

Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta Decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Stefano Rodotà;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni del settore privato, aventi sede in Canada, nei cui confronti si applica la legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act") del 13 aprile 2000, in conformità a quanto previsto alla Decisione della Commissione europea del 20 dicembre 2001 n. 2002/2/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e all'art. 3 della Decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 30 aprile 2003

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

Decisione della Commissione del 20 dicembre 2001 conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ^(*) (2002/2/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ⁽¹⁾, in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) Conformemente alla direttiva 95/46/CE gli Stati membri sono tenuti ad operare affinché i trasferimenti di dati personali verso paesi terzi possano avvenire solo se il paese terzo in questione garantisce un livello adeguato di tutela e se, prima del trasferimento, viene rispettata la legislazione dello Stato membro che attua altre disposizioni della direttiva.

(2) La Commissione può constatare che un paese terzo garantisce un livello adeguato di tutela. In tal caso gli Stati membri vi possono trasferire dati personali senza richiedere ulteriori garanzie.

(3) Conformemente alla direttiva 95/46/CE, il livello di tutela dei dati deve essere valutato tenendo presenti tutte le circostanze in cui si svolgono le operazioni di trasferimento dei dati e tenendo conto di determinate condizioni. Il gruppo di lavoro sulla tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito indicazioni per effettuare tale valutazione ⁽²⁾.

(4) Data la diversità degli approcci alla protezione dei dati nei paesi terzi, è opportuno che la valutazione dell'adeguatezza avvenga e che ogni decisione, basata sull'articolo 25, § 6, della direttiva 95/46/CE, fosse presa ed attuata senza dar luogo a discriminazioni arbitrarie o ingiustificate verso o tra paesi terzi in cui esistono condizioni analoghe e senza dar luogo a barriere occulte per gli scambi commerciali, visti gli attuali impegni della Comunità a livello internazionale.

(5) La legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act") del 13 aprile 2000 ⁽³⁾ si applica a organizzazioni del settore privato che rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali. Essa entra in vigore in tre fasi:

Dal 1° gennaio 2001, la legge canadese si applica alle informazioni personali, purché non a carattere sanitario, rilevate, utilizzate o comunicate da organizzazioni quali imprese, stabilimenti o aziende federali. Questi tipi di organizzazioni sono presenti nel settore del trasporto aereo, bancario, radiotelevisivo, dei trasporti interprovinciali e delle telecomunicazioni. La legge canadese si applica anche a tutte le organizzazioni che comunicano dati personali dietro compenso al di fuori della provincia o del Canada e ai dati riguardanti i dipendenti di imprese, stabilimenti o aziende federali.

(*) Notificata con il numero C(2001) 4539.

(1) GU L 281 del 23.11.1995, pag. 31.

(2) WP 12: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva comunitaria sulla tutela dei dati, documento adottato dal Gruppo di lavoro il 24 luglio 1998, disponibile al seguente indirizzo:

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wpdocs_98.htm

(3) Electronically published (paper and web) versions of the Act are available at

http://www.parl.gc.ca/36/2/paribus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html and

http://www.parl.gc.ca/36/2/paribus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html. Printed versions are available at Public Works and Government Services Canada - Publishing, Ottawa, Canada K1A 0S9.

Dal 1° gennaio 2002 la legge canadese si applica anche alle informazioni riguardanti la salute personale per le organizzazioni e le attività già coperte nella prima fase.

Dal 1° gennaio 2004 la legge canadese si applica a tutte le organizzazioni, federali o non federali, che rilevano, utilizzano o comunicano dati personali nell'ambito di attività commerciali. La legge canadese non si applica a organizzazioni soggette al Federal Privacy Act o regolate dal settore pubblico a livello provinciale, alle organizzazioni caritatevoli e senza scopo di lucro a meno che non siano di natura commerciale. Analogamente, essa non copre dati sui lavoratori dipendenti usati per scopi non commerciali diversi da quelli relativi ai dipendenti del settore privato regolato a livello federale. Il "Canadian Federal Privacy Commissioner" (Autorità di vigilanza canadese sulla privacy) può fornire ulteriori informazioni in tali casi.

(6) Al fine di rispettare il diritto delle province di legiferare nei loro ambiti di competenza la legge prevede che, successivamente all'approvazione di leggi provinciali sostanzialmente simili, possa essere concessa un'esenzione alle organizzazioni o attività oggetto della legislazione provinciale sulla riservatezza dei dati. La sezione 26(2) della legge canadese sulla tutela delle informazioni personali e sui documenti elettronici autorizza il gabinetto federale (se constatata che la legislazione di una provincia, sostanzialmente simile alla presente parte, si applica a un'organizzazione, a una classe di organizzazioni, a un'attività o a una classe di attività) ad esentare l'organizzazione, l'attività o la classe dall'applicazione della presente parte per quanto riguarda la rilevazione, l'utilizzo o la comunicazione di informazioni personali nell'ambito di tale provincia. Il Governor in Council (gabinetto federale canadese) autorizza le esenzioni per legislazioni sostanzialmente simili tramite un Order-in-Council.

