105 La Repubblica ceca ha considerato la conservazione dei dati «assolutamente indispensabile in un gran numero di casi»; l'Ungheria ha affermato che era «indispensabile nelle attività ordinarie [delle agenzie di contrasto]»; la Slovenia ha indicato che l'assenza di dati conservati «paralizzerebbe l'attività delle agenzie di contrasto»; un'agenzia di polizia del Regno Unito ha descritto la disponibilità di dati relativi al traffico come «assolutamente essenziale … per condurre indagini riguardanti il terrorismo e i reati gravi».

106 Germania, Polonia, Slovenia, Regno Unito.

Nell'UE non esiste una definizione generale di «reato grave» e, di conseguenza, non esistono statistiche a livello europeo sull'incidenza dei reati gravi o delle indagini o azioni penali riguardanti reati gravi, sebbene vengano regolarmente pubblicati dati sulla criminalità e sulla giustizia. Secondo i diciannove Stati membri che hanno fornito alcuni tipi di dati per il 2009 e/o il 2008, il volume aggregato delle richieste di dati conservati ammonta a circa 2,6 milioni. Rispetto alle più recenti statistiche sui reati e sulla giustizia penale disponibili per tali diciannove Stati membri – che si riferiscono a tutti i reati denunciati, non soltanto a quelli gravi – si può affermare che vi sono state poco più di due richieste per ciascun agente di polizia l'anno, ovvero circa undici richieste ogni cento reati registrati[107].

Sulla base delle statistiche e degli esempi forniti, che collegano l'uso dei dati storici di comunicazione conservati al numero di condanne, assoluzioni, archiviazioni e reati evitati, si possono trarre alcune conclusioni in merito al ruolo e all'utilità dei dati conservati nelle indagini penali.

Ricostruzione della dinamica di un reato

In primo luogo, i dati conservati permettono di ricostruire gli eventi che hanno condotto a un reato. Sono utilizzati per distinguere o per corroborare altre forme di prova sulle attività e sui legami tra persone sospette. In particolare, i dati relativi all'ubicazione sono stati usati, sia dalle autorità di contrasto sia dagli imputati, per escludere sospetti dalla scena del crimine e per verificare alibi. Tali prove possono quindi escludere una persona da un'indagine penale, eliminando così la necessità di ricerche più intrusive, o determinarne l'assoluzione in sede processuale. Il Belgio ha citato il caso della condanna nel 2008 dei responsabili del rapimento di un dipendente del tribunale di Anversa, nel quale i dati relativi all'ubicazione, che collegavano le attività dei malviventi in tre diverse città, sono stati decisivi per persuadere i giurati della loro complicità. In un altro caso, riguardante un omicidio collegato a una banda di motociclisti nel 2007, i dati relativi all'ubicazione dei telefoni cellulari degli imputati hanno dimostrato che si trovavano nella zona in cui era stato commesso l'omicidio e hanno portato a una parziale confessione[108]. Secondo il Belgio, l'Irlanda e il Regno Unito, alcuni reati riguardanti le comunicazioni via Internet possono essere accertati *soltanto* per mezzo della conservazione dei dati: per esempio, le minacce di violenza espresse nelle *chat room* spesso non lasciano altre tracce se non i dati relativi al traffico informatico. Una situazione analoga si applica nel caso di reati commessi telefonicamente. L'Ungheria e la Polonia hanno citato un caso di frode ai danni di persone anziane tra la fine del 2009 e l'inizio del 2010, perpetrata mediante chiamate telefoniche nelle quali i malviventi fingevano di essere familiari che avevano bisogno di un prestito; è stato possibile identificare i responsabili soltanto tramite i dati conservati relativi alla telefonia.

Avvio di indagini penali

---

107 Nel 2007 nell'UE-27 erano presenti 1,7 milioni di agenti di polizia, 1,2 milioni dei quali nei diciannove Stati membri che hanno fornito statistiche sulle richieste di dati conservati; nel 2007 le forze di polizia dell'UE hanno registrato 29,2 milioni di reati, 24 milioni dei quali nei diciannove Stati membri che hanno fornito statistiche (fonte: Eurostat 2009).

108 National Policing Improvement Agency (Regno Unito), *The Journal of Homicide and Major Incident Investigation*, vol. 5, n. 1, primavera 2009, pagg. 39-51.

In secondo luogo, vi sono stai casi in cui, in assenza di prove forensi o testimoni oculari, l'unico modo di avviare un'indagine è stato fare ricorso ai dati conservati. La Germania ha citato l'esempio dell'omicidio di un agente di polizia, in cui il malvivente era fuggito a bordo del veicolo della vittima e poi lo aveva abbandonato. È stato possibile accertare che in seguito aveva fatto una telefonata per reperire un altro mezzo di trasporto. Non esistevano prove forensi o testimoni oculari che permettessero di identificare l'assassino e per proseguire le indagini le autorità hanno fatto assegnamento sulla disponibilità di dati relativi al traffico. Nei casi di abusi sessuali sui minori legati a Internet, la conservazione dei dati è stata indispensabile per il buon esito delle indagini. Assieme ad altre tecniche investigative, i dati conservati permettono di identificare i consumatori di contenuti pedopornografici[109] e di agevolare l'identificazione e il soccorso delle vittime. La Repubblica ceca ha riferito che in assenza dell'accesso ai dati conservati relativi a Internet non sarebbe stato possibile avviare indagini nell'ambito dell'«Operazione Vilma», riguardante una rete di utenti e divulgatori di pedopornografia. A livello UE, l'efficacia dell'«Operazione Salvataggio» (facilitata dall'Europol) nel proteggere i minori dagli abusi è stata ostacolata dall'assenza di una legge di attuazione in materia di conservazione dei dati, che ha impedito ad alcuni Stati membri di condurre indagini sui membri di una vasta rete internazionale di pedofili che usavano indirizzi IP potenzialmente attivi da più di un anno.

