

LE COMUNICAZIONI ELETTRONICHE NEL CODICE DELLA PRIVACY: SICUREZZA, RISERVATEZZA E SPAMMING

La disciplina di attuazione della direttiva 2002/58/CE

Avv. Giuseppe Briganti

avv.briganti@iusreporter.it

IUSReporter.it

www.iusreporter.it

Premessa una breve analisi della direttiva 2002/58/CE, il testo si sofferma, in un primo momento, sulle disposizioni generali valide per tutti i trattamenti di dati personali dettate dalla parte I del Codice della privacy, per poi approfondire le specifiche disposizioni di attuazione della direttiva sulle comunicazioni elettroniche contenute nella parte II del Codice. Particolare attenzione è riservata alla disciplina delle comunicazioni commerciali, con speciale riferimento al fenomeno dello spamming, in rapporto al regime di opt-in introdotto oggi in via generale dall'art. 130 del Codice. Considerati i diversi profili di contatto, vengono esaminate altresì le disposizioni di attuazione della direttiva europea sul commercio elettronico contenute nel D.L.vo 70/2003. Un ultimo capitolo, infine, illustra brevemente le forme di tutela disponibili per l'interessato nonché l'apparato sanzionatorio predisposto dal Codice della privacy.

L'autore è avvocato del Foro di Urbino. Ha pubblicato diversi scritti inerenti il Diritto delle nuove tecnologie informatiche e di Internet ed è ideatore e curatore di www.iusreporter.it, sito dedicato alla ricerca giuridica sul Web.

INDICE

Introduzione

pag. 4

I. La direttiva europea sulle comunicazioni elettroniche (direttiva 2002/58/CE)

1. Premessa – 2. Campo di applicazione della direttiva 2002/58/CE e definizioni – 3. Sicurezza – 4. Riservatezza delle comunicazioni – 4.1. Spyware, web bugs e cookies – 5. Dati relativi al traffico – 6. Dati relativi all'ubicazione diversi dai dati relativi al traffico – 7. Fatturazione dettagliata, identificazione della linea chiamante, trasferimento automatico della chiamata, elenchi di abbonati

pag. 6

II. Il Codice della privacy

1. Premessa – 2. Definizioni – 3. Principi generali. Oggetto e ambito di applicazione – 4. Diritti dell'interessato – 5. Regole generali per il trattamento dei dati – 6. *Segue*: regole ulteriori per i soggetti pubblici – 7. *Segue*: il consenso dell'interessato – 8. *Segue*: Comunicazione e diffusione dei dati – 9. *Segue*: dati sensibili e semisensibili – 10. Soggetti che effettuano il trattamento – 11. Sicurezza dei dati e dei sistemi – 11.1. *Misure minime per i trattamenti effettuati con strumenti elettronici* – 11.2. *Misure minime per i trattamenti effettuati senza l'ausilio di strumenti elettronici* – 12. Adempimenti – 13. Trasferimento dei dati all'estero

pag. 40

III. La disciplina di attuazione della direttiva 2002/58/CE sulle comunicazioni elettroniche

1. Premessa. Ambito di applicazione e definizioni – 2. Sicurezza – 3. Riservatezza delle comunicazioni – 4. Dati relativi al traffico – 5. Fatturazione dettagliata – 6. Identificazione della linea – 7. Dati relativi all'ubicazione – 8. Chiamate di disturbo e di emergenza – 9. Trasferimento automatico della chiamata – 10. Elenchi di abbonati – 11. Comunicazioni indesiderate e spamming – 11.1. *Le comunicazioni indesiderate (unsolicited communications) nella direttiva 2002/58/CE* – 11.2. *La disciplina contenuta nel D.L.vo 171/1998 di attuazione della direttiva 97/66/CE* – 11.3. *L'art. 13 della direttiva 2002/58/CE* – 11.4. *L'art. 130 del Codice della privacy* – 11.5. *Codice di deontologia e di buona condotta per il marketing diretto* – 11.6. *Altre norme rilevanti in materia di spamming* – 12. *Segue*: il provvedimento generale sullo spamming del Garante per la protezione dei dati personali – 13. *Segue*: le regole della Netiquette, l'attività della Naming Authority; iniziative e responsabilità dei provider – 14. Informazioni ad abbonati e utenti – 15. Conservazione di dati di traffico per altre finalità – 16. Internet e reti telematiche – 17. Videosorveglianza