(7) Qualora una provincia adotti una legislazione sostanzialmente simile le organizzazioni, classi di organizzazioni o attività coperte saranno esentate dall'applicazione della legge federale per le transazioni all'interno della provincia; la legge federale continuerà invece ad essere applicata a tutte le attività di rilevazione, utilizzo e comunicazione di informazioni personali fra province nonché in tutte le situazioni per le quali le province non hanno previsto, integralmente o parzialmente, una legislazione sostanzialmente simile.

(8) Il 29 giugno 1984, il Canada ha aderito formalmente agli orientamenti dell'OCSE del 1980 sulla protezione della sfera privata e i flussi transfrontalieri di dati personali. Il Canada ha altresì sostenuto gli orientamenti delle Nazioni Unite riguardanti gli archivi elettronici di dati personali, adottati dall'Assemblea generale il 14 dicembre 1990.

(9) La legge canadese comprende tutti i principi fondamentali necessari a garantire un livello adeguato di protezione alle persone fisiche, contemplando però eccezioni e limitazioni per la salvaguardia di importanti interessi pubblici e per riconoscere determinate informazioni esistenti nel settore pubblico. L'applicazione di tali norme è garantita dai ricorsi giurisdizionali nonché dal controllo indipendente esercitato da autorità quali il commissario federale per la tutela della privacy (Federal Privacy Commissioner), al quale sono conferiti poteri di investigazione e intervento. Inoltre, ai casi di trattamento illecito dei dati con conseguenze pregiudizievoli per la persona, si applicano le norme di legge canadesi riguardanti la responsabilità civile.

(10) Per garantire la trasparenza e salvaguardare la capacità delle autorità competenti degli Stati membri di tutelare i cittadini per quanto riguarda il trattamento dei loro dati personali è necessario specificare nella presente decisione le circostanze eccezionali nelle quali la sospensione di determinati flussi di dati può essere giustificata, malgrado sia stato constatato un livello di protezione adeguato.

(11) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito un parere sul livello di protezione della legge canadese di cui si è tenuto conto nella preparazione della presente decisione.

(12) Le misure previste dalla presente decisione sono conformi al parere del comitato di cui all'articolo 31 della direttiva 95/46/CE,

(4) Parere 2/2001 sull'adeguatezza della legge canadese sulle informazioni personali e i documenti elettronici - WP 39 del 26 gennaio 2001, disponibile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE il Canada è ritenuto fornire un adeguato livello fornisca un livello adeguato di protezione ai dati personali trasferiti dalla Comunità a destinatari soggetti alla legge sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act").

Articolo 2

La presente decisione riguarda solo l'adeguatezza della protezione fornita in Canada dalla legge canadese, al fine di soddisfare i requisiti di cui all'articolo 25, paragrafo 1 della direttiva 95/46/CE e non produce alcun effetto su altre condizioni o restrizioni conseguenti all'attuazione di altre disposizioni della direttiva riguardanti il trattamento dei dati personali all'interno degli Stati membri.

Articolo 3

1. Fatti salvi i poteri di intervenire al fine di garantire il rispetto dei provvedimenti nazionali adottati in conformità delle disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri hanno la facoltà di sospendere flussi di dati verso destinatari in Canada le cui attività rientrano nel campo d'applicazione della legge canadese al fine di proteggere i cittadini nell'ambito del trattamento dei loro dati personali nei casi seguenti:

a) qualora un'autorità competente canadese abbia constatato che il destinatario non rispetta le norme applicabili relative alla protezione; oppure

b) qualora sussista una sostanziale probabilità di violazione delle norme relative alla protezione; qualora vi siano motivi ragionevoli di credere che le autorità competenti canadesi non stiano o non intendano adottare misure adeguate e tempestive per risolvere il caso in questione; se, continuando il trasferimento dei dati, si verrebbe a creare un rischio imminente di grave danneggiamento delle persone cui si riferiscono i dati e le autorità competenti degli Stati membri hanno fatto il possibile, date le circostanze, per avvertire il responsabile del trattamento in Canada, dando a quest'ultimo l'opportunità di replicare.

La sospensione cesserà non appena sarà garantito il rispetto delle norme di protezione e ne sarà stata data notifica all'autorità competente in questione nella Comunità.

2. Gli Stati membri informano la Commissione immediatamente dell'adozione di provvedimenti in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano reciprocamente anche dei casi in cui l'intervento degli organismi canadesi responsabili per il rispetto delle norme di protezione non riesce a garantire tale rispetto.

4. Se le informazioni rilevate in base ai paragrafi 1, 2 e 3 provano che gli organismi canadesi incaricati di garantire il rispetto delle norme di protezione non svolgono la loro funzione in modo efficace, la Commissione avverte le autorità canadesi competenti e, se necessario, presenta progetti di misure conformemente alla procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di abrogare o sospendere la presente decisione o limitarne il campo d'applicazione.