Nelle indagini riguardanti la criminalità informatica, spesso il primo indizio è un indirizzo IP. Le autorità di contrasto, tramite l'estrazione dei dati relativi al traffico, possono identificare l'abbonato che si cela dietro un indirizzo IP, prima di stabilire se sia possibile avviare un'indagine penale. Tali dati possono inoltre permettere alle forze di polizia di avvertire le potenziali vittime di attacchi informatici: quando sequestrano un server di comando e di controllo utilizzato da operatori di *botnet* (rete di sistemi compromessi che eseguono programmi sotto un comando comune), gli investigatori possono vedere soltanto gli indirizzi IP collegati a tale server; tuttavia, tramite l'accesso ai dati conservati, possono identificare e avvertire le potenziali vittime cui appartengono tali indirizzi IP.

I dati conservati sono parte integrante delle indagini penali

In terzo luogo, sebbene le autorità di polizia e giudiziarie nella maggior parte degli Stati membri non raccolgano dati statistici sul tipo di prove che si sono rivelate decisive per assicurare condanne o assoluzioni, i dati conservati sono parte integrante delle indagini e dell'azione penale nell'UE. Alcuni Stati membri hanno affermato di non essere sempre in grado di isolare l'incidenza dei dati conservati sul buon esito delle indagini e delle azioni penali, perché le autorità giurisdizionali esaminano tutte le prove presentate e raramente considerano decisivo un singolo elemento di prova[110]. I Paesi Bassi hanno riferito che, tra gennaio e luglio 2010, i dati storici relativi al traffico sono stati un fattore decisivo in 24 decisioni giudiziarie. La Finlandia ha indicato che nel 56% delle 3 405 richieste, i dati conservati si sono rivelati «importanti» o «essenziali» per l'accertamento e/o il perseguimento di reati. Il Regno Unito ha fornito dati che tentano di quantificare l'impatto della conservazione dei dati sull'azione penale; ha comunicato che, per tre delle sue agenzie di

---

109 Il progetto «Misurazione e analisi dell'attività p2p contro i contenuti pedofili», sostenuto nel quadro del programma per l'uso più sicuro di Internet, ha fornito informazioni accurate sull'attività di pedofilia nel sistema peer-to-peer eDonkey e ha permesso di identificare 178 000 utenti (su 89 milioni di utenti vagliati) che hanno richiesto contenuti pedofili.

110 Belgio, Repubblica ceca, Lituania.

contrasto, i dati conservati sono stati necessari nella maggior parte se non in tutte le indagini sfociate in azioni penali o condanne.

5.5. Sviluppi tecnologici e uso di carte SIM prepagate

Le autorità di contrasto devono essere al passo con gli sviluppi tecnologici cui i criminali fanno ricorso per commettere reati o rendersene complici. La conservazione dei dati fa parte degli strumenti di indagine necessari per dotare le autorità di contrasto di mezzi atti a rispondere alle attuali sfide della criminalità, nella loro diversità, quantità e rapidità, in maniera gestibile ed economica. Alcune forme di comunicazione sempre più diffuse non rientrano nel campo di applicazione della direttiva. Le reti virtuali private (*Virtual Private Networks,* VPN), per esempio nelle università o nelle grandi aziende, permettono a diversi utenti di connettersi a Internet attraverso un unico punto di accesso e utilizzando lo stesso indirizzo IP. Tuttavia una nuova tecnologia che permette di attribuire indirizzi ai singoli utenti delle VPN è in fase di introduzione.

La percentuale di utenti della telefonia mobile che usano servizi prepagati varia all'interno dell'UE. Alcuni Stati membri hanno affermato che le carte SIM anonime prepagate, soprattutto se acquistate in un altro Stato membro, potrebbero anche essere usate da persone coinvolte in attività criminali per evitare l'identificazione nelle indagini penali[111]. Sei Stati membri (Danimarca, Spagna, Italia, Grecia, Slovacchia, Bulgaria) hanno adottato misure che impongono la registrazione delle carte SIM prepagate. Questi e altri Stati membri (Polonia, Cipro, Lituania) si sono espressi a favore di una disposizione a livello UE che preveda la registrazione obbligatoria dell'identità degli utenti di servizi prepagati. Non sono stati forniti elementi che confermino l'efficacia di tali misure nazionali. Sono stati evidenziati limiti potenziali, per esempio in caso di furto di identità o quando una carta SIM è acquistata da una terza persona, oppure quando un utente utilizza una carta acquistata in un paese terzo servendosi del roaming. Nel complesso per il momento la Commissione non è convinta della necessità di un'azione a livello UE in questo ambito.

6. IMPATTO DELLA CONSERVAZIONE DEI DATI SUGLI OPERATORI E SUI CONSUMATORI

6.1. Operatori e consumatori

In una dichiarazione congiunta alla Commissione, cinque importanti associazioni del settore hanno affermato che l'impatto economico della direttiva è «considerevole» o «enorme» per i «fornitori di servizi di piccole dimensioni», in quanto lo strumento lascia «ampi margini di manovra»[112]. Otto operatori hanno presentato stime estremamente variabili dei costi – in termini di spese in conto capitale e spese di esercizio – per conformarsi alla direttiva. Queste affermazioni possono trovare conferma nei livelli di rimborso delle spese sostenute dagli operatori comunicati da quattro Stati membri (cfr. tabella 6).

Uno studio condotto prima del recepimento della direttiva nella maggior parte degli Stati membri stimava il costo di installazione di un sistema di conservazione dei dati per un fornitore di servizi Internet con mezzo milione di clienti intorno a 375 240 euro nel primo

---

111 Conclusioni del Consiglio sulla lotta contro l'utilizzo delle comunicazioni elettroniche e del loro anonimato a fini criminali.