- 2 -

pag. 110

IV. Il D.L.vo 70/2003 di attuazione della direttiva europea sul commercio elettronico

1. Premessa – 2. Obiettivi e campo di applicazione del D.L.vo 70/2003 – 3. Definizioni – 4. Mercato interno – 5. Regime di stabilimento e di informazione – 6. Comunicazioni commerciali e spamming – 7. Informazioni dirette alla conclusione del contratto e inoltro dell'ordine – 8. Responsabilità dei prestatori intermediari (provider) – 8.1. *Responsabilità nell'attività di semplice trasporto (mere conduit)* – 8.2. *Responsabilità nell'attività di memorizzazione temporanea (caching)* – 8.3. *Responsabilità nell'attività di memorizzazione di informazioni (hosting)* – 8.4. *Assenza dell'obbligo generale di sorveglianza* – 9. Codici di condotta, composizione delle controversie e cooperazione – 10. Sanzioni

pag. 180

V. Tutela dell'interessato e sanzioni

1. Premessa – 2. Tutela dell'interessato – 2.1. *Forme di tutela dinanzi al Garante* – 2.2. *Tutela giurisdizionale* – 3. Sanzioni – 3.1. *Violazioni amministrative* – 3.2. *Illeciti penali* – 4. È sanzionabile la spedizione di una prima e-mail di richiesta di consenso per il successivo invio di comunicazioni commerciali?

pag. 242

Introduzione

Con la direttiva 2002/58/CE il legislatore europeo ha inteso disciplinare il trattamento dei dati personali e tutelare la vita privata nello specifico settore delle *comunicazioni elettroniche*, adeguando a tal fine la direttiva 97/66/CE, 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 – agli sviluppi verificatisi negli ultimi anni nei mercati e nelle tecnologie dei servizi di comunicazione elettronica.

L'Italia, com'è noto, ha dato attuazione alla direttiva europea sulle comunicazioni elettroniche con una disciplina inserita nel *Codice in materia di protezione dei dati personali* (D.L.vo 196/2003) entrato in vigore il primo gennaio 2004. Detto provvedimento abroga e sostituisce la nota legge 675/1996 sulla privacy nonché il menzionato D.L.vo 171/1998.

Pertanto, premessa una breve analisi della direttiva 2002/58/CE, il testo si sofferma, in un primo momento, sulle *disposizioni generali* valide per tutti i trattamenti di dati personali dettate dalla parte I del Codice della privacy (artt. 1-45), fornendone un sintetico e completo quadro, per poi approfondire le specifiche disposizioni di attuazione della direttiva sulle comunicazioni elettroniche, contenute nel titolo X della parte II del Codice (artt. 121-134).

Particolare attenzione è riservata alla disciplina delle *comunicazioni commerciali*, con speciale riferimento al fenomeno dello *spamming*, ossia dell'invio di comunicazioni elettroniche non richieste ad un lungo elenco di destinatari, in rapporto al regime di *opt-in* introdotto oggi in via generale dall'art. 130 del Codice della privacy. Viene altresì affrontata la questione se l'invio di una *prima*

e-mail di richiesta di consenso per il successivo inoltro di comunicazioni commerciali possa o meno essere considerato passibile di sanzione alla luce dell'art. 167 del provvedimento.

Considerati i diversi profili di contatto tra le due discipline, un capitolo viene poi dedicato all'esame delle disposizioni del D.L.vo 70/2003 di attuazione della direttiva 2000/31/CE sul *commercio elettronico*, con particolare riguardo a comunicazioni commerciali e responsabilità dei provider. Infatti, la nozione di "servizi della società dell'informazione" contemplata da detto provvedimento coincide, parzialmente, con quella di "servizi di comunicazione elettronica" fornita oggi dal Codice della privacy.

Un ultimo capitolo, infine, esamina brevemente le *forme di tutela dell'interessato*, dinanzi al Garante per la protezione dei dati personali o dinanzi al giudice ordinario, disciplinate dal Codice, nonché le *sanzioni*, amministrative o penali, stabilite dal provvedimento in relazione alla violazione di alcune delle disposizioni rilevanti in materia di comunicazioni elettroniche.

