



Comunicazioni elettroniche

Sicurezza, riservatezza, spamming

**La Direttiva 2002/58/CE
relativa al trattamento dei dati personali e alla tutela della vita
privata nel settore delle comunicazioni elettroniche**

iusreporter.it ebook

di **[Giuseppe Briganti](mailto:avv.briganti@iusreporter.it)**
avv.briganti@iusreporter.it
© 2002 Giuseppe Briganti
www.iusreporter.it



SOMMARIO

1. Premessa
2. Campo di applicazione della direttiva 2002/58/CE e definizioni
3. Sicurezza
4. Riservatezza
 - 4.1. Spyware, web bugs e cookies
5. Segue: dati relativi al traffico
6. Segue: dati relativi all'ubicazione diversi dai dati relativi al traffico
7. Segue: fatturazione dettagliata, identificazione della linea chiamante, trasferimento automatico della chiamata, elenchi di abbonati
8. Le comunicazioni indesiderate (*unsolicited communications*)
 - 8.1. La disciplina attuale (art. 10 D.L.vo 171/1998)
 - 8.2. Le nuove regole: l'art. 13 della direttiva 2002/58/CE
 - 8.3. L'art. 7 della direttiva sul commercio elettronico (direttiva 2000/31/CE)

1. Premessa

Con la [direttiva 2002/58/CE](#) del 12 luglio 2002¹, il legislatore europeo ha inteso disciplinare il trattamento dei dati personali e tutelare la vita privata nello specifico settore delle *comunicazioni elettroniche*².

¹ 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)*, GUCE L 201 del 31 luglio 2002.

La direttiva è entrata in vigore il giorno stesso della sua pubblicazione nella Gazzetta ufficiale delle Comunità europee (art. 20 del provvedimento).

² Così il Garante per la protezione dei dati personali presenta la direttiva 2002/58/CE (*Newsletter 29 luglio – 4 agosto 2002*, www.garanteprivacy.it):

“Maggiore privacy per telefonia ed Internet dal Parlamento europeo. Conferma europea delle scelte già operate dal legislatore italiano per l’invio di e-mail commerciali e pubblicitarie solo agli utenti che abbiano espresso il proprio consenso. Divieto di inviare messaggi di posta elettronica, a scopo di *direct marketing*, omettendo o camuffando l’identità del mittente o senza l’indicazione di un indirizzo valido, cui il destinatario possa inviare una richiesta di cessazione. Regolamentazione dell’uso di *cookies*, *spyware* e *bug*. Particolare tutela per i dati relativi alla localizzazione dei cellulari raccolti nel corso della fornitura di nuovi tipi di servizi erogati da reti cellulari e satellitari che consentono di individuare esattamente l’apparecchiatura terminale dell’utente. Iscrizione negli elenchi telefonici pubblici, cartacei o elettronici, solo con il consenso degli abbonati e secondo modalità da loro scelte. Queste in sintesi le principali novità introdotte dalla nuova direttiva europea relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, entrata in vigore il 31 luglio 2002, giorno della sua pubblicazione sulla Gazzetta ufficiale delle Comunità europee (Direttiva n.2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002). Gli Stati membri dovranno conformarsi alle nuove disposizioni europee entro il 31 ottobre 2003.

La nuova direttiva sostituisce la 97/66/CE (attuata in Italia con il decreto legislativo 171 del 1998) mantenendo elevato il livello di protezione dei dati personali e della vita privata da questa garantito.

Il nuovo testo riprende infatti una buona parte delle disposizioni della direttiva vigente apportando variazioni indispensabili per tener conto degli sviluppi intervenuti nei servizi e nelle tecnologie delle comunicazioni elettroniche. L’adeguamento permetterà così a utenti e consumatori di godere effettivamente di uno stesso livello di tutela, qualunque sia la tecnologia - digitale o analogica - utilizzata per la fornitura del servizio (definito non più di telecomunicazioni ma più correttamente di comunicazioni elettroniche).

La necessità di adeguare la vecchia direttiva 97/66/CE - sottolinea il Parlamento europeo - nasce dagli sviluppi che si sono verificati nei mercati e nelle tecnologie dei servizi di comunicazione elettronica tenendo conto che l’accesso ad Internet apre nuove possibilità agli utenti, ma rappresenta anche nuovi pericoli per i loro dati personali e per la loro vita privata. Analogamente l’uso di software spia (*spyware*), o di banchi invisibili (*web bug*), che possono introdursi nel terminale e permettere di accedere illecitamente e in modo non trasparente ad informazioni, o di seguire gli spostamenti in rete dell’utente, può rappresentare una grave intrusione nella vita privata e deve essere consentito unicamente per scopi legittimi e informando previamente l’interessato.

Nella direttiva si sollecita inoltre la progettazione di sistemi di fornitura di reti e servizi di comunicazione che limitino al minimo la quantità di dati personali necessari. Si prevede che i dati dei naviganti in Internet possano essere conservati dopo l’erogazione del servizio per il quale sono stati forniti, al pari di quelli delle chiamate telefoniche, ai fini della fatturazione e del pagamento per interconnessione.

Ogni ulteriore trattamento deve essere autorizzato dall’abbonato. Ad esempio se il provider vuole commercializzare altri prodotti o fornire servizi a valore aggiunto (orientamento stradale, previsioni meteorologiche, informazioni tariffarie o turistiche) deve raccogliere uno specifico consenso del cliente.

A quanto si legge nel considerando 6 del provvedimento, “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”.

Si è reso di conseguenza necessario, secondo il legislatore europeo, adeguare la direttiva 97/66/CE³, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni – attuata in Italia con il [D.L.vo 171/1998](#)⁴ – agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, così 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 (considerando 4 della direttiva 2002/58/CE).

La direttiva in esame prevede pertanto l'espressa abrogazione della suddetta direttiva 97/66/CE, sostituendosi ad essa (art. 19)⁵.

In questo quadro, il provvedimento si propone di armonizzare le disposizioni degli Stati membri nella misura necessaria per assicurare un livello equivalente di tutela

Per quanto riguarda il settore della telefonia la direttiva conferma il principio generale, già affermato nella 97/66/CE, che i dati sul traffico dell’utente devono essere cancellati o resi anonimi al termine della comunicazione. Permette comunque, entro precisi limiti e sulla base di determinate garanzie, la possibilità di introdurre delimitati tempi di conservazione laddove vi siano necessità di interventi proporzionali per finalità di accertamento e prevenzione di reati o motivi di sicurezza nazionale”.

³ GUCE L 24 del 30 gennaio 1998.

⁴ D.L.vo 13 maggio 1998, n. 171, *Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica*, GU Serie gen. 127 del 3 giugno 1998.

⁵ Ai sensi dell’art. 19 del provvedimento, la direttiva 97/66/CE è abrogata con efficacia a decorrere dalla data di applicazione di cui all’art. 17, par. 1.