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF.

anno e successivamente a 9 870 euro al mese in spese di esercizio[113], e il costo di installazione di un sistema di estrazione dei dati a 131 190 euro, con spese di esercizio pari a 28 960 euro al mese. Tuttavia la corte costituzionale tedesca, nella sua sentenza del 2 marzo 2010, ha rilevato che l'imposizione di un obbligo di conservazione «non era eccessivamente onerosa per i fornitori di servizi interessati [né] sproporzionata per quanto riguarda gli oneri finanziari sostenuti dalle imprese in conseguenza dell'obbligo di conservazione»[114]. I costi unitari di conservazione dei dati sono inversamente proporzionali alle dimensioni dell'operatore e al livello di normalizzazione adottato da uno Stato membro per l'interazione con gli operatori[115].

Nelle risposte al questionario della Commissione, la maggior parte degli operatori non è stata in grado di quantificare l'impatto della direttiva sulla concorrenza, sui prezzi al dettaglio per i consumatori o sugli investimenti in nuove infrastrutture e servizi.

Non esistono conferme di un effetto quantificabile o sostanziale della direttiva sui prezzi al consumo dei servizi di comunicazione elettronica; nell'ambito della consultazione pubblica del 2009 non sono pervenuti contributi dei rappresentanti dei consumatori. Secondo uno studio condotto in Germania per conto di un'organizzazione della società civile, i consumatori intendono modificare il loro comportamento in materia di comunicazioni ed evitare l'uso dei servizi di comunicazione elettronica in alcune circostanze; tuttavia non sono disponibili dati sufficienti a dimostrare che un cambiamento di comportamento sia effettivamente avvenuto negli Stati membri interessati o nell'UE in generale[116].

La Commissione intende valutare l'impatto delle future modifiche della direttiva sul settore e sui consumatori, eventualmente anche mediante un'indagine eurobarometro specifica per sondare le percezioni dei cittadini.

6.2. Rimborso delle spese

La direttiva non disciplina il rimborso delle spese sostenute dagli operatori in conseguenza dell'obbligo di conservazione dei dati. Tali spese si possono intendere come:

(a) *spese di esercizio*, cioè i costi di funzionamento o le spese correnti legate al funzionamento dell'attività economica, di un dispositivo, di un componente, di un elemento delle attrezzature o dell'infrastruttura; e

(b) *spese in conto capitale*, cioè le spese che creano benefici futuri, o il costo di sviluppo o fornitura di parti durevoli per il prodotto o il sistema, che può comprendere il costo della manodopera e le spese per l'infrastruttura, quali l'affitto e i servizi pubblici.

Tutti gli Stati membri garantiscono una forma di rimborso se i dati sono richiesti nel contesto di un procedimento giudiziario penale. Due Stati membri hanno indicato che rimborsano sia le spese di esercizio sia le spese in conto capitale. Sei rimborsano soltanto le spese di esercizio.

---

113 Wilfried Gansterer e Michael Ilger, *Data Retention – The EU Directive 2006/24/EC from a Technological Perspective*, Verlag Medien und Recht, Vienna 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 del 2 marzo 2010, punto 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx.

116 Lo studio è stato condotto da Forsa e richiesto da AK Vorratsdatenspeicherung; http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

Nessun altro regime di rimborso è stato notificato alla Commissione. Per i particolari si rimanda alla tabella 6.

Tabella 6: Stati membri che rimborsano le spese			
Stato membro	**Spese di esercizio**	**Spese in conto capitale**	**Costi di rimborso annui (milioni di EUR)**
Belgio	Sì	No	22 (2008)
Bulgaria	No	No	-
Repubblica ceca	Non recepita[117]		
Danimarca	Sì	No	-
Germania	Non recepita		
Estonia	Sì	No	-
Irlanda	No	No	-
Grecia	No	No	-
Spagna	No	No	-
Francia	Sì	No	-
Italia	-	-	-
Cipro	No	No	-
Lettonia	No	No	-
Lituania	Sì, se richiesto e motivato	No	-
Lussemburgo	No	No	-
Ungheria	No	No	-
Malta	No	No	-
Paesi Bassi	Sì	No	-
Austria	Non recepita		
Polonia	No	No	-
Portogallo	No	No	-
Romania	Non recepita		
Slovenia	No	No	-
Slovacchia	No	No	-
Finlandia	Sì	Sì	1
Svezia	Non recepita		
Regno Unito	Sì	Sì	55 (rimborsati complessivamente per i costi sostenuti nell'arco di tre anni)

Da quanto precede si può concludere che la direttiva non ha pienamente conseguito il suo obiettivo di creare condizioni omogenee per gli operatori nell'UE. La Commissione prenderà in considerazione soluzioni volte a ridurre al minimo gli ostacoli al funzionamento del mercato interno, assicurando che i costi che gli operatori sostengono per conformarsi agli obblighi in materia di conservazione dei dati siano rimborsati in modo uniforme, con particolare riguardo per gli operatori di piccole e medie dimensioni.

[117] Prima che la legge di attuazione ceca fosse dichiarata incostituzionale, la Repubblica ceca rimborsava sia le spese operative sia le spese in conto capitale e per il 2009 aveva indicato costi di rimborso pari a 6,8 milioni di euro.