Avv. Giuseppe Briganti

avv.briganti@iusreporter.it

marzo 2004

Per aggiornamenti sugli argomenti trattati si invita a consultare l'*Osservatorio* di www.iusreporter.it raggiungibile all'indirizzo www.iusreporter.it/osservatorio.htm.

CAPITOLO I

LA DIRETTIVA EUROPEA

SULLE COMUNICAZIONI ELETTRONICHE

(DIRETTIVA 2002/58/CE)

SOMMARIO: 1. [Premessa](#) – 2. [Campo di applicazione della direttiva 2002/58/CE e definizioni](#) – 3. [Sicurezza](#) – 4. [Riservatezza delle comunicazioni](#) – 4.1. [Spyware, web bugs e cookies](#) – 5. [Dati relativi al traffico](#) – 6. [Dati relativi all'ubicazione diversi dai dati relativi al traffico](#) – 7. [Fatturazione dettagliata, identificazione della linea chiamante, trasferimento automatico della chiamata, elenchi di abbonati](#)

[INDICE](#)

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

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. Il testo del provvedimento è disponibile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/direttiva-2002-58-ce.htm.

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

specifico settore delle *comunicazioni elettroniche*.

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/CE², *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](#)³ – 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)⁴.

² GUCE L 24 del 30 gennaio 1998. Il testo del provvedimento è consultabile su www.privacy.it all’indirizzo www.privacy.it/dir66-97.html.

³ 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, e successive modifiche. Il testo del provvedimento è disponibile su www.iusreporter.it all’indirizzo www.iusreporter.it/Testi/dlvo171-98.htm.

⁴ 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 (*31 ottobre 2003*, data fissata per il recepimento della direttiva da parte degli Stati membri). I riferimenti alla direttiva abrogata devono, da tale data, intendersi operati alla direttiva 2002/58/CE (art. 19, par. 2).

Con riguardo all’ordinamento giuridico italiano, come si vedrà, la normativa di attuazione della direttiva 2002/58/CE contenuta nel Codice della privacy ha previsto l’abrogazione del D.L.vo

In questo quadro, il provvedimento si propone di armonizzare le disposizioni degli Stati membri nella misura necessaria 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 (art. 1, par. 1)⁵.

La direttiva 2002/58/CE sulle comunicazioni elettroniche si compone di un preambolo (considerando 1-49) e di 21 articoli.

171/1998 di recepimento della direttiva 97/66/CE a far data dalla sua entrata in vigore, vale a dire dal *primo gennaio 2004*.

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.

⁵ 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 imposte, 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*.

I paragrafi 2 e 3 dell'art. 14 dispongono quanto segue.

“2. Qualora talune disposizioni della presente direttiva possano essere attuate soltanto attraverso la prescrizione di caratteristiche tecniche specifiche per le reti di comunicazione elettronica, gli Stati membri informano la Commissione secondo le procedure di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

3. All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni”.

Entro il suo campo di applicazione (artt. 1 e 3), essa disciplina la materia della sicurezza (art. 4), la riservatezza delle comunicazioni (art. 5), i dati sul traffico (art. 6), la fatturazione dettagliata (art. 7), la presentazione e restrizione dell'identificazione della linea chiamante e collegata (art. 8), i dati relativi all'ubicazione (art. 9), il trasferimento automatico della chiamata (art. 11), gli elenchi di abbonati (art. 12), e, infine, le comunicazioni indesiderate (art. 13)⁶.

⁶ Così il Garante per la protezione dei dati personali ha presentato 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.

Il presente capitolo analizza brevemente le suddette disposizioni della direttiva sulle comunicazioni elettroniche, in via preliminare rispetto all'esame della disciplina di attuazione del provvedimento europeo nell'ordinamento giuridico italiano, contenuta nel *Codice della privacy*, la quale sarà oggetto dei successivi capitoli⁷.

Sommario

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

Le disposizioni della direttiva sulle comunicazioni elettroniche (art. 1, par. 2)

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.

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".

In generale, sulle principali novità introdotte dalla direttiva in esame, si veda M. Cammarata, *Qualcosa si muove contro "spammatori" 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.

⁷ Con riguardo alle "comunicazioni indesiderate" di cui all'art. 13 della direttiva si rimanda sin d'ora al capitolo III.

*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 dapprima con la nota legge 675/1996 ed oggi, come si vedrà, con il *Codice della privacy*.*

Esse inoltre prevedono la tutela dei legittimi interessi degli abbonati persone giuridiche⁹.