L’art. 17, par. 1, della direttiva in esame stabilisce che gli Stati membri mettano in vigore le disposizioni necessarie per conformarsi ad essa entro il 31 ottobre 2003.

I riferimenti alla direttiva abrogata dovranno, da tale data, intendersi operati alla direttiva 2002/58/CE (art. 19, par. 2).

L’art. 18 della direttiva 2002/58/CE prevede inoltre che la Commissione presenti al Parlamento europeo e al Consiglio, non oltre tre anni dalla data di cui all’art. 17, par. 1, una relazione sull’applicazione della direttiva e il relativo impatto sugli operatori economici e sui consumatori, in particolare per quanto riguarda le disposizioni sulle comunicazioni indesiderate, tenendo conto dell’ambiente internazionale.

Ove opportuno, la Commissione potrà presentare proposte di modifica del provvedimento, tenendo conto dei risultati di detta relazione, di ogni modifica del settore e di ogni altra proposta che ritenga necessaria per migliorare l’efficacia della direttiva.

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 (art. 1, par. 1)⁶.

La direttiva 2002/58/CE sulle comunicazioni elettroniche si compone di un preambolo (considerando 1-49) e di 21 articoli, le cui disposizioni verranno analizzate nel prosieguo⁷.

Sommario

2. Campo di applicazione della direttiva 2002/58/CE e definizioni

Le disposizioni della direttiva sulle comunicazioni elettroniche *precisano ed integrano le disposizioni contenute nella direttiva 95/46/CE*⁸, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, attuata in Italia con la nota [legge 675/1996](#)⁹ (art. 1, par. 2).

Esse inoltre prevedono la tutela dei legittimi interessi degli abbonati persone giuridiche¹⁰.

La direttiva 95/46/CE continuerà comunque a trovare applicazione nell'ambito delle comunicazioni elettroniche, in particolare per quanto riguarda tutti gli aspetti relativi

⁶ L'art. 14, par. 1, della direttiva in esame prevede che – salvo il disposto dei paragrafi 2 e 3 del medesimo articolo – nell'attuare le disposizioni del provvedimento gli Stati membri assicurino che non siano imposti, per i terminali o altre apparecchiature di comunicazione elettronica, norme inderogabili relative a caratteristiche tecniche specifiche che possano ostacolare l'immissione sul mercato e la libera circolazione di tali apparecchiature tra i vari Stati membri e al loro interno.

⁷ In generale, sulle principali novità introdotte dalla direttiva in esame, si veda M. Cammarata, *Qualcosa si muove contro "spamatori" e spioni*, in InterLex, www.interlex.it, www.interlex.it/675/qualcosa.htm; P. Morelli, *Privacy e comunicazioni elettroniche: le principali novità della Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio*, in NetJus, www.netjus.org, www.netjus.org/pages/page.asp?article=159.

⁸ GUCE L 281 del 23 novembre 1995.

⁹ Legge 31 dicembre 1996, n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, GU Serie gen. 5 dell'8 gennaio 1997.

La legge è stata recentemente modificata ed integrata dal D.L.vo 467/2001. Si rimanda in proposito al mio scritto *Modifiche ed integrazioni alla legge sulla privacy* in Iusreporter, www.iusreporter.it, www.iusreporter.it/Testi/doc-privacy.htm.

¹⁰ Ciò non comporta, d'altra parte, l'obbligo per gli Stati membri di estendere l'applicazione della direttiva 95/46/CE alla tutela dei legittimi interessi delle persone giuridiche, tutela che rimane assicurata nel quadro della vigente normativa comunitaria e nazionale (considerando 12).

Occorre ricordare a questo proposito che, nell'ordinamento italiano, la [legge 675/1996](#), di attuazione della direttiva 95/46/CE, già ricomprende tra i soggetti tutelati, oltre le persone fisiche, anche le persone giuridiche, gli enti e le associazioni cui si riferiscono i dati personali (art. 1, lett. f)).

alla tutela dei diritti e delle libertà fondamentali non specificamente disciplinati dalla direttiva in esame, compresi gli obblighi del responsabile del trattamento dei dati e i diritti delle persone fisiche (considerando 10)¹¹.

A questo proposito, l'art. 15, par. 2, del provvedimento sulle comunicazioni elettroniche stabilisce che le disposizioni del capo III della direttiva 95/46/CE concernenti *i ricorsi giurisdizionali, le responsabilità e le sanzioni* si applichino relativamente alle disposizioni nazionali adottate in base alla direttiva 2002/58/CE e con riguardo ai diritti individuali risultanti dalla stessa.

Ai sensi dell'art. 3, par. 1, le disposizioni della direttiva 2002/58/CE si applicano specificamente al *trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità*¹².

Ai fini del provvedimento, trovano applicazione le definizioni contenute nella direttiva 95/46/CE¹³ e nella recente [direttiva 2002/21/CE](#)¹⁴, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (c.d. direttiva quadro).

Si ricordano in particolare le seguenti definizioni date dalla direttiva quadro:

¹¹ Si specifica inoltre che la direttiva 95/46/CE è applicabile ai servizi di comunicazione non accessibili al pubblico (considerando 10).

¹² Gli articoli 8 (“Presentazione e restrizione dell’identificazione della linea chiamante e collegata”), 10 (“Deroghe”) e 11 (“Trasferimento automatico della chiamata”) del provvedimento in esame si applicano alle linee di abbonati collegate a *centrali telefoniche digitali e, qualora sia tecnicamente possibile e non richieda un onere economico sproporzionato, alle linee di abbonati collegate a centrali telefoniche analogiche* (art. 3, par. 2).

Gli Stati membri devono notificare alla Commissione i casi in cui l’osservanza delle prescrizioni di cui agli articoli 8, 10 e 11 risulti tecnicamente impossibile o richieda un onere economico sproporzionato (art. 3, par. 3).

¹³ Si ricordano in particolare le seguenti definizioni date dall’art. 1 della legge italiana sulla privacy ([L. 675/1996](#)) in attuazione della direttiva 95/46/CE:

a) *trattamento*: qualunque operazione o complesso di operazioni, svolti con o senza l’ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati;

b) *dato personale*: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) *titolare*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;

d) *interessato*: la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali.

¹⁴ GUCE L 108 del 24 aprile 2002.

a) *reti di comunicazione elettronica*: i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

b) *servizio di comunicazione elettronica*: i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE¹⁵ non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica;

c) *rete pubblica di comunicazioni*: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

d) *abbonato*: la persona fisica o giuridica che sia parte di un contratto con il fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi;

e) *fornitura di una rete di comunicazione elettronica*: la realizzazione, la gestione, il controllo o la messa a disposizione di una siffatta rete.

Ai sensi dell'art. 2 della direttiva in esame, si applicano inoltre le seguenti definizioni:

a) *utente*: qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

¹⁵ Direttiva 98/34/CE, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, GUCE L 204 del 21 luglio 1998.

Ai sensi dell'art. 1 del suddetto provvedimento, per *servizio della società dell'informazione* deve intendersi "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi".

b) *dati relativi al traffico*: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) *dati relativi all'ubicazione*: ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) *comunicazione*: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico¹⁶.