7. IMPLICAZIONI DELLA CONSERVAZIONE DEI DATI PER I DIRITTI FONDAMENTALI

7.1. I diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali

La conservazione dei dati costituisce una limitazione del diritto al rispetto della vita privata e del diritto alla protezione dei dati personali, entrambi diritti fondamentali nell'Unione europea[118]. Ai sensi dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, tali limitazioni devono essere «previste dalla legge e rispettare il contenuto essenziale di detti diritti […] nel rispetto del principio di proporzionalità», ed essere necessarie e rispondere a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Nella pratica, ciò significa che le eventuali limitazioni devono essere[119]:

(a) formulate con precisione e prevedibilità;

(b) necessarie per realizzare una finalità di interesse generale o per proteggere i diritti e le libertà altrui;

(c) proporzionate alla finalità perseguita; e

(d) conformi al contenuto essenziale dei diritti fondamentali in questione.

Anche l'articolo 8, paragrafo 2, della convenzione europea dei diritti dell'uomo riconosce che l'ingerenza di un'autorità pubblica nell'esercizio del diritto al rispetto della vita privata può essere giustificata se necessaria alla sicurezza nazionale, alla pubblica sicurezza e alla prevenzione dei reati[120]. L'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche e i considerando della direttiva sulla conservazione dei dati ribadiscono tali principi, sui quali si fonda l'approccio dell'UE alla conservazione dei dati.

La successiva giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo ha definito le condizioni che eventuali limitazioni del diritto al rispetto della vita privata devono soddisfare. Tale giurisprudenza è rilevante al fine di stabilire se la direttiva debba essere modificata, in particolare per quanto riguarda le condizioni relative all'accesso e al ricorso ai dati conservati.

Le eventuali limitazioni del diritto al rispetto della vita privata devono essere precise e garantire la prevedibilità

Nella causa *Österreichischer Rundfunk*, la Corte di giustizia ha stabilito che un articolo di legge che comporti un'ingerenza nel diritto alla vita privata deve essere «redatto in modo

---

118 Articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (GU C 83 del 30.3.2010, pag. 389); l'articolo 8 sancisce il diritto di ogni persona «alla protezione dei dati di carattere personale che la riguardano». Anche l'articolo 16 del trattato sul funzionamento dell'Unione europea (GU C 83 del 30.3.2010, pag. 1) sancisce il diritto di ogni persona «alla protezione dei dati di carattere personale che la riguardano».

119 Cfr. la «*check-list* diritti fondamentali» della Commissione per tutte le proposte legislative, di cui alla comunicazione della Commissione «Strategia per un'attuazione effettiva della Carta dei diritti fondamentali dell'Unione europea» (COM (2010) 573/4).

120 Articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, STCE n. 5, del Consiglio d'Europa del 4.11.1950.

sufficientemente preciso per consentire ai destinatari della legge di regolare la loro condotta … [al fine di soddisfare] il requisito di prevedibilità».

Eventuali limitazioni del diritto al rispetto della vita privata devono essere necessarie e accompagnate da salvaguardie minime

Nella causa *Copland/Regno Unito*, riguardante la sorveglianza da parte dello Stato delle chiamate telefoniche, della posta elettronica e dell'accesso a Internet di una persona, la Corte europea dei diritti dell'uomo ha stabilito che tale limitazione del diritto al rispetto alla vita privata poteva considerarsi necessaria soltanto se fondata sulla legislazione nazionale vigente[121]. Nella causa *S. e Marper/Regno Unito*, riguardante la conservazione dei profili genetici o delle impronte digitali di persone dopo la conclusione del procedimento penale nei loro confronti per assoluzione o archiviazione, la Corte ha stabilito che tale limitazione del diritto al rispetto della vita privata può essere giustificata soltanto se risponde a esigenze sociali inderogabili, è proporzionata allo scopo perseguito e i motivi addotti dall'autorità pubblica per giustificarla sono pertinenti e sufficienti[122]. Secondo i principi fondamentali in materia di protezione dei dati, la conservazione dei dati deve essere proporzionata allo scopo per cui sono stati raccolti e limitata nel tempo[123]. Per quanto riguarda le intercettazioni telefoniche, la sorveglianza segreta e la raccolta segreta di intelligence, «è essenziale stabilire norme chiare e dettagliate che disciplinino la portata e l'applicazione delle misure e prevedano salvaguardie minime concernenti, in particolare, la durata, l'immagazzinamento, l'uso, l'accesso di terzi, le procedure volte a preservare l'integrità e la riservatezza dei dati e le procedure di distruzione degli stessi, prevedendo così sufficienti garanzie contro il rischio di abusi e arbitrarietà».

Eventuali limitazioni del diritto al rispetto della vita privata devono essere proporzionate all'interesse generale

Analogamente, nella causa *Schecke e Eifert*, riguardante la pubblicazione su un sito Internet di tutti i beneficiari di sovvenzioni agricole[124], la Corte di giustizia ha ritenuto che il legislatore dell'UE non sembrava avere adottato provvedimenti adeguati per garantire l'equilibrio tra il rispetto del contenuto essenziale del diritto al rispetto alla vita privata e le finalità di interesse generale (la trasparenza) riconosciute dall'UE. In particolare, la Corte ha constatato che il legislatore non aveva preso in considerazione altre modalità che fossero conformi all'obiettivo e meno lesive del diritto dei beneficiari delle sovvenzioni al rispetto della loro vita privata e alla protezione dei loro dati personali. Di conseguenza, la Corte ha concluso che il legislatore aveva superato i limiti della proporzionalità, in quanto «le limitazioni alla protezione dei dati personali devono operare entro i limiti dello stretto necessario».

---

121 Sentenza della Corte europea dei diritti dell'uomo del 3.4.2007, nella causa *Copland/Regno Unito*, Strasburgo, pag. 9.

122 Sentenza della Corte europea dei diritti dell'uomo del 4.12.2008, nella causa *S. e Marper/Regno Unito*, Strasburgo, pag. 31.

123 *S. e Marper*, pag. 30.

124 Causa C-92/09, *Volker e Markus Schecke GbR/Land Hessen*, e causa C-93/09, *Eifert/Land Hessen e Bundesanstalt für Landwirtschaft und Ernahrung*, 9.11.10.