Articolo 4

1. La presente decisione può essere modificata in qualsiasi momento, alla luce delle esperienze relative al suo funzionamento o di modifiche della legislazione canadese, compresi provvedimenti che riconoscano che una provincia canadese dispone di una legislazione sostanzialmente simile. Tre anni dopo la notifica della presente decisione agli Stati membri la Commissione ne valuta il funzionamento in base alle informazioni disponibili; essa comunica qualsiasi elemento utile al comitato istituito dall'articolo 31 della direttiva 95/46/CE, inclusi quelli in grado di influire su quanto enunciato dall'articolo 1 della presente decisione in merito all'adeguatezza della protezione canadese ai sensi dell'articolo 25 della direttiva 95/46/CE e di provare l'esistenza di discriminazioni nell'attuazione della presente decisione.

2. Se necessario, la Commissione presenta progetti di misure conformemente alla procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 5

Gli Stati membri adottano tutte le misure necessarie per uniformarsi alla presente decisione entro novanta giorni dalla data di notifica della decisione stessa.

Articolo 6

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 20 dicembre 2001.

Per la Commissione
Frederik Bolkestein
Membro della Commissione

99

Provvedimento in materia di codici di deontologia e di buona condotta - 10 aprile 2002 (*)**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'art. 31, comma 1, lettera h), della citata legge n. 675/1996, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 28 dicembre 2001, n. 467, recante disposizioni integrative e correttive della normativa in materia di protezione dei dati personali ai sensi della legge 24 marzo 2001, n. 127, e in particolare l'art. 20, comma 1, il quale prevede che il Garante, al fine di garantire la piena attuazione dei principi previsti dalla disciplina in materia di trattamento dei dati personali deve promuovere entro il 30 giugno 2002 la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali nei settori indicati al comma 2 del medesimo articolo, tenendo conto della specificità dei trattamenti nei diversi ambiti, nonché dei criteri direttivi delle raccomandazioni del Consiglio d'Europa indicate nell'articolo 1, comma 1, lettera b), della legge n. 676/1996;

Considerato che il citato comma 2 dell'art. 20 del d.lg. n. 467/2001 prevede la sottoscrizione di codici riguardanti il trattamento di dati personali:

a) effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica (con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole ed interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 9 della legge n. 675/1996, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato);

b) necessari per finalità previdenziali o per la gestione del rapporto di lavoro (prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili);

c) effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva (prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni);

d) svolto a fini di informazione commerciale (prevedendo anche, in correlazione con quanto previsto dall'articolo 10, comma 4, della legge n. 675/1996, modalità semplificate per l'informativa all'interessato e idonei meccanismi per favorire la qualità e l'esattezza dei dati raccolti e comunicati);

e) effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di

(*) Pubblicato nella G.U. 8 maggio 2002, n. 106.

concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati (individuando anche specifiche modalità per favorire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato);

f) provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (anche individuando i casi in cui debba essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla raccomandazione del Consiglio d'Europa N. R (91) 10 in relazione all'articolo 9 della legge n. 675/1996);

g) effettuato con strumenti automatizzati di rilevazione di immagini (prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantirne la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 9 della legge n. 675/1996);

Considerato che, ai sensi dell'art. 20, comma 3, del d.lg. n. 467/2001, il rispetto delle disposizioni contenute nei codici deontologici sopra indicati costituisce condizione essenziale per la liceità del trattamento dei dati;

Considerato che, ai sensi dell'art. 20, comma 4, del d.lg. n. 467/2001, i codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e riportati in allegato al testo unico delle disposizioni in materia previsto dall'articolo 1, comma 4, della legge 24 marzo 2001, n. 127;

Considerata la necessità di adempiere alle predette disposizioni di legge osservando il principio di rappresentatività nell'ambito delle categorie coinvolte e di acquisire maggiori elementi di valutazione dai diversi soggetti potenzialmente interessati alla sottoscrizione di codici di deontologia e di buona condotta per determinati settori;

Ritenuta l'opportunità di conferire la massima pubblicità all'iniziativa del Garante e al procedimento per la sottoscrizione dei predetti codici di deontologia e di buona condotta anche attraverso la pubblicazione del presente provvedimento nella Gazzetta Ufficiale;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva, adottate dagli Stati membri;

Considerata la necessità che i codici su base nazionale siano adottati tenendo conto degli eventuali progetti di codici di condotta comunitari;

Riservata l'iniziativa di promuovere ulteriori codici di deontologia e di buona condotta in altri settori di rilevante interesse generale;

Visti gli atti d'ufficio e le richieste di soggetti pubblici e privati sinora pervenute;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000;

Relatore il prof. Stefano Rodotà;

TUTTO CIÒ PREMESSO IL GARANTE:

1. promuove la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali in relazione alle finalità ed ai criteri indicati dal citato art. 20 e richiamati in premessa, nei settori di seguito indicati:

a) trattamenti di dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica;

b) trattamenti di dati personali necessari per finalità previdenziali o per la gestione del rapporto di lavoro;

- c) trattamenti di dati personali effettuati a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva;
- d) trattamenti di dati personali svolti a fini di informazione commerciale;
- e) trattamenti di dati personali effettuati nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati;
- f) trattamenti di dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici;
- g) trattamenti di dati personali effettuati con strumenti automatizzati di rilevazione di immagini;

2. invita tutti i soggetti pubblici e privati aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività di cui all'art. 31, comma 1, lettera h), della legge n. 675/1996, a darne comunicazione a questa Autorità entro il 31 maggio 2002 al seguente indirizzo: Garante per la protezione dei dati personali, Piazza di Monte Citorio 121 - 00186 Roma – fax 06/69677715 - e-mail: codici@garanteprivacy.it;

3. riserva ad altri provvedimenti la verifica della conformità alle leggi e ai regolamenti dei progetti di codici, l'esame di eventuali osservazioni, nonché le iniziative necessarie ai sensi del citato art. 31, comma 1, lettera h), per garantirne la diffusione e il rispetto.