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 (considerando 15);

e) *chiamata*: la connessione istituita da un servizio telefonico accessibile al pubblico che consente la comunicazione bidirezionale in tempo reale;

f) *consenso*: sia per le persone fisiche che per le persone giuridiche (considerando 17), corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE.

A questo proposito si ricorda che la direttiva 95/46/CE definisce il consenso dell'interessato come "qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento".

L'art. 11 della legge italiana sulla privacy ([L. 675/1996](#)) dispone che "il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato", salvi i casi di esclusione del consenso di cui all'art. 12 della legge.

Ai sensi della medesima disposizione, il consenso è validamente prestato solo se *espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 10 della legge*.

Il considerando 17 della direttiva sulle comunicazioni elettroniche precisa che il consenso può essere fornito secondo *qualsiasi modalità appropriata che consenta*

¹⁶ "Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato" (art. 2, lett. d)).

Si veda anche il considerando 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".

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;

g) *servizio a valore aggiunto*: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

h) *posta elettronica*: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente fino a che il ricevente non ne ha preso conoscenza.

[Sommaro](#)

3. Sicurezza

Ai sensi dell'art. 4, par. 1, della direttiva sulle comunicazioni elettroniche, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere *appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi*, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete¹⁷.

Secondo la medesima disposizione, tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure debbono essere *idonee ad assicurare un livello di sicurezza adeguato al rischio esistente*.

Qualora esista un particolare rischio di violazione della sicurezza di rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, ove il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore del servizio, tutti i possibili rimedi, compresi i relativi costi presumibili (art. 4, par. 2).

¹⁷ In materia di sicurezza, l'art. 2 del vigente D.L.vo 171/1998 prevede quanto segue.

“1. Il fornitore di un servizio di telecomunicazioni accessibile al pubblico adotta le misure tecniche ed organizzative di cui all'articolo 15, comma 1, della legge [675/1996] per salvaguardare la sicurezza del servizio e dei dati personali.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio le adotta congiuntamente con il fornitore della rete pubblica di telecomunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni, ai sensi dell'articolo 18 del decreto del Presidente della Repubblica 19 settembre 1997, n. 318, sentito il Garante.

3. Il fornitore di un servizio di telecomunicazioni accessibile al pubblico ha l'obbligo di informare gli abbonati quando sussiste un particolare rischio di violazione della sicurezza della rete, indicando i possibili rimedi e i relativi costi. Analoga informativa è resa all'Autorità per le garanzie nelle comunicazioni e al Garante”.

I rischi oggetto della disciplina in esame possono presentarsi segnatamente per i servizi di comunicazione elettronica su una rete aperta come Internet o per i servizi prestati nell'ambito della 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 programmi 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, impreveduti rischi relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio” (considerando 20).

La fornitura all'abbonato di informazioni sui rischi relativi alla sicurezza dovrebbe essere gratuita, fatta eccezione per i costi nominali che egli può trovarsi a sostenere quando riceva le informazioni o prenda di esse conoscenza, ad esempio scaricando un messaggio di posta elettronica.

Il considerando 20 della direttiva in esame precisa infine che la sicurezza deve essere valutata alla luce dell'articolo 17 della direttiva 95/46/CE.

Per quanto riguarda l'ordinamento italiano, ci si dovrà rifare pertanto alle norme di attuazione della direttiva 95/46/CE contenute nella legge 675/1996, segnatamente all'art. 15, relativo appunto alla “sicurezza dei dati”, nonché alle altre disposizioni della legge sulla privacy a questo connesse¹⁸.

¹⁸ Si riporta il testo dell'art. 15 L. 675/1996:

“1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.

3. Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.

In materia di sicurezza delle comunicazioni elettroniche, la direttiva 2002/58/CE conferma dunque le analoghe previsioni già contenute nell'art. 2 del D.L.vo 171/1998 di attuazione della direttiva 97/66/CE.

Sommario

4. Riservatezza

“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” (considerando 21).

Sulla base di siffatta premessa, l'art. 5, par. 1, della direttiva sulle comunicazioni elettroniche prevede pertanto che gli Stati membri assicurino, mediante disposizioni di legge nazionali, la *riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico*¹⁹.

4. Le misure di sicurezza relative ai dati trattati dagli organismi di cui all'articolo 4, comma 1, lettera b), sono stabilite con decreto del Presidente del Consiglio dei ministri con l'osservanza delle norme che regolano la materia”.

Le misure minime di sicurezza di cui al comma 2 sono state individuate con il D.P.R. 28 luglio 1999, n. 318, *Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675*, GU Serie gen. 216 del 14 settembre 1999.

Sull'argomento si veda G. Riem, *Privacy e Sicurezza. Linee guida e formulari per gli adempimenti previsti dal D.P.R. 318/1999*, Napoli, Ed. Simone 2000; T. Minella, *La Privacy. Guida all'applicazione della legge 675/1996*, Napoli, Ed. Simone, 2001, pp. 369 ss.; S. Sutti, *La sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie*, in *Diritto delle nuove tecnologie informatiche e dell'Internet*, a cura di G. Cassano, Ipsoa, 2002, pp. 837 ss.; F. Tommasi, *La sicurezza dei sistemi informativi ed il documento programmatico sulla sicurezza*, in *Diritto delle nuove tecnologie informatiche e dell'Internet cit.*, pp. 853 ss.

¹⁹ Il vigente art. 3 D.L.vo 171/1998 (“Riservatezza nelle comunicazioni”) prevede quanto segue.

“1. Il fornitore di un servizio di telecomunicazioni accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'abbonato deve informare l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.

3. L'utente deve informare l'altro utente quando nel corso della conversazione vengono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti”.

In particolare, debbono vietarsi *l'ascolto, la captazione, la memorizzazione ed altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi*, eccetto quando ciò sia legalmente autorizzato ai sensi dell'art. 15, par. 1, della direttiva²⁰.

Quanto appena detto non deve impedire d'altra parte la *memorizzazione tecnica necessaria alla trasmissione della comunicazione*, fatto salvo il principio della riservatezza (art. 5, par. 1).

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 infatti a vietare eventuali *memorizzazioni automatiche, intermedie e temporanee* di tali informazioni, fintantoché ciò venga fatto unicamente (considerando 22):

- a) a scopo di trasmissione nella rete di comunicazione elettronica e
- b) 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
- c) durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione.

Inoltre, 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 direttiva in esame non osta a che dette 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 (considerando 22).

Oltre a ciò, il paragrafo 1 dell'art. 5 della direttiva, appena analizzato, non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la *prova di una transazione o di una qualsiasi altra comunicazione commerciale* (art. 5, par. 2). La direttiva 95/46/CE deve però trovare applicazione per detto trattamento.