7.2. Critiche al principio di conservazione dei dati

Varie organizzazioni della società civile hanno scritto alla Commissione affermando che la conservazione dei dati, in linea di principio, costituisce una limitazione ingiustificata e non necessaria del diritto al rispetto della vita privata. Ritengono che la conservazione «generale e indiscriminata» dei dati di telecomunicazione relativi al traffico, all'ubicazione e all'abbonato, senza consenso dell'interessato, costituisca una limitazione illegittima dei diritti fondamentali. A seguito di un'azione legale intentata in uno Stato membro (Irlanda) da un gruppo di difesa dei diritti civili, la questione della validità della direttiva sarà esaminata dalla Corte di giustizia[125]. Anche il garante europeo della protezione dei dati ha espresso dubbi in merito alla necessità dello strumento.

7.3. Richiesta di norme più severe in materia di sicurezza e protezione dei dati

Secondo la relazione del Gruppo di lavoro «articolo 29» sulla seconda azione di controllo dell'applicazione, la conservazione di qualsiasi dato relativo al traffico comporta il rischio di violazione della riservatezza delle comunicazioni e della libertà di espressione. Il Gruppo ha criticato alcuni aspetti dell'attuazione a livello nazionale, segnatamente la trasmissione dei dati, i periodi di conservazione, le categorie di dati conservati e le misure di sicurezza dei dati. Ha indicato casi in cui sono state conservate informazioni sul *contenuto* di comunicazioni via Internet, escluse dal campo di applicazione della direttiva, tra cui gli indirizzi IP di destinazione e gli URL di siti Internet, l'intestazione dei messaggi di posta elettronica e l'elenco dei destinatari nel campo «cc». Ha quindi chiesto che venga precisato che le categorie sono esaustive e che non vengano imposti agli operatori ulteriori obblighi di conservazione di dati.

Il garante europeo della protezione dei dati ha affermato che la direttiva «non ha armonizzato la legislazione nazionale» e che il ricorso ai dati conservati non si limita allo stretto necessario per contrastare i reati gravi[126]. Ha sostenuto che uno strumento dell'UE contenente norme in materia di conservazione obbligatoria dei dati, qualora ne sia dimostrata la necessità, dovrebbe contenere anche norme in materia di accesso e successivo uso dei dati da parte delle autorità di contrasto. Ha invitato l'UE ad adottare un quadro legislativo completo che, oltre a imporre agli operatori l'obbligo di conservare i dati, disciplini anche il modo in cui gli Stati membri usano i dati a fini di contrasto, al fine di garantire la «certezza del diritto per i cittadini».

In generale, le autorità di protezione dei dati hanno affermato che la conservazione dei dati di per sé comporta il rischio di potenziali violazioni della vita privata che la direttiva non affronta a livello UE, richiedendo invece agli Stati membri di garantire il rispetto delle norme nazionali di protezione dei dati. Sebbene non vi siano esempi concreti di gravi violazioni della vita privata, il rischio di violazioni della sicurezza dei dati rimane, e potrebbe aumentare con gli sviluppi tecnologici e le tendenze in atto nelle forme di comunicazione, indipendentemente dal fatto che i dati siano conservati a fini commerciali o di sicurezza, all'interno o all'esterno dell'UE, a meno che non si introducano ulteriori salvaguardie.

---

125 Il 5 maggio 2010 la Irish High Court ha accolto l'istanza di Digital Rights Ireland Limited e ha proposto una domanda di pronuncia pregiudiziale alla Corte di giustizia dell'UE, ai sensi dell'articolo 267 del trattato sul funzionamento dell'Unione europea.

126 Intervento di Peter Hustinx alla conferenza «*Taking on the Data Retention Directive*» del 3 dicembre 2010.

8. CONCLUSIONI E RACCOMANDAZIONI

La presente relazione evidenzia una serie di vantaggi e i margini di miglioramento dell'attuale regime di conservazione dei dati nell'UE. L'UE ha adottato la direttiva in un momento di massima allerta contro imminenti attacchi terroristici. La valutazione d'impatto che la Commissione intende effettuare offre l'opportunità di esaminare la conservazione dei dati nell'UE alla luce dei principi di necessità e proporzionalità, tenuto conto e nell'interesse della sicurezza nazionale, del buon funzionamento del mercato interno e del rafforzamento del rispetto della vita privata e del diritto fondamentale alla protezione dei dati personali. La proposta della Commissione di revisione del quadro giuridico in materia di conservazione dei dati dovrebbe basarsi sulle seguenti conclusioni e raccomandazioni.

8.1. L'Unione europea dovrebbe sostenere e disciplinare la conservazione dei dati quale misura di sicurezza

La maggior parte degli Stati membri è del parere che le norme dell'UE in materia di conservazione dei dati continuino a essere uno strumento necessario per l'attività di contrasto, la protezione delle vittime e la giustizia penale. Le informazioni fornite dagli Stati membri sotto forma di statistiche ed esempi, pur essendo per certi aspetti limitate, confermano il ruolo importantissimo dei dati conservati ai fini delle indagini penali. Tali dati forniscono validi indizi e prove per prevenire e perseguire i reati e amministrare la giustizia. Il ricorso ai dati conservati ha permesso la condanna di colpevoli in casi che, senza la conservazione dei dati, forse non sarebbero mai stati risolti. Ha altresì permesso l'assoluzione di persone innocenti. L'armonizzazione delle norme in questo ambito dovrebbe fare della conservazione dei dati un efficace strumento di lotta alla criminalità, garantire la certezza del diritto per il settore e il buon funzionamento del mercato interno, e assicurare l'applicazione uniforme in tutta l'UE di un livello elevato di rispetto del diritto alla vita privata e del diritto alla protezione dei dati personali.