Roma, 10 aprile 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

Unione europea

100

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)(*)

Preambolo

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95,

vista la proposta della Commissione ¹,

visto il parere del Comitato economico e sociale ²,

visto il parere del Comitato delle regioni,

deliberando secondo la procedura di cui all'articolo 251 del trattato ³,

considerando quanto segue:

(1) La direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ⁴ richiede che gli Stati membri assicurino la tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali, e particolarmente del diritto alla vita privata, al fine di garantire il libero flusso dei dati personali nella Comunità.

(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(3) La riservatezza nelle comunicazioni è garantita conformemente agli strumenti internazionali relativi ai diritti dell'uomo, in particolare alla convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali e alle costituzioni degli Stati membri.

(4) La 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 ⁵ ha tradotto i principi enunciati dalla direttiva 95/46/CE in norme specifiche per il settore delle telecomunicazioni.

(*) Pubblicata nella G.U.C.E. L 201 del 31 luglio 2002.

(1) G.U. C 365 E del 19.12.2000, pag. 223.

(2) G.U. C 123 del 25.4.2001, pag. 53.

(3) Parere del Parlamento europeo del 13 novembre 2001, posizione comune del Consiglio del 28 gennaio 2002, decisione del Parlamento europeo del 30 maggio 2002, decisione del Consiglio del 25 giugno 2002.

(4) G.U. L 281 del 23.11.1995, pag. 31.

(5) GU L 24 del 30.1.1998, pag. 1.

La direttiva 97/66/CE deve essere adeguata agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate. Tale direttiva dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(5) Nelle reti pubbliche di comunicazione della Comunità è in atto l'introduzione di nuove tecnologie digitali avanzate che pongono esigenze specifiche con riguardo alla tutela dei dati personali e della vita privata degli utenti. Lo sviluppo della società dell'informazione è caratterizzato dall'introduzione di nuovi servizi di comunicazione elettronica. L'accesso alle reti digitali mobili è ormai a disposizione e alla portata di un vasto pubblico. Queste reti digitali hanno grandi capacità e possibilità di trattare i dati personali. Il positivo sviluppo transfrontaliero di questi servizi dipende in parte dalla fiducia che essi riscuotono presso gli utenti in relazione alla loro capacità di tutelare la loro vita privata.

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(8) Occorre armonizzare le disposizioni legislative, regolamentari e tecniche adottate dagli Stati membri in materia di tutela dei dati personali, della vita privata nonché del legittimo interesse delle persone giuridiche nel settore delle comunicazioni elettroniche affinché non sorgano ostacoli nel mercato interno delle comunicazioni elettroniche, ai sensi dell'articolo 14 del trattato. L'armonizzazione dovrebbe limitarsi alle prescrizioni necessarie per garantire che non vengano ostacolate la promozione e lo sviluppo di nuovi servizi e reti di comunicazione elettronica tra Stati membri.

(9) È opportuno che gli Stati membri, i fornitori e gli utenti interessati, come pure gli organi comunitari competenti, cooperino all'introduzione e allo sviluppo delle tecnologie pertinenti laddove ciò sia necessario per realizzare le garanzie previste dalla presente direttiva, tenuto debito conto dell'obiettivo di ridurre al minimo il trattamento dei dati personali e di utilizzare dati anonimi o pseudonimi nella misura del possibile.

(10) Nel settore delle comunicazioni elettroniche trova applicazione la direttiva 95/46/CE, in particolare per quanto riguarda tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali non specificamente disciplinati dalle disposizioni della presente direttiva, compresi gli obblighi del responsabile e i diritti delle persone fisiche. La direttiva 95/46/CE si applica ai servizi di comunicazione non accessibili al pubblico.

(11) La presente direttiva, analogamente alla direttiva 95/46/CE, non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precisata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(12) Gli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico possono essere persone fisiche o persone giuridiche. La presente direttiva, integrando la direttiva 95/46/CE, è volta a tutelare i diritti fondamentali delle persone fisiche e in particolare il loro diritto alla vita privata, nonché i legittimi interessi delle persone giuridiche. La presente direttiva non comporta in alcun caso per gli Stati membri l'obbligo di estendere l'applicazione della direttiva 95/46/CE alla tutela dei legittimi interessi delle persone giuridiche, tutela che è assicurata nel quadro della vigente normativa comunitaria e nazionale.