Le parti in comunicazione dovrebbero inoltre essere informate sulla registrazione, il suo scopo e la durata della sua memorizzazione, preventivamente alla stessa. La

²⁰ Secondo l'art. 15, par. 1, del provvedimento, "gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea".

comunicazione registrata dovrebbe essere cancellata non appena possibile ed in ogni caso non oltre la fine del periodo durante il quale la transazione possa essere impugnata legittimamente (considerando 23).

4.1. Spyware, web bugs e cookies

I cosiddetti software spia (*spyware*), i bachi invisibili (*web bugs*), gli 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 seguirne le attività; essi possono costituire dunque una grave intrusione nella vita privata dell'utente.

L'uso di tali dispositivi dovrebbe pertanto *essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza* (considerando 24)²¹.

Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno infatti 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 fondamentali²².

Se questo è vero, il legislatore comunitario prende però atto che simili dispositivi, in particolare i cosiddetti marcatori (*cookies*)²³, possono rappresentare uno strumento legittimo ed 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, in particolare i *cookies*, siano destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, *il loro uso dovrebbe essere dunque consentito purché siano fornite agli utenti informazioni chiare e*

²¹ In generale, sull'argomento si veda: V. Rossi, *Lo spyware e la privacy*, in *Diritto delle nuove tecnologie informatiche e dell'Internet cit.*, pp. 184 ss.; J. Monducci, *Il trattamento dei dati personali nei contratti on line*, in *Diritto delle nuove tecnologie informatiche e dell'Internet cit.*, pp. 589 ss.; L. M. De Grazia, *Privacy e sicurezza nei contratti on line*, in *Trattato Breve di diritto della Rete*, a cura di A. Sirotti Gaudenti, Rimini, Maggioli Editore, 2001, pp. 185 ss.

²² Legge 4 agosto 1955, n. 848, *Ratifica ed esecuzione della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 e del Protocollo addizionale alla Convenzione stessa, firmato a Parigi il 20 marzo 1952*, GU 221 del 24 settembre 1955.

²³ “I cookies, altrimenti denominati ‘biscotti’, sono delle istruzioni sotto forma di piccoli software che riceviamo mentre navighiamo ma, possono esserci inviati, prelevati, rielaborati e nuovamente rimandati senza che l'utente si accorga di nulla [...] Tecnicamente il cookie consiste in un meccanismo che permette al server (l'elaboratore su cui risiedono le pagine web) di ricevere informazioni e di scaricarle con lo scopo di estendere le possibilità delle applicazioni basate sul rapporto tra client (l'elaboratore utilizzato per la navigazione) ed il server [...] Il server, in tal modo, registra tutto ciò che avviene durante la navigazione in quel determinato sito internet, ovvero quante volte lo abbiamo visitato, con quale frequenza, i link e i percorsi seguiti e tanto altro ancora” (F. Tommasi, *La sicurezza dei sistemi informativi ed il documento programmatico sulla sicurezza*, in *Diritto delle nuove tecnologie informatiche e dell'Internet cit.*, p. 859).

precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi (considerando 25).

Ciò per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando.

Essi dovrebbero d'altra parte 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 alle informazioni sensibili in relazione alla vita privata contenute 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 possano 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.

Specifica infine il considerando 25 della direttiva che l'accesso al contenuto di un dato sito Internet 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.

Sulla base di quanto appena illustrato, l'art. 5, par. 3, della direttiva 2002/58/CE disciplina dunque espressamente la materia imponendo innanzitutto agli Stati membri di assicurare che *l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento*²⁴.

Secondo la medesima disposizione, quanto da essa previsto non deve impedire d'altra parte l'eventuale *memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.*

²⁴ “Le conseguenze di questa norma possono essere molto importanti. Infatti non solo viene proibito l’uso dei cookie senza una dettagliata informativa sul loro scopo e senza il consenso dell’interessato, ma si pongono fuori legge tutte le informazioni che il sistema operativo registra sulle operazioni compiute dall’utente (mettendole, di fatto, a disposizione di chiunque sappia come catturarle), senza che l’utente stesso sappia quali dati sono registrati e in quali misteriosi recessi del computer siano archiviati. Si deve pensare non solo ai comportamenti sospetti di una nota software house statunitense, ma anche alla possibilità che l’amministratore di una rete aziendale raccolga dati sull’attività dei dipendenti, leggendo le informazioni archiviate in ogni macchina collegata” (M. Cammarata, *Qualcosa si muove contro “spammers” e spioni*, in InterLex cit.).

Sommario

5. Segue: dati relativi al traffico

Il considerando 26 del provvedimento in esame afferma che *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.

Detti *dati relativi al traffico* possono essere dunque memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, 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” (considerando 26).

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 (considerando 27).

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 d'altra parte, secondo il preambolo della direttiva, 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 (considerando 28).

Secondo quanto affermato dal considerando 29, il fornitore di servizi è legittimato a trattare, inoltre, 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 consistente nell'uso del servizio di comunicazione elettronica senza il corrispondente pagamento (considerando 29).

I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere in ogni caso progettati per limitare al minimo la quantità di dati personali necessari (considerando 30).

Oltre a ciò, 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 possano 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 (considerando 30).

Sulla base di siffatte premesse, l'art. 6 della direttiva sulle comunicazioni elettroniche disciplina i "dati sul traffico" prevedendo innanzitutto che tali dati, relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica, debbano essere *cancellati o resi anonimi quando non siano più necessari ai fini della trasmissione di una comunicazione* (art. 6, par. 1)²⁵.

²⁵ Per un confronto con la disciplina attuale si veda l'art. 4 D.L.vo 171/1998:

“4. (Dati relativi al traffico e alla fatturazione). 1. I dati personali relativi al traffico, trattati per inoltrare chiamate e memorizzati dal fornitore di un servizio di telecomunicazioni accessibile al pubblico o dal fornitore della rete pubblica di telecomunicazioni, sono cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei commi 2 e 3.

2. Il trattamento finalizzato alla fatturazione per l'abbonato, ovvero ai pagamenti tra fornitori di reti in caso di interconnessione, è consentito sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. Per le medesime finalità, possono essere sottoposti a trattamento i dati concernenti:

- a) il numero o l'identificazione della stazione dell'abbonato;
- b) l'indirizzo dell'abbonato e il tipo di stazione;
- c) il numero dell'abbonato chiamato;

Viene d'altra parte fatto salvo il disposto dell'art. 15, par. 1²⁶, della direttiva nonché quanto segue.

- I dati relativi al traffico che risultano necessari ai fini della *fatturazione* per l'abbonato e dei *pagamenti di interconnessione* possono essere sottoposti a trattamento. Tale trattamento è però consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento (art. 6, par. 2).

- Ai fini della *commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto*, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui all'art. 6, par. 1, sopra illustrato, nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia dato il proprio *consenso*. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento (art. 6, par. 3).