8.2. Il recepimento non è omogeneo

La legislazione di attuazione è in vigore in ventidue Stati membri. L'ampio margine di manovra che l'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche lascia agli Stati membri per adottare le disposizioni in materia di conservazione dei dati rende altamente problematica la valutazione della direttiva sulla conservazione dei dati. Sussistono notevoli differenze tra le leggi di attuazione quanto alla limitazione delle finalità, l'accesso ai dati, i periodi di conservazione, la protezione e la sicurezza dei dati e le statistiche. Tre Stati membri violano la direttiva, in quanto le loro leggi di attuazione sono state dichiarate incostituzionali dalle rispettive corti costituzionali. Altri due Stati membri non hanno ancora provveduto al recepimento. La Commissione continuerà a collaborare con gli Stati membri per garantire l'applicazione efficace della direttiva, e continuerà altresì a svolgere il suo ruolo di garante dell'applicazione del diritto dell'UE, se necessario facendo ricorso al procedimento di infrazione.

8.3. La direttiva non ha pienamente armonizzato l'approccio alla conservazione dei dati e non ha creato condizioni omogenee per gli operatori

La direttiva ha assicurato che la maggior parte degli Stati membri ora provveda alla conservazione dei dati. Non garantisce di per sé che i dati conservati siano immagazzinati, estratti e usati nel pieno rispetto del diritto alla vita privata e del diritto alla protezione dei dati personali. Spetta agli Stati membri garantire che tali diritti siano rispettati. La direttiva mirava

soltanto a un'armonizzazione parziale dei sistemi di conservazione dei dati e non sorprende quindi che non esista un approccio comune, né in termini di disposizioni specifiche della direttiva stessa, quali la limitazione delle finalità o i periodi di conservazione, né in termini di aspetti esclusi dal suo campo di applicazione, come il rimborso delle spese. Tuttavia, al di là del livello di variabilità espressamente previsto dalla direttiva, le differenze nell'applicazione nazionale della conservazione dei dati hanno creato notevoli difficoltà per gli operatori.

8.4. I costi sostenuti dagli operatori dovrebbero essere rimborsati in modo uniforme

Continua a sussistere una mancanza di certezza del diritto per il settore. L'obbligo di conservare ed estrarre i dati rappresenta un costo considerevole per gli operatori, soprattutto quelli di piccole dimensioni. Gli operatori ricevono inoltre un trattamento diverso nei vari Stati membri, anche per quanto riguarda il rimborso delle spese. Non vi sono tuttavia prove del fatto che il settore delle telecomunicazioni nel suo insieme abbia subito ripercussioni negative a causa della direttiva. La Commissione esaminerà soluzioni volte a garantire agli operatori un rimborso uniforme dei costi sostenuti.

8.5. Garantire la proporzionalità nell'intero processo di immagazzinamento, estrazione e uso dei dati

La Commissione garantirà che ogni futura proposta in materia di conservazione dei dati rispetti il principio di proporzionalità e sia idonea a realizzare l'obiettivo di contrastare i reati gravi e il terrorismo senza andare al di là di quanto necessario a tal fine. Farà sì che eventuali deroghe o limitazioni riguardanti la protezione dei dati personali siano applicate soltanto nella misura strettamente necessaria. Effettuerà una valutazione completa delle implicazioni che una regolamentazione più severa sull'immagazzinamento, l'accesso e il ricorso ai dati relativi al traffico può avere sull'efficacia e sull'efficienza della giustizia penale e delle attività di contrasto, sul diritto alla vita privata e sui costi a carico della pubblica amministrazione e degli operatori. Nell'ambito della valutazione d'impatto si dovranno esaminare, in particolare, gli aspetti seguenti:

- coerenza tra la limitazione delle finalità della conservazione dei dati e le categorie di reati per le quali si possono consultare e usare i dati conservati;
- maggiore armonizzazione ed eventuale riduzione dei periodi di conservazione obbligatoria dei dati;
- garanzia di un controllo indipendente delle richieste di accesso e del regime generale di conservazione dei dati e di accesso agli stessi applicato in tutti gli Stati membri;
- limitazione delle autorità autorizzate a consultare i dati;
- riduzione delle categorie di dati da conservare;
- orientamenti in materia di misure di sicurezza tecniche e organizzative per l'accesso ai dati, comprese le procedure di trasmissione;
- orientamenti sull'uso dei dati, compresa la prevenzione del *data mining*; e
- elaborazione di procedure di quantificazione e di notifica per agevolare il confronto dell'applicazione e la valutazione di uno strumento futuro.

La Commissione valuterà inoltre se e come un approccio a livello UE alla conservazione per ordine giudiziario possa integrare la conservazione dei dati.

In relazione con la «*check-list* diritti fondamentali» e l'approccio alla gestione delle informazioni nello spazio di libertà, sicurezza e giustizia[127], la Commissione esaminerà ciascuno di questi aspetti in funzione del principio di proporzionalità e del requisito di prevedibilità. Garantirà inoltre la coerenza con la revisione in corso del quadro giuridico dell'UE in materia di protezione dei dati[128].

8.6. Prossime tappe

Alla luce della presente valutazione, la Commissione proporrà una revisione dell'attuale quadro giuridico in materia di conservazione dei dati. Elaborerà alcune soluzioni in consultazione con le autorità di contrasto, le autorità giudiziarie, i rappresentanti del settore, le associazioni dei consumatori, le autorità di protezione dei dati e le organizzazioni della società civile. Condurrà ulteriori ricerche per sondare le percezioni dei cittadini riguardo alla conservazione dei dati e il suo impatto sui comportamenti. I risultati di tali attività saranno integrati in una valutazione d'impatto delle soluzioni politiche individuate, che costituirà la base per la proposta della Commissione.