(13) Il rapporto contrattuale tra abbonato e fornitore di servizi può comportare un versamento unico o periodico per il servizio fornito o che deve essere fornito. Anche le schede prepagate sono considerate un contratto.

(14) I dati relativi all'ubicazione possono riferirsi alla latitudine, longitudine ed altitudine dell'apparecchio terminale dell'utente, alla direzione di viaggio, al livello di accuratezza dell'informazione sull'ubicazione, all'identificazione della cella di rete in cui l'apparecchio terminale è ubicato in un determinato momento, e al momento in cui l'informazione sull'ubicazione è stata registrata.

(15) Una comunicazione può comprendere qualsiasi informazione relativa al nome, al numero e all'indirizzo fornita da chi emette la comunicazione o dall'utente di un collegamento al fine di effettuare la comunicazione. I dati relativi al traffico possono comprendere qualsiasi traslazione dell'informazione da parte della rete sulla quale la comunicazione è trasmessa allo scopo di effettuare la trasmissione. I dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento. Possono anche consistere nel formato in cui la comunicazione è trasmessa dalla rete.

(16) Le informazioni trasmesse nel quadro di un servizio di radiodiffusione tramite una rete di comunicazione pubblica sono destinate a un pubblico potenzialmente illimitato e non costituiscono una comunicazione ai sensi della presente direttiva. Comunque, nei casi in cui il singolo abbonato o utente che riceve tali informazioni possa essere identificato, per esempio con servizi video on demand, le informazioni trasmesse rientrano nella nozione di comunicazione ai sensi della presente direttiva.

(17) Ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46/CE. Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet.

(18) Servizi a valore aggiunto possono consistere ad esempio in consigli sui pacchetti tariffari meno costosi, orientamento stradale, informazioni sul traffico, previsioni meteorologiche, e informazioni turistiche.

(19) L'applicazione di taluni requisiti relativi alla presentazione ed alla restrizione dell'identificazione della linea chiamante e collegata e al trasferimento automatico di chiamate a linee collegate a centrali analogiche non dovrebbe essere resa obbligatoria in casi specifici in cui tale applicazione risulti essere tecnicamente impossibile o richieda uno sforzo economico sproporzionato. È importante che le parti interessate siano informate di tali casi e che gli Stati membri li notifichino alla Commissione.

(20) I fornitori di servizi dovrebbero adottare misure appropriate per salvaguardare la sicurezza dei servizi da essi offerti, se necessario congiuntamente al fornitore della rete, e dovrebbero informare gli abbonati sui particolari rischi di violazione della sicurezza della rete. Tali rischi possono presentarsi segnatamente per i servizi di comunicazione elettronica su una rete aperta come l'Internet o la telefonia mobile analogica. È di particolare importanza per gli utenti e gli abbonati di tali servizi essere pienamente informati dal loro fornitore di servizi dell'esistenza di rischi alla sicurezza al di fuori della portata dei possibili rimedi esperibili dal fornitore stesso. I fornitori di servizi che offrono servizi di comunicazione elettronica accessibili al pubblico su Internet dovrebbero informare gli utenti e gli abbonati delle misure che questi ultimi possono prendere per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di pro-

grammi o tecniche di criptaggio. L'obbligo di informare gli abbonati su particolari rischi relativi alla sicurezza non esonera il fornitore di servizi dall'obbligo di prendere, a sue proprie spese, provvedimenti adeguati ed immediati per rimediare a tutti i nuovi, imprevisi rischi relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio. La fornitura all'abbonato di informazioni sui rischi relativi alla sicurezza dovrebbe essere gratuita fatta eccezione per i costi nominali che l'abbonato può sostenere quando riceve o prende conoscenza delle informazioni, per esempio scaricando un messaggio di posta elettronica. La sicurezza viene valutata alla luce dell'articolo 17 della direttiva 95/46/CE.

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

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione. Ove ciò sia necessario per rendere più efficiente l'inoltro di tutte le informazioni accessibili al pubblico ad altri destinatari del servizio su loro richiesta, la presente direttiva non osta a che tali informazioni possano essere ulteriormente memorizzate, a condizione che esse siano in ogni caso accessibili al pubblico senza restrizioni e che tutti i dati che si riferiscono ai singoli abbonati o utenti che richiedono tali informazioni siano cancellati.

(23) La riservatezza delle comunicazioni dovrebbe essere assicurata anche nel quadro di legittime prassi commerciali. Ove necessario e legalmente autorizzato, le comunicazioni possono essere registrate allo scopo di fornire la prova di una transazione commerciale. La direttiva 95/46/CE si applica a tale trattamento. Le parti in comunicazione dovrebbero essere informate sulla registrazione, il suo scopo e la durata della sua memorizzazione preventivamente alla stessa. La comunicazione registrata dovrebbe essere cancellata non appena possibile ed in ogni caso non oltre la fine del periodo durante il quale la transazione può essere impugnata legittimamente.

(24) Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza.

(25) Tuttavia, tali dispositivi, per esempio i cosiddetti marcatori ("cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di

comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi.