- Il fornitore dei servizi deve comunque *informare* l'abbonato o l'utente sulla *natura dei dati* relativi al traffico che sono sottoposti a trattamento e sulla *durata* del trattamento ai fini enunciati all'art. 6, par. 2, sopra illustrato, e, prima di ottenere il consenso, ai fini enunciati all'art. 6, par. 3, appena esaminato (art. 6, par. 4).

d) il numero totale degli scatti da considerare nel periodo di fatturazione;

e) il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi;

f) la data della chiamata o dell'utilizzazione del servizio;

g) altre informazioni concernenti i pagamenti.

3. Ai fini della commercializzazione di servizi di telecomunicazioni, propri o altrui, il fornitore di un servizio di telecomunicazioni accessibile al pubblico può trattare i dati di cui al comma 2 se l'abbonato ha dato il proprio consenso.

4. Il trattamento dei dati relativi al traffico e alla fatturazione è consentito unicamente agli incaricati che agiscono sotto la diretta autorità del fornitore del servizio di telecomunicazioni accessibile al pubblico, o, a seconda dei casi, del fornitore della rete pubblica di telecomunicazioni, e che si occupano della fatturazione o della gestione del traffico, di analisi per conto dei clienti, dell'accertamento di frodi o della commercializzazione dei servizi di telecomunicazione del fornitore. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

5. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione delle controversie ai sensi del decreto del Presidente della Repubblica 19 settembre 1997, n. 318, in particolare di quelle attinenti all'interconnessione o alla fatturazione”.

²⁶ V. nota n. 20.

Il trattamento dei dati relativi al traffico ai sensi delle disposizioni finora analizzate deve essere in ogni caso limitato alle *persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico* che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. *Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività* (art. 6, par. 5).

Deve rilevarsi infine che le norme di cui all'art. 6 della direttiva non pregiudicano la facoltà degli organismi competenti di ottenere i dati relativi al traffico in base alla normativa applicabile al fine della *risoluzione delle controversie*, in particolare di quelle attinenti all'interconnessione e alla fatturazione (art. 6, par. 6).

Sommario

6. Segue: dati relativi all'ubicazione diversi dai dati relativi al traffico

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 disciplinati dall'art. 6 della direttiva, esaminato nel paragrafo precedente.

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.

Secondo il considerando 35 del provvedimento in esame, il trattamento di siffatti dati 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.

Ciò posto, l'art. 9 della direttiva sulle comunicazioni elettroniche disciplina il trattamento di questa tipologia di dati prevedendo innanzitutto che se i dati relativi all'ubicazione, diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, possono essere sottoposti a trattamento, essi possano esserlo *soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto* (art. 9, par. 1)²⁷.

²⁷ L'art. 10, lett. b), della direttiva prevede che gli Stati membri assicurino l'esistenza di procedure trasparenti in base alle quali il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico *possa sottoporre a trattamento i dati relativi all'ubicazione, nonostante il rifiuto o il*

Prima di chiedere il loro consenso, il fornitore del servizio deve *informare* gli utenti e gli abbonati sulla *natura dei dati* relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli *scopi* e sulla *durata* di quest'ultimo, nonché sull'eventualità che i dati siano *trasmessi ad un terzo per la prestazione del servizio a valore aggiunto*. Gli utenti e gli abbonati devono avere la possibilità di *ritirare il loro consenso* al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento (art. 9, par. 1).

Se hanno dato il consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, l'utente e l'abbonato devono comunque continuare ad avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni (art. 9, par. 2).

Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico ai sensi dei paragrafi 1 e 2 dell'art. 9, appena esaminati, deve essere in ogni caso *limitato alle persone che agiscono sotto l'autorità del fornitore della rete pubblica di telecomunicazione o del servizio di comunicazione elettronica accessibile al pubblico o del terzo che fornisce il servizio a valore aggiunto, e deve essere circoscritto a quanto è strettamente necessario per la fornitura di quest'ultimo* (art. 9, par. 3).

Sommario

7. Segue: fatturazione dettagliata, identificazione della linea chiamante, trasferimento automatico della chiamata, elenchi di abbonati

Occorre ora analizzare brevemente le disposizioni della direttiva sulle comunicazioni elettroniche che disciplinano la fatturazione dettagliata, l'identificazione della linea chiamante, il trasferimento automatico di chiamata e gli elenchi di abbonati²⁸.

A) Fatturazione dettagliata.

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 (considerando 33).

mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate. Sull'ambito di applicazione dell'art. 10 della direttiva 2002/58/CE, v. nota n. 12.

Gli Stati membri possono inoltre adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui all'art. 9 in esame nei casi previsti dall'art. 15, par. 1 (v. nota n. 20).

²⁸ Per un confronto con la disciplina attuale si rimanda agli artt. 5, 6, 7, 8 e 9 del [D.L.vo 171/1998](#).

Ai sensi dell'art. 7, par. 1, della direttiva 2002/58/CE, agli abbonati viene pertanto riconosciuto il *diritto di ricevere fatture non dettagliate*.

Gli Stati membri devono inoltre applicare norme nazionali idonee a conciliare i diritti degli abbonati che ricevono fatture dettagliate con il diritto alla vita privata degli utenti chiamanti e degli abbonati chiamati, ad esempio garantendo che detti utenti e abbonati possano disporre, per le comunicazioni e per i pagamenti, di sufficienti modalità alternative che tutelino maggiormente la vita privata (art. 7, par. 2).

Gli Stati membri dovrebbero infatti 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 ommesso un certo numero di cifre dei numeri chiamati (considerando 33).

B) Presentazione e restrizione dell'identificazione della linea chiamante e collegata.

Qualora sia disponibile la *presentazione dell'identificazione della linea chiamante*, il fornitore dei servizi deve offrire all'utente chiamante la *possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata*. L'abbonato chiamante deve avere tale possibilità *linea per linea* (art. 8, par. 1)²⁹.

Ove sia disponibile la *presentazione dell'identificazione della linea chiamante*, il fornitore di servizi deve inoltre offrire all'abbonato chiamato la *possibilità, mediante una funzione semplice e gratuitamente, per ogni ragionevole utilizzo di tale funzione, di impedire la presentazione dell'identificazione delle chiamate entranti* (art. 8, par. 2).

Qualora sia disponibile la *presentazione dell'identificazione della linea chiamante* e tale indicazione avvenga prima che la comunicazione sia stabilita, il fornitore di servizi deve offrire altresì all'abbonato chiamato la *possibilità, mediante una funzione semplice, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante* (art. 8, par. 3).

Ove sia disponibile la *presentazione dell'identificazione della linea collegata*, il fornitore di servizi deve offrire all'abbonato chiamato la *possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea collegata all'utente chiamante* (art. 8, par. 4).

²⁹ Si vedano anche i considerando 34 e 36 della [direttiva 2002/58/CE](#). Sul campo di applicazione dell'art. 8 del provvedimento, v. nota n. 12.

Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui all'art. 8 in esame nei casi previsti dall'art. 15, par. 1 (v. nota n. 20).