La direttiva 95/46/CE continuerà comunque a trovare applicazione nell'ambito delle comunicazioni elettroniche, in particolare per quanto riguarda tutti gli aspetti relativi 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)¹⁰.

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* trovino applicazione relativamente alle disposizioni nazionali adottate in base alla direttiva 2002/58/CE e con riguardo ai diritti individuali risultanti dalla stessa.

⁸ GUCE L 281 del 23 novembre 1995. Il testo della direttiva 95/46/CE può essere consultato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/direttiva1995-46-ce.htm.

⁹ 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 ricomprendeva 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)). Tale tutela, come si vedrà, è stata confermata dal vigente Codice della privacy (art. 4, comma 1, lett. i)).

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

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*¹¹.

Ai fini del provvedimento, trovano applicazione le definizioni contenute nella direttiva 95/46/CE¹² e nella recente [direttiva 2002/21/CE](#)¹³, che istituisce un

¹¹ 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 artt. 8, 10 e 11 risulti tecnicamente impossibile o richieda un onere economico sproporzionato (art. 3, par. 3).

¹² Si ricordano le seguenti definizioni date dall’art. 2 della direttiva 95/46/CE:

a) *dati personali*: qualsiasi informazione concernente una persona fisica identificata o identificabile (*persona interessata*); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) *trattamento di dati personali (trattamento)*: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;

c) *archivio di dati personali (archivio)*: qualsiasi insieme strutturato di dati personali accessibili, secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

d) *responsabile del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

e) *incaricato del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento;

f) *terzi*: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta;

g) *destinatario*: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati, che si tratti o meno di un terzo. Tuttavia, le autorità che possono ricevere comunicazione di dati nell'ambito di una missione d'inchiesta specifica non sono considerate destinatari;

h) *consenso della persona interessata*: 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.

¹³ GUCE L 108 del 24 aprile 2002. Il testo del provvedimento è disponibile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/direttiva_2002-21-ce.htm.

La direttiva 2002/21/CE è stata recentemente attuata in Italia con il *Codice delle comunicazioni elettroniche* (D.L.vo 1 agosto 2003, n. 259, GU 214 del 15 settembre 2003, Suppl. ord.).

Come può leggersi in www.governo.it, la parte più significativa del codice e maggiormente innovativa per il mercato delle comunicazioni elettroniche è quella contenuta nei primi due titoli, dedicati ai principi generali ed alle reti e servizi di comunicazione elettronica ad uso pubblico.

Queste le principali novità:

- si abbandona il regime della licenza e viene introdotto il *regime unico dell'autorizzazione generale*, vale a dire una autorizzazione che consegue automaticamente, in assenza di un diniego dell'amministrazione, alla dichiarazione dell'operatore, consentendo di dare inizio all'attività senza attendere un formale provvedimento di abilitazione;

- gli obblighi posti a carico degli ex monopolisti e degli operatori, individuati dall'Autorità per le garanzie nelle comunicazioni come aventi un significativo potere di mercato, dipendono dall'esito di una analisi di mercato effettuata dalla stessa Autorità, che indica, caso per caso, le misure occorrenti, volte ad apportare i necessari correttivi alle eventuali distorsioni del mercato;

- vengono promossi l'innovazione e lo sviluppo di reti e servizi di comunicazione elettronica a larga banda; in questo settore rivestono un ruolo di grande rilievo le Regioni e gli Enti locali che dovranno individuare i livelli avanzati di reti e servizi a larga banda, definire quelli minimi di disponibilità a livello locale, promuovere iniziative per fornire un sostegno agli anziani, ai disabili, ai consumatori a basso reddito, utilizzando i fondi pubblici che si renderanno disponibili;

- viene introdotto il cosiddetto *trading delle frequenze*, vale a dire la possibilità per gli operatori di cedere sul mercato frequenze loro assegnate ad altri operatori muniti dei necessari requisiti;

- restano in piedi tutti gli *obblighi di servizio universale* (fornitura di postazione telefonica fissa, elenco abbonati, telefoni pubblici a pagamento, misure per i disabili, numeri di emergenza, tra cui il numero unico di emergenza europeo 112);

- la *completa depenalizzazione* della violazione originariamente prevista dall'art. 195 del codice postale per l'esercizio di un impianto di telecomunicazione senza autorizzazione, salvo quando l'impianto sia destinato alla radiodiffusione, ipotesi questa in cui permane il reato.