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati che il fornitore dei servizi di comunicazione elettronica accessibili al pubblico volesse effettuare per la commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione o per la fornitura di servizi a valore aggiunto dovrebbero inoltre essere cancellati o resi anonimi dopo che il servizio è stato fornito. I fornitori dei servizi dovrebbero informare sempre i loro abbonati riguardo alla natura dei dati che stanno sottoponendo a trattamento, nonché agli scopi e alla durata del trattamento stesso.

(27) Il momento esatto del completamento della trasmissione di una comunicazione, dopo il quale i dati relativi al traffico dovrebbero essere cancellati salvo ai fini di fatturazione, può dipendere dal tipo di servizio di comunicazione elettronica che è fornito. Per esempio per una chiamata di telefonia vocale la trasmissione sarà completata quando uno dei due utenti termina il collegamento. Per la posta elettronica la trasmissione è completata quando il destinatario prende conoscenza del messaggio, di solito dal server del suo fornitore di servizi.

(28) L'obbligo di cancellare o di rendere anonimi i dati relativi al traffico quando non sono più necessari ai fini della trasmissione di una comunicazione non contraddice le procedure utilizzate su Internet, come la realizzazione di copie "cache", nel sistema dei nomi di dominio, di indirizzi IP o la realizzazione di copie "cache" di un indirizzo IP legato ad un indirizzo fisico o l'uso di informazioni riguardanti l'utente per controllare il diritto d'accesso a reti o servizi.

(29) Il fornitore di servizi può trattare i dati sul traffico relativi agli abbonati ed agli utenti ove necessario in singoli casi per individuare problemi tecnici od errori materiali nella trasmissione delle comunicazioni. I dati relativi al traffico necessari ai fini della fatturazione possono anche essere sottoposti a trattamento da parte del fornitore per accertare e sospendere la frode che consiste nell'uso del servizio di comunicazione elettronica senza il corrispondente pagamento.

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari. Tutte le attività relative alla fornitura del servizio di comunicazione elettronica che va oltre la trasmissione di una comunicazione e la relativa fatturazione dovrebbero essere basate su dati relativi al traffico aggregati che non possono essere collegati agli abbonati o utenti. Tali attività, se non possono essere basate su dati aggregati, dovrebbero essere considerate come servizi a valore aggiunto per i quali è necessario il consenso dell'abbonato.

(31) Si stabilirà se il consenso necessario per il trattamento dei dati personali per fornire un particolare servizio a valore aggiunto debba essere ottenuto dall'utente o dall'abbonato in base ai dati che devono essere trattati e al tipo di servizio da fornire nonché alla possibilità tecnica, procedurale e contrattuale di distinguere l'individuo che usa un servizio di comunicazione elettronica dalla persona giuridica o fisica che si è abbonata.

(32) Se il fornitore di un servizio di comunicazione elettronica o di un servizio a valore aggiunto fa ricorso a forme di subappalto a un'altra impresa per il trattamento dei dati personali necessari per la fornitura di tali servizi, questo subappalto ed il conseguente trattamento dei dati dovrebbe essere nella piena

osservanza delle disposizioni relative ai responsabili e agli incaricati del trattamento e dei dati personali come riportato nella direttiva 95/46/CE. Se la fornitura di un servizio a valore aggiunto richiede che i dati relativi al traffico o all'ubicazione siano inviati da un fornitore di servizi di comunicazione elettronica a un fornitore di servizi a valore aggiunto, gli abbonati o utenti a cui i dati si riferiscono dovrebbero essere pienamente informati di questo invio prima di dare il loro consenso al trattamento dei dati.

(33) L'introduzione di fatture dettagliate ha aumentato le possibilità dell'abbonato di verificare l'esattezza delle somme addebitate dal fornitore del servizio ma, al tempo stesso, può mettere in pericolo la vita privata degli utenti dei servizi di comunicazione elettronica accessibili al pubblico. Pertanto, per tutelare la vita privata degli utenti, gli Stati membri dovrebbero incoraggiare lo sviluppo di opzioni per i servizi di comunicazione elettronica, quali possibilità alternative di pagamento che permettano un accesso anonimo o rigorosamente privato ai servizi di comunicazione elettronica accessibili al pubblico, per esempio carte telefoniche o possibilità di pagamento con carta di credito. Allo stesso scopo, gli Stati membri possono chiedere agli operatori di offrire ai loro abbonati un tipo diverso di fattura dettagliata, dalla quale è stato omissso un certo numero di cifre dei numeri chiamati.