Il paragrafo 1 dell'art. 8, sopra esaminato, si applica anche alle chiamate provenienti dalla Comunità e dirette verso paesi terzi. I paragrafi 2, 3 e 4 della medesima disposizione si applicano anche alle chiamate in entrata provenienti da paesi terzi (art. 8, par. 5).

Gli Stati membri devono assicurare che, qualora sia disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, *il fornitore di servizi di comunicazione elettronica accessibili al pubblico informi quest'ultimo di tale possibilità e delle possibilità di cui ai paragrafi 1, 2, 3 e 4 dell'art. 8, sopra illustrati* (art. 8, par. 6).

Ai sensi dell'art. 10 del provvedimento in esame, gli Stati membri devono assicurare infine l'esistenza di procedure trasparenti in base alle quali il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico³⁰:

a) *possa annullare, in via temporanea, la soppressione della presentazione dell'identificazione della linea chiamante a richiesta di un abbonato che chieda la presentazione dell'identificazione di chiamate malintenzionate o importune.* In tal caso, in base al diritto nazionale, i dati che identificano l'abbonato chiamante sono memorizzati e resi disponibili dal fornitore di una rete pubblica di comunicazioni e/o di un servizio di comunicazioni elettroniche accessibile al pubblico;

b) *possa annullare la soppressione della presentazione dell'identificazione della linea chiamante, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate.*

C) *Trasferimento automatico della chiamata.*

L'art. 11 della direttiva sulle comunicazioni elettroniche dispone che gli Stati membri provvedano affinché ciascun abbonato abbia la *possibilità, gratuitamente e mediante una funzione semplice, di bloccare il trasferimento automatico delle chiamate verso il proprio terminale da parte di terzi*³¹.

D) *Elenchi di abbonati.*

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 postulano, per gli abbonati, il diritto di determinare

³⁰ Sull'ambito di applicazione dell'art. 10 della direttiva 2002/58/CE, v. nota n. 12.

³¹ Si veda anche il considerando 37 della [direttiva 2002/58/CE](#). Sul campo di applicazione dell'art. 11 del provvedimento, v. nota n. 12.

se i loro dati personali possano essere pubblicati in un elenco e, in caso affermativo, quali (considerando 38).

È opportuno pertanto 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.

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 (considerando 39).

Sulla base di queste premesse l'art. 12, par. 1, della direttiva 2002/58/CE stabilisce che gli Stati membri provvedano affinché *gli abbonati siano informati, gratuitamente e prima di essere inseriti nell'elenco, in merito agli scopi degli elenchi cartacei o elettronici a disposizione del pubblico o ottenibili attraverso i servizi che forniscono informazioni sugli elenchi, nei quali possono essere inclusi i loro dati personali, nonché in merito ad ogni ulteriore possibilità di utilizzo basata su funzioni di ricerca incorporate nelle versioni elettroniche degli elenchi stessi* (art. 12, par. 1).

Gli Stati membri devono assicurare altresì che *gli abbonati abbiano la possibilità di decidere se i loro dati personali – e, nell'affermativa, quali – debbano essere riportati in un elenco pubblico, sempreché i dati siano pertinenti per gli scopi dell'elenco dichiarati dal suo fornitore. Gli Stati membri devono provvedere inoltre affinché gli abbonati abbiano le possibilità di verificare, rettificare o ritirare tali dati*. Il fatto che i dati non siano riportati in un elenco pubblico di abbonati, la verifica, la correzione o il ritiro dei dati non devono comportare oneri (art. 12, par. 2).

Gli Stati membri possono disporre che sia chiesto il *consenso ulteriore degli abbonati per tutti gli scopi di un elenco pubblico diversi dalla ricerca di dati su persone sulla base del loro nome e, ove necessario, di un numero minimo di altri elementi di identificazione* (art. 12, par. 3).

I paragrafi 1 e 2 dell'art. 12, appena esaminati, si applicano agli abbonati che siano persone fisiche. Gli Stati membri devono assicurare inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela anche degli

interessi legittimi degli abbonati che non siano persone fisiche relativamente all'inclusione negli elenchi pubblici (art. 12, par. 4)³².

[Sommar](#)

8. Le comunicazioni indesiderate (*unsolicited communications*)

Il considerando 40 della direttiva sulle comunicazioni elettroniche afferma che si è reso necessario prevedere misure per tutelare gli abbonati da interferenze nella loro vita privata attuate mediante *comunicazioni indesiderate a scopo di commercializzazione diretta (direct marketing)*, in particolare mediante *dispositivi automatici di chiamata, telefax o posta elettronica, compresi i messaggi SMS*.

Le suddette forme di comunicazioni commerciali indesiderate possono infatti, 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 queste forme di comunicazioni indesiderate a scopo di commercializzazione diretta è pertanto giustificato, conclude il considerando 40, prevedere che le relative chiamate possano essere inviate ai destinatari solo *previo consenso esplicito* di questi ultimi.

Sulla base di siffatte premesse, l'art. 13 della direttiva in esame detta dunque una disciplina specifica delle comunicazioni indesiderate, destinata a sostituire quella attualmente contenuta nel D.L.vo 171/1998 di attuazione della direttiva 97/66/CE.

8.1. La disciplina attuale (art. 10 D.L.vo 171/1998)

L'art. 10, comma 1, del [D.L.vo 171/1998](#) ("chiamate indesiderate"), con riguardo alla tutela della vita privata nel settore delle telecomunicazioni, stabilisce che "l'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento

³² Deve ricordarsi infine che l'art. 12 della direttiva sulle comunicazioni elettroniche non si applica agli elenchi già prodotti o immessi sul mercato su supporto cartaceo o elettronico off-line prima dell'entrata in vigore delle disposizioni nazionali adottate in forza del provvedimento (art. 16, par. 1).

Se i dati personali degli abbonati a servizi pubblici fissi o mobili di telefonia vocale sono stati inseriti in un elenco pubblico degli abbonati in conformità con le disposizioni della direttiva 95/46/CE e dell'articolo 11 della direttiva 97/66/CE prima dell'entrata in vigore delle disposizioni nazionali adottate conformemente alla direttiva 2002/58/CE, i dati personali di tali abbonati potranno restare inseriti in tale elenco pubblico cartaceo o elettronico, comprese le versioni con funzioni di ricerca inverse, salvo altrimenti da essi comunicato dopo essere stati pienamente informati degli scopi e delle possibilità in conformità con l'articolo 12 della direttiva in esame (art. 16, par. 2).

di ricerche di mercato o di comunicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato”.

Ai fini del provvedimento richiamato, per *abbonato* deve intendersi “qualunque persona fisica, persona giuridica, ente o associazione che sia parte di un contratto con un fornitore di servizi di telecomunicazioni accessibili al pubblico, per la fornitura dei medesimi servizi” (art. 1, lett. a)³³.

La disposizione prevede inoltre che le chiamate effettuate per le medesime finalità di cui sopra, ma con mezzi diversi da quelli ivi indicati, siano consentite ai sensi degli articoli 11 e 12 della [legge sulla privacy](#) (art. 10, comma 2, D.L.vo 171/1998).