---

127 Per il riferimento alla comunicazione sull'attuazione della Carta dei diritti fondamentali cfr. *supra*; «Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia», COM(2010) 385 del 20.7.2010.

128 COM (2010) 609 del 4.11.2010.

Allegato: Statistiche supplementari sulla conservazione dei dati relativi al traffico

Note relative all'allegato:

1. Per età dei dati si intende il tempo trascorso fra la data in cui i dati sono stati conservati e la data in cui le autorità competenti ne hanno richiesto la trasmissione.

2. Per dati relativi a Internet si intendono i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet.

3. Le statistiche per la Repubblica ceca, la Lettonia e la Polonia sono soggette ad avvertenze (cfr. punto 5.1).

Statistiche fornite dagli Stati membri per il 2008

Tabella 7: Richieste di dati conservati relativi al traffico per età nel 2008

Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	102691	18440	10110	319	0	0	0	0	131560
Danimarca	2669	672	185	37	23	2	7	4	3599
Germania	9363	2336	985	0	0	0	0	0	12684
Estonia	2773	733	157	827	0	0	0	0	4490
Irlanda	8981	2016	936	1855	90	85	78	54	14095
Grecia	Ripartizione per età non fornita								584
Spagna	22629	15868	10298	4783	0	0	0	0	53578
Francia	Ripartizione per età non fornita								503437
Italia	Dati non forniti								
Cipro	30	4	0	0	0	0	0	0	34
Lettonia	10539	2739	1368	1211	597	438	0	0	16892
Lituania	55735	23817	5251	512	0	0	0	0	85315
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	810	59	0	0	0	0	0	0	869
Paesi Bassi	Ripartizione per età non fornita								85000
Austria	Ripartizione per età non fornita								3093
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Ripartizione per età non fornita								2821
Slovacchia	Dati non forniti								
Finlandia	9134	1144	448	214	268				4008
Svezia	Dati non forniti								
Regno Unito	315350	88339	34665	19398	6385	2973	1536	1576	470222
Totale	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Esclusa la Finlandia

Tabella 8: Richieste di dati conservati relativi al traffico per tipo di dati nel 2008 (tra parentesi numero di casi in cui non è stato possibile soddisfare le richieste di dati - se fornito)				
Tipo di dati / Stato membro	**Telefonia di rete fissa**	**Telefonia mobile**	**Internet**	**Totale**
Belgio	Dati non forniti			
Bulgaria	Dati non forniti			
Repubblica Ceca	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Danimarca	192 (0)	3273 (5)	134 (0)	3599 (5)
Germania	Ripartizione per tipo di dati non fornita			12684 (931)
Estonia	4114 (1519)	376 (7)	Dati non forniti	4490 (1526)
Irlanda	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Grecia	Ripartizione per tipo di dati non fornita			584
Spagna	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Francia	Ripartizione per tipo di dati non fornita			503437
Italia	Dati non forniti			
Cipro	3 (0)	31 (5)	0 (0)	34 (5)
Lettonia	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Lituania	765 (72)	84550 (5657)	Dati non forniti	85315 (5729)
Lussemburgo	Dati non forniti			
Ungheria	Dati non forniti			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Paesi Bassi	Ripartizione per tipo di dati non fornita			85000
Austria	Ripartizione per tipo di dati non fornita			3093
Polonia	Dati non forniti			
Portogallo	Dati non forniti			
Romania	Dati non forniti			
Slovenia	Ripartizione per tipo di dati non fornita			2821
Slovacchia	Dati non forniti			
Finlandia	Ripartizione per tipo di dati non fornita			4008
Svezia	Dati non forniti			
Regno Unito	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Totale				1392281

Tabella 9: Richieste di dati conservati relativi al traffico di *telefonia di rete fissa* trasmesse, per età, nel 2008									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	3669	916	143	124	0	0	0	0	4852
Danimarca	133	28	31	0	0	0	0	0	192
Germania	Dati non forniti								
Estonia	1876	161	74	484	0	0	0	0	2595
Irlanda	4118	712	197	182	32	21	23	16	5301
Grecia	Dati non forniti								
Spagna	1948	1431	741	328	0	0	0	0	4448
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	3	0	0	0	0	0	0	0	3
Lettonia	698	213	167	193	104	137	0	0	1512
Lituania	251	442	0	0	0	0	0	0	693
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	28	1	0	0	0	0	0	0	29
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	54805	27052	5340	753	1135	437	1050	175	90747
Totale	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Tabella 10: Richieste di dati conservati relativi al traffico di *telefonia mobile* trasmesse, per età, nel 2008									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	98232	17013	7518	1	0	0	0	0	122764
Danimarca	2433	628	143	33	20	1	7	3	3268
Germania	Dati non forniti								
Estonia	248	58	35	28	0	0	0	0	369
Irlanda	4326	820	230	240	57	63	52	37	5825
Grecia	Dati non forniti								
Spagna	17403	12114	7444	3052	0	0	0	0	40013
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	23	3	0	0	0	0	0	0	26
Lettonia	8928	2298	1085	746	394	257	0	0	13708
Lituania	55484	23375	14	20	0	0	0	0	78893
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	575	53	0	0	0	0	0	0	628
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	229375	52241	26228	16040	3333	521	339	1344	329421
Totale	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Tabella 11: Richieste di dati conservati relativi al traffico *via Internet* trasmesse, per età, nel 2008									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	737	412	137	168	0	0	0	0	1454
Danimarca	102	14	11	2	3	1	0	1	134
Germania	Dati non forniti								
Estonia	Dati non forniti								
Irlanda	492	460	498	1422	0	0	0	0	2872
Grecia	Dati non forniti								
Spagna	3278	2323	2113	1403	0	0	0	0	9117
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	0	0	0	0	0	0	0	0	0
Lettonia	424	150	75	219	74	34	0	0	976
Lituania	Dati non forniti								
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	76	3	0	0	0	0	0	0	79
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	31170	9046	3097	2605	1917	2015	147	57	50054
Totale	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Statistiche fornite dagli Stati membri per il 2009