(34) Con riguardo all'identificazione della linea chiamante è necessario tutelare il diritto dell'autore della chiamata di eliminare l'indicazione della linea dalla quale si effettua la chiamata, nonché il diritto del chiamato di respingere chiamate da linee non identificate. In casi specifici esistono giustificati motivi per disattivare la soppressione dell'indicazione della linea chiamante. Alcuni abbonati, in particolare le linee di assistenza e servizi analoghi, hanno interesse a garantire l'anonimato dei loro chiamanti. Con riferimento all'identificazione della linea collegata, è necessario tutelare il diritto e il legittimo interesse del chiamato a sopprimere l'indicazione della linea alla quale il chiamante è realmente collegato, in particolare in caso di chiamate trasferite. I fornitori di servizi di comunicazione elettronica accessibili al pubblico dovrebbero informare i loro abbonati dell'esistenza nella rete dell'indicazione della linea chiamante e collegata, nonché di tutti i servizi offerti in base all'identificazione della linea chiamante e collegata, come pure delle opzioni disponibili per la salvaguardia della vita privata. Ciò permetterà agli abbonati di operare una scelta consapevole in merito alle possibilità di cui desiderano avvalersi a tutela della loro vita privata. Le opzioni per la salvaguardia della vita privata offerte linea per linea non devono necessariamente essere disponibili come servizio di rete automatico, ma possono configurarsi come un servizio disponibile su richiesta rivolta al fornitore del servizio di comunicazione elettronica accessibile al pubblico.

(35) Nelle reti mobili digitali i dati relativi all'ubicazione, che consentono di determinare la posizione geografica dell'apparecchiatura terminale dell'utente mobile vengono sottoposti a trattamento in modo da consentire la trasmissione di comunicazioni. Tali dati sono quelli relativi al traffico di cui all'articolo 6 della presente direttiva. Tuttavia, in aggiunta ad essi, le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Il trattamento di dati siffatti ai fini della fornitura di servizi a valore aggiunto dovrebbe essere autorizzato soltanto previo esplicito consenso dell'abbonato. Anche in questo caso, tuttavia, gli abbonati dovrebbero disporre, gratuitamente, di un mezzo semplice per bloccare temporaneamente il trattamento dei dati relativi alla loro ubicazione.

(36) Gli Stati membri possono limitare il diritto alla vita privata degli utenti e degli abbonati riguardo all'identificazione della linea chiamante allorché ciò sia necessario per identificare le chiamate importune, e riguardo all'identificazione della linea chiamante e ai dati relativi all'ubicazione allorché ciò sia necessario per consentire ai servizi di emergenza di svolgere il loro compito nel modo più efficace possibile. A tale scopo gli Stati membri possono adottare disposizioni specifiche per autorizzare i fornitori di servizi di comunicazione elettronica a fornire l'accesso all'identificazione della linea chiamante e ai dati relativi all'ubicazione senza il previo consenso degli utenti o abbonati interessati.

(37) Occorre prevedere misure per tutelare gli abbonati dal disturbo che può essere causato dal trasferimento automatico di chiamate da parte di altri. Inoltre, in tali casi, l'abbonato deve avere la possibilità di impedire che le chiamate trasferite siano inoltrate sul suo terminale, mediante una semplice richiesta al fornitore del servizio di comunicazione elettronica accessibile al pubblico.

(38) Gli elenchi degli abbonati ai servizi di comunicazione elettronica sono pubblici ed ampiamente distribuiti. Il rispetto della vita privata delle persone fisiche e i legittimi interessi delle persone giuridiche postulant, per gli abbonati, il diritto di determinare se i loro dati personali possano essere pubblicati in un elenco e, in caso affermativo, quali. È opportuno che i fornitori di elenchi pubblici informino gli abbonati che vi figureranno degli scopi dell'elenco stesso e di ogni specifico impiego che possa essere fatto delle versioni elettroniche degli elenchi pubblici, in particolare mediante le funzioni di ricerca incorporate nel software, come ad esempio le funzioni di ricerca inversa che consentono agli utenti dell'elenco di risalire al nome e all'indirizzo dell'abbonato in base al solo numero telefonico.

(39) L'obbligo di informare gli abbonati sugli scopi di elenchi pubblici in cui i loro dati personali devono essere inclusi dovrebbe essere imposto alla parte che raccoglie i dati per tale inclusione. Se i dati possono essere trasmessi a uno o più terzi, l'abbonato dovrebbe essere informato su questa possibilità e sul ricevente o sulle categorie di possibili riceventi. Le trasmissioni dovrebbero essere soggette alla condizione che i dati non possono essere usati per scopi diversi da quelli per cui sono stati raccolti. Se la parte che raccoglie i dati dall'abbonato o i terzi a cui i dati sono stati trasmessi desiderano usarli per uno scopo ulteriore, la parte che ha raccolto i dati in origine o il terzo a cui i dati sono stati trasmessi deve ottenere nuovamente il consenso dell'abbonato.

(40) Occorre prevedere misure per tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta, in particolare mediante dispositivi automatici di chiamata, telefax o posta elettronica, compresi i messaggi SMS. Tali forme di comunicazioni commerciali indesiderate possono da un lato essere relativamente facili ed economiche da inviare e dall'altro imporre un onere e/o un costo al destinatario. Inoltre, in taluni casi il loro volume può causare difficoltà per le reti di comunicazione elettronica e le apparecchiature terminali. Per tali forme di comunicazioni indesiderate a scopo di commercializzazione diretta è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi. Il mercato unico prevede un approccio armonizzato per garantire norme semplici a livello comunitario per le aziende e gli utenti.