In caso di violazione dell'art. 10, l'art. 11 D.L.vo 171/1998 stabilisce l'applicazione delle sanzioni penali di cui all'art. 35 L. 675/1996.

La disposizione ora in esame riguarda esclusivamente le ipotesi dell'invio di materiale pubblicitario, della vendita diretta, del compimento di ricerche di mercato e della comunicazione commerciale interattiva nell'ambito dei servizi di telecomunicazioni.

Se la chiamata è effettuata per scopi diversi, l'art. 10 D.L.vo 171/1998 non potrà dunque, in nessun caso, trovare applicazione³⁴.

Il primo comma dell'articolo in parola non menziona espressamente la posta elettronica; problemi sono sorti pertanto con riguardo al suo campo di applicazione: in particolare ci si è chiesti se nella nozione di *sistema automatizzato di chiamata* possa ricomprendersi anche l'invio di e-mail per i fini contemplati dalla norma.

In caso di risposta affermativa troverebbe infatti applicazione il primo comma dell'art. 10 D.L.vo 171/1998, mentre in caso di risposta negativa, stante il richiamo operato dal secondo comma, ci si dovrebbe rifare agli artt. 11 e 12 L. 675/1996³⁵.

8.2. Le nuove regole: l'art. 13 della direttiva 2002/58/CE

L'art. 13 della direttiva sulle comunicazioni elettroniche disciplina le *comunicazioni indesiderate (unsolicited communications)* stabilendo in primo luogo che l'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi

³³ Per la definizione di *servizio di telecomunicazioni* si veda l'art. 1, lett. d), del [D.L.vo 171/1998](#).

Come sopra visto, la direttiva 2002/58/CE fa oggi riferimento non più al “servizio di telecomunicazioni” bensì al “servizio di comunicazione elettronica”, così come definito dalla direttiva quadro 2002/21/CE.

³⁴ Potranno allora trovare eventuale applicazione nella fattispecie le altre norme dell'ordinamento italiano rilevanti in materia di spamming. Si veda in proposito G. Briganti, *Spamming e diritto*, in Iusreporter, www.iusreporter.it, www.iusreporter.it/Testi/doc-spamming.htm.

³⁵ Sul problema dell'ambito di applicazione dell'art. 10, comma 1, D.L.vo 171/1998 si rimanda a G. Briganti, *Spamming e diritto*, cit., par. 3.1.

automatici di chiamata), del telefax o della posta elettronica *a fini di commercializzazione diretta (direct marketing)* sia consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro *consenso* (art. 13, par. 1).

L'invio di comunicazioni elettroniche a scopo di *direct marketing* è dunque soggetto al *preliminare consenso dell'abbonato*, vale a dire, come sopra visto, ad una manifestazione di volontà *libera, specifica e informata* con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di trattamento ai sensi della direttiva 95/46/CE.

Confrontando il testo di questa disposizione della direttiva in esame con quello del vigente art. 10, comma 1, D.L.vo 171/1998, sopra analizzato, rileva immediatamente l'espressa menzione della posta elettronica tra i mezzi l'uso dei quali richiede il preliminare consenso dell'abbonato.

La nuova disposizione pare dunque destinata a risolvere gli accennati problemi interpretativi relativi al campo di applicazione del primo comma dell'art. 10 D.L.vo 171/1998.

Fatto salvo il paragrafo 1 dell'art. 13, appena esaminato, nell'ambito di una *relazione di clientela già esistente*, la direttiva prevede inoltre che quando una persona fisica o giuridica ottenga dai propri clienti le *coordinate elettroniche per la posta elettronica* nel contesto della vendita di un prodotto o servizio, ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica potrà utilizzare in seguito tali coordinate elettroniche *a scopi di commercializzazione diretta di propri analoghi prodotti o servizi* (art. 13, par. 2).

Ciò a condizione che ai clienti sia offerta *in modo chiaro e distinto al momento della raccolta* delle coordinate elettroniche e *ad ogni messaggio* la possibilità di *opporsi*, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora essi non abbiano rifiutato inizialmente tale uso.

L'articolo in esame impone altresì agli Stati membri di adottare le misure appropriate per garantire che, gratuitamente, le comunicazioni indesiderate a scopo di commercializzazione diretta, *in casi diversi da quelli appena esaminati, non siano permesse se manca il consenso degli abbonati interessati oppure se gli abbonati esprimano il desiderio di non ricevere questo tipo di chiamate* (art. 13, par. 3).

La scelta tra le due alternative (*opt-in* o *opt-out*) è lasciata in questo caso *alle singole normative nazionali*.

La disposizione riguarda forme di commercializzazione diretta più onerose per il mittente, che non impongano però costi finanziari per gli abbonati, quali chiamate telefoniche vocali interpersonali (considerando 42).

E' espressamente vietata dal provvedimento, comunque, la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta *camuffando* o

celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni (art. 13, par. 4).

Alcuni sistemi di posta elettronica consentono agli abbonati di vedere il mittente e l'oggetto di una e-mail nonché di cancellare il messaggio senza dover scaricare il resto del contenuto dell'e-mail o degli allegati, riducendo quindi i costi che potrebbero derivare dal *download* di e-mail o allegati indesiderati.

Secondo il considerando 44 della direttiva, tali modalità potranno continuare ad essere utili, in taluni casi, come *strumento supplementare* rispetto ai requisiti generali stabiliti dal provvedimento. Ciò anche in considerazione degli obblighi informativi che, come si vedrà, la direttiva sul commercio elettronico (direttiva 2000/31/CE) pone a carico del mittente di siffatti messaggi, proprio al fine di rendere la *junk e-mail* immediatamente identificabile dal destinatario.

Deve notarsi a questo punto come tutta la disciplina contenuta nella direttiva 2002/58/CE faccia esclusivo riferimento all'invio di comunicazioni indesiderate a *scopo di commercializzazione diretta*.

Ove manchi un simile fine, come ad esempio nell'ipotesi di comunicazioni effettuate a scopo di propaganda politica o proselitismo religioso, l'art. 13 in esame non potrà dunque trovare applicazione³⁶.

Ai sensi del paragrafo 5 della suddetta disposizione, gli Stati membri dovranno infine garantire, relativamente alle comunicazioni indesiderate, un'adeguata tutela anche degli interessi legittimi degli abbonati che non siano persone fisiche³⁷.

In conclusione, occorre rilevare che, a quanto si legge nel considerando 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.

Le sanzioni, ai sensi del medesimo considerando, dovrebbero essere applicate ad ogni persona, sia essa soggetta al diritto pubblico o privato, che non ottemperi alle disposizioni nazionali adottate a norma della direttiva.