Tabella 12: Richieste di dati conservati per età nel 2009									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	210975	56623	11620	1053	0	0	0	0	280271
Danimarca	2980	685	179	104	54	38	12	14	4066
Germania	Non fornito								
Estonia	4299	1836	1210	1065	0	0	0	0	8410
Irlanda	8117	1652	805	297	168	134	69	41	11283
Grecia	Dati non forniti								
Spagna	29775	19346	13999	6970	0	0	0	0	70090
Francia	Ripartizione per età non fornita								514813
Italia	Dati non forniti								
Cipro	31	8	1	0	0	0	0	0	40
Lettonia	20758	2414	1088	796	565	475	0	0	26096
Lituania	30247	35456	5886	884	0	0	0	0	72473
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	3336	362	151	174	0	0	0	0	4023
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Polonia	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovenia	Ripartizione per età non fornita								1918
Slovacchia	Ripartizione per età non fornita								5214
Finlandia	2000	1310	532	152	76	0	0	0	4070
Svezia	Dati non forniti								
Regno Unito	Dati non forniti								
Totale	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Tabella 13: Richieste di dati conservati per tipo di dati nel 2009 (tra parentesi numero di casi in cui non è stato possibile soddisfare le richieste di dati - se fornito)				
Tipo di dati / Stato membro	**Telefonia di rete fissa**	**Telefonia mobile**	**Internet**	**Totale**
Belgio	Dati non forniti			
Bulgaria	Dati non forniti			
Repubblica Ceca	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Danimarca	133 (0)	3771 (10)	162 (1)	4066 (11)
Germania	Dati non forniti			
Estonia	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irlanda	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grecia	Dati non forniti			
Spagna	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Francia	Ripartizione per tipo di dati non fornita			514813
Italia	Dati non forniti			
Cipro	0 (0)	23 (3)	14 (0)	40 (3)
Lettonia	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Lituania	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Lussemburgo	Dati non forniti			
Ungheria	Dati non forniti			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Paesi Bassi	Dati non forniti			
Austria	Dati non forniti			
Polonia	Ripartizione per tipo di dati non fornita			1048318
Portogallo	Dati non forniti			
Romania	Dati non forniti			
Slovenia	Ripartizione per tipo di dati non fornita			1918 (48)
Slovacchia	Ripartizione per tipo di dati non fornita			5214 (157)
Finlandia	Ripartizione per tipo di dati non fornita			4070
Svezia	Dati non forniti			
Regno Unito	Dati non forniti			
Totale				2051082 (1069885)

Tabella 14: Richieste di dati conservati relativi alla *telefonia di rete fissa* trasmesse, per età, nel 2009									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	9919	2907	47	36	0	0	0	0	12909
Danimarca	105	19	7	2	0	0	0	0	133
Germania	Dati non forniti								
Estonia	2254	866	599	424	0	0	0	0	4143
Irlanda	3934	337	69	70	50	39	16	11	4526
Grecia	Dati non forniti								
Spagna	2371	1492	844	348	0	0	0	0	5055
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	0	0	0	0	0	0	0	0	0
Lettonia	744	253	157	143	68	89	0	0	1454
Lituania	469	773	73	6	0	0	0	0	1321
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	83	25	18	20	0	0	0	0	146
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	Dati non forniti								
Totale	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Tabella 15: Richieste di dati conservati relativi alla *telefonia mobile* trasmesse, per età, nel 2009									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	197620	48841	472	0	0	0	0	0	246933
Danimarca	2777	639	162	98	47	19	12	7	3761
Germania	Dati non forniti								
Estonia	318	397	96	70	0	0	0	0	881
Irlanda	3669	835	220	210	115	92	50	28	5219
Grecia	Dati non forniti								
Spagna	24065	15648	11147	5273	0	0	0	0	56133
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	17	16	0	0	0	0	0	0	23
Lettonia	18832	1912	778	515	394	263	0	0	22694
Lituania	25713	19595	28	0	0	0	0	0	45336
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	2332	246	111	122	0	0	0	0	2811
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	Dati non forniti								
Totale	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Tabella 16: Richieste di dati conservati *relativi a Internet* trasmesse, per età, nel 2009									
Età dei dati richiesti (mesi) / Stato membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totale**
Belgio	Dati non forniti								
Bulgaria	Dati non forniti								
Repubblica Ceca	3369	4811	861	942	0	0	0	0	9983
Danimarca	98	27	10	4	4	7	0	1	151
Germania	Dati non forniti								
Estonia	315	145	56	102	0	0	0	0	618
Irlanda	489	455	502	0	0	0	0	0	1446
Grecia	Dati non forniti								
Spagna	3339	2206	2008	1349	0	0	0	0	8902
Francia	Dati non forniti								
Italia	Dati non forniti								
Cipro	12	2	0	0	0	0	0	0	14
Lettonia	852	198	74	90	88	86	0	0	1388
Lituania	4060	15087	1	88	0	0	0	0	19236
Lussemburgo	Dati non forniti								
Ungheria	Dati non forniti								
Malta	150	14	0	0	0	0	0	0	164
Paesi Bassi	Dati non forniti								
Austria	Dati non forniti								
Polonia	Dati non forniti								
Portogallo	Dati non forniti								
Romania	Dati non forniti								
Slovenia	Dati non forniti								
Slovacchia	Dati non forniti								
Finlandia	Dati non forniti								
Svezia	Dati non forniti								
Regno Unito	Dati non forniti								
Totale	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**