(41) Nel contesto di una relazione di clientela già esistente è ragionevole consentire l'uso delle coordinate elettroniche per offrire prodotti o servizi analoghi, ma unicamente da parte della medesima società che ha ottenuto le coordinate elettroniche a norma della direttiva 95/46/CE. Allorché tali coordinate sono ottenute, il cliente dovrebbe essere informato sul loro uso successivo a scopi di commercializzazione diretta in maniera chiara e distinta, ed avere la possibilità di rifiutare tale uso. Tale opportunità dovrebbe continuare ad essere offerta gratuitamente per ogni successivo messaggio a scopi di commercializzazione diretta, ad eccezione degli eventuali costi relativi alla trasmissione del suo rifiuto.

(42) Altre forme di commercializzazione diretta che siano più onerose per il mittente e non impongano costi finanziari per gli abbonati e gli utenti, quali chiamate telefoniche vocali interpersonali, possono giustificare il mantenimento di un sistema che dà agli abbonati o agli utenti la possibilità di indicare che non desiderano ricevere siffatte chiamate. Ciò nondimeno, al fine di non ridurre i livelli di tutela della vita privata esistenti, gli Stati membri dovrebbero essere autorizzati a mantenere sistemi nazionali che autorizzano tali chiamate unicamente destinate agli abbonati e agli utenti che hanno fornito il loro consenso preliminare.

(43) Al fine di facilitare l'attuazione efficace delle norme comunitarie in materia di messaggi indesiderati a scopi di commercializzazione diretta, occorre proibire l'uso di false identità o falsi indirizzi o numeri di risposta allorché sono inviati messaggi indesiderati a scopi di commercializzazione diretta.

(44) Taluni sistemi di posta elettronica consentono agli abbonati di vedere il mittente e l'oggetto di una e-mail e, inoltre, di cancellare il messaggio senza dover scaricare il resto del contenuto dell'e-mail o degli allegati, riducendo quindi i costi che potrebbero derivare dallo scaricamento di e-mail o allegati indesiderati. Queste modalità possono continuare ad essere utili in taluni casi come strumento supplementare rispetto ai requisiti generali stabiliti dalla presente direttiva.

(45) La presente direttiva non pregiudica le misure che gli Stati membri prendono per tutelare legittimi interessi delle persone giuridiche in relazione a comunicazioni indesiderate a scopo di commercializzazione diretta. Allorquando gli Stati membri costituiscono un registro "opt-out" per siffatte chiamate a persone giu-

ridiche, principalmente imprese, sono pienamente applicabili le disposizioni dell'articolo 7 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ⁶ (direttiva sul commercio elettronico).

(46) Le funzionalità necessarie per la fornitura di servizi di comunicazione elettronica possono essere incorporate nella rete o in una parte qualsiasi dell'apparecchiatura terminale dell'utente, compreso il software. La tutela dei dati personali e della vita privata dell'utente di servizi di comunicazione elettronica accessibili al pubblico dovrebbe essere indipendente dalla configurazione delle varie componenti necessarie a fornire il servizio e dalla distribuzione delle necessarie funzionalità tra queste componenti. La direttiva 95/46/CE contempla tutti i tipi di trattamento dei dati personali, indipendentemente dalla tecnologia utilizzata. L'esistenza di norme specifiche per i servizi di comunicazione elettronica, oltre che di norme generali per le altre componenti necessarie per la fornitura di tali servizi, non sempre agevola la tutela dei dati personali e della vita privata in modo tecnologicamente neutrale. Può essere pertanto necessario adottare provvedimenti che prescrivano ai fabbricanti di taluni tipi di apparecchiature impiegate per i servizi di comunicazione elettronica di costruire il loro prodotto in modo da incorporarvi dispositivi che garantiscano la tutela dei dati personali e della vita privata dell'utente e dell'abbonato. L'adozione di tali provvedimenti a norma della direttiva 1999/5/CE del Parlamento europeo e del Consiglio, del 9 marzo 1999, riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità ⁷, avrà l'effetto di armonizzare l'introduzione nelle apparecchiature di comunicazione elettronica di determinate caratteristiche tecniche, compresi i software, volte a tutelare i dati secondo modalità compatibili con il buon funzionamento del mercato unico.

(47) La normativa nazionale dovrebbe prevedere la possibilità di adire gli organi giurisdizionali, nei casi in cui i diritti degli utenti e degli abbonati non siano rispettati. Si dovrebbero applicare sanzioni ad ogni persona, sia essa soggetta al diritto pubblico o privato, che non ottemperi alle disposizioni nazionali adottate a norma della presente direttiva.

(48) Nel campo di applicazione della presente direttiva è opportuno ricorrere all'esperienza del "gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali", composto dai rappresentanti delle autorità nazionali di controllo degli Stati membri, istituito dall'articolo 29 della direttiva 95/46/CE.

(49) Allo scopo di agevolare l'osservanza della presente direttiva, sono necessarie alcune disposizioni specifiche per il trattamento dei dati già in corso alla data di entrata in vigore delle disposizioni nazionali emanate in attuazione alla presente direttiva,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1 - Finalità e campo d'applicazione

1. La presente direttiva armonizza le disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

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

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benes-

(6) G.U. L 178 del 17.7.2000, pag. 1.

(7) G.U. L 91 del 7.4.1999, pag. 10.