A questo proposito, come già ricordato, l'art. 15, par. 2, del provvedimento stabilisce che le disposizioni del capo III della direttiva 95/46/CE – attuata in Italia con la [legge 675/1996](#) – relative ai ricorsi giurisdizionali, alle responsabilità ed alle sanzioni si

³⁶ Analogamente a quanto accade oggi, come sopra visto, con l'art. 10 D.L.vo 171/1998.

³⁷ Precisa infatti il considerando 45 che la direttiva in esame non pregiudica le misure che gli Stati membri prendono per tutelare i legittimi interessi delle persone giuridiche in relazione a comunicazioni indesiderate a scopo di commercializzazione diretta.

Allorquando gli Stati membri costituiscano un registro *opt-out* per siffatte chiamate a persone giuridiche, principalmente imprese, saranno pienamente applicabili le disposizioni dell'art. 7 della direttiva 2000/31/CE sul commercio elettronico (sulle quali si veda *infra*, par. 8.3.).

applichino relativamente alle disposizioni nazionali adottate in base alla direttiva in esame e con riguardo ai diritti individuali risultanti dalla stessa.

8.3. L'art. 7 della direttiva sul commercio elettronico (direttiva 2000/31/CE)

Con la [direttiva 2000/31/CE](#) dell'8 giugno 2000³⁸, il legislatore comunitario, com'è noto, ha voluto disciplinare “taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno”.

Ai fini del provvedimento, per *servizi della società dell'informazione* devono intendersi tutti quei servizi prestati normalmente dietro retribuzione, a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione (compresa la compressione digitale) e di memorizzazione di dati, su richiesta individuale del destinatario dei servizi.

Per *comunicazioni commerciali* devono intendersi tutte le forme di comunicazione destinate, in modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di una persona che esercita un'attività commerciale, industriale, artigianale o una libera professione (art. 2, lett. f), del provvedimento).

Non costituiscono di per sé comunicazioni commerciali, ai fini della direttiva sul commercio elettronico:

- le indicazioni necessarie per accedere direttamente all'attività dell'impresa, organizzazione o persona, come un nome di dominio (*domain name*) o un indirizzo di posta elettronica;
- le comunicazioni relative a beni, servizi o all'immagine dell'impresa, organizzazione o persona elaborate in modo da essa indipendente, in particolare se a titolo gratuito.

Con specifico riguardo allo spamming, l'art. 7, par. 1, della direttiva 2000/31/CE dispone che, oltre agli altri obblighi posti dal diritto comunitario, gli Stati membri i quali permettano *comunicazioni commerciali non sollecitate per posta elettronica* debbano provvedere affinché tali comunicazioni, trasmesse da un prestatore stabilito nel proprio territorio, siano *identificabili come tali, in modo chiaro ed inequivocabile, fin dal momento in cui il destinatario le riceve*.

L'identificabilità come tale della *junk e-mail* sin dal momento della sua ricezione consentirà al destinatario (e ai *provider*) di approntare filtri che eliminino

³⁸ GUCE L 178 del 17 luglio 2000.

La direttiva sul commercio elettronico è in fase di attuazione in Italia. L'art. 31 della legge comunitaria per il 2001 (Legge 1 marzo 2002, n. 39) delega infatti il Governo ad emanare un decreto legislativo di attuazione della direttiva, fissandone i principi e i criteri direttivi.

Per un commento all'intero provvedimento si veda G. Briganti, *La direttiva sul commercio elettronico*, in Iusreporter, www.iusreporter.it, www.iusreporter.it/Testi/doc-dircommel.htm.

automaticamente la posta indesiderata, impedendo così agli *spammer* di inviare messaggi in grado di ingannare il destinatario sulla loro natura pubblicitaria.

L'art. 6 della direttiva, riguardante le comunicazioni commerciali in genere, prevede inoltre che la persona fisica o giuridica per conto della quale venga effettuata la comunicazione commerciale debba essere *chiaramente identificabile*.

Come sopra visto, la direttiva 2002/58/CE prevede oggi il divieto espresso di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione delle comunicazioni.

Fatte salve la direttiva 97/7/CE e la direttiva 97/66/CE, gli Stati membri devono altresì adottare i provvedimenti necessari affinché i prestatori che inviino per posta elettronica comunicazioni commerciali non sollecitate consultino regolarmente e rispettino i *registri negativi (opt-out)* in cui possono iscriversi le persone fisiche che non desiderino ricevere tali comunicazioni commerciali (art. 7, par. 2).

L'invio per posta elettronica di tale genere di comunicazioni non dovrebbe infine, secondo la direttiva sul commercio elettronico, dar luogo a costi supplementari per il destinatario.

La direttiva 2000/31/CE, come appena visto, non si occupa della disciplina relativa al *consenso dei destinatari* delle comunicazioni commerciali non sollecitate (considerando 30; art. 7, par. 2)³⁹.

Il provvedimento riserva infatti la questione del consenso, in particolare, alla direttiva 97/7/CE sui contratti a distanza conclusi dai consumatori⁴⁰ e alla richiamata direttiva 97/66/CE, attuata in Italia con il D.L.vo 171/1998.

A questo proposito, come già si è avuto modo di rilevare, occorre precisare che la direttiva 2002/58/CE sulle comunicazioni elettroniche, disponendo *l'abrogazione della direttiva 97/66/CE*, prevede che "i riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva" (art. 19, par. 2).

I riferimenti operati dalla direttiva sul commercio elettronico alla direttiva 97/66/CE, a partire dalla data di abrogazione di quest'ultima, dovranno quindi intendersi rivolti alla direttiva 2002/58/CE.

³⁹ Si legge nel considerando 30 della direttiva sul commercio elettronico che "l'invio per posta elettronica di comunicazioni commerciali non sollecitate può risultare inopportuno per i consumatori e per i fornitori di servizi della società dell'informazione e perturbare il buon funzionamento delle reti interattive. La questione del consenso dei destinatari di talune forme di comunicazione commerciale non sollecitata non è disciplinata dalla presente direttiva bensì, in particolare dalla direttiva 97/7/CE e dalla direttiva 97/66/CE".

⁴⁰ Direttiva attuata in Italia con il D.L.vo 22 maggio 1999, n. 185, *Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza*, GU Serie gen. 143 del 21 giugno 1999.



L'art. 31, comma 1, lett. b), della legge comunitaria 2001, nel delegare il Governo all'attuazione della direttiva sul commercio elettronico, prevede che l'emanando decreto legislativo definisca "gli obblighi di informazione sia per la comunicazione commerciale che per la comunicazione non sollecitata; quanto a quest'ultima, ai sensi della normativa sul trattamento dei dati personali, devono essere incoraggiati ed agevolati sistemi di filtraggio da parte delle imprese. In ogni caso, l'invio di comunicazioni non sollecitate per posta elettronica non deve dare luogo a costi supplementari di comunicazione per il destinatario".

Deve infine ricordarsi che la direttiva sul commercio elettronico lascia altresì impregiudicata la disciplina in materia di protezione dei dati personali di cui alla direttiva 95/46/CE, attuata in Italia con la L. 675/1996.

[Sommaro](#)