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:

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'art. 1 della direttiva 98/34/CE¹⁴ non consistenti interamente o prevalentemente

Il testo completo del Codice delle comunicazioni elettroniche può essere consultato su www.altalex.com all'indirizzo www.altalex.com/index.php?idnot=6497.

¹⁴ 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".

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;

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;

Sui servizi della società dell'informazione si veda anche quanto si dirà nel capitolo IV, par. 3, a proposito dell'attuazione in Italia della direttiva europea sul commercio elettronico.

d) *comunicazione*: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico¹⁵.

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".

¹⁵ "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".

Il considerando 17 della direttiva sulle comunicazioni elettroniche precisa che 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;*

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.

Sommario

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 rete*.

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).

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, imprevisti 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 riceve le informazioni o prende 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/CE¹⁶.

In materia di sicurezza, la direttiva 2002/58/CE sulle comunicazioni elettroniche conferma dunque sostanzialmente le analoghe previsioni già contenute nell'abrogata direttiva 97/66/CE, attuata in Italia con il sopra ricordato D.L.vo 171/1998¹⁷.

¹⁶ L'art. 17 ("Sicurezza dei trattamenti") della direttiva 95/46/CE prevede quanto segue.

"1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.

2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure.

3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:

- che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;

- che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.

4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente".

¹⁷ In materia di sicurezza, l'art. 4 dell'abrogata direttiva 97/66/CE stabiliva quanto segue.

"1. Il fornitore di un servizio di telecomunicazione offerto al pubblico deve prendere le appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di telecomunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei costi di attuazione, dette misure devono garantire un livello di sicurezza adeguato al rischio incorso.

Sommario

4. Riservatezza delle comunicazioni

“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 elettroniche¹⁸ 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.*

In particolare, debbono vietarsi *l’ascolto, la captazione, la memorizzazione ed altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi*

2. In caso di un particolare rischio di violazione della sicurezza della rete il fornitore di un servizio di telecomunicazione offerto al pubblico ha l’obbligo di informarne gli abbonati indicando tutti i possibili rimedi, compresi i relativi costi”.

¹⁸ L’art. 5 (“Riservatezza delle comunicazioni”) dell’abrogata direttiva 97/66/CE stabiliva in proposito quanto segue.

“1. Gli Stati membri garantiscono mediante normative nazionali la riservatezza delle comunicazioni effettuate mediante la rete pubblica di telecomunicazione e i servizi di telecomunicazione offerti al pubblico. In particolare essi vietano l’ascolto, l’intercettazione, la memorizzazione o altri generi di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza il consenso di questi ultimi, eccetto quando sia autorizzato legalmente, a norma dell’articolo 14, paragrafo 1.

2. Il paragrafo 2 non riguarda la registrazione di comunicazioni legalmente autorizzata, nel quadro delle legittime prassi commerciali, allo scopo di fornire la prova di una transazione o di qualsiasi altra comunicazione commerciale”.

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 direttiva¹⁹.

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

¹⁹ Secondo l'art. 15, par. 1, del provvedimento in parola, "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".

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 altresì 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 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)²⁰.

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 fondamentali²¹.

Se questo è vero, il legislatore comunitario prende però atto che simili dispositivi, in particolare i cosiddetti marcatori (*cookies*)²², possono rappresentare uno

²⁰ In generale, sull'argomento, si veda: V. Rossi, *Lo spyware e la privacy*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET*, a cura di G. Cassano, Ipsoa, 2002, 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 Gaudenzi, Rimini, Maggioli Editore, 2001, pp. 185 ss.; A. Lisi, *Tutela della privacy in Internet*, in *La privacy in Internet*, a cura di A. Lisi, Napoli, Ed. Simone, 2003, pp. 60 ss.; M. De Giorgi, *La tutela della privacy per il consumatore in Rete*, in *La privacy in Internet* cit., pp. 182 ss.; M.P. Berlingieri, *I rischi della navigazione in Internet*, in *Privacy.it*, www.privacy.it, www.privacy.it/berlingieri01.html.

Si richiama anche la raccomandazione 1/99 del Gruppo europeo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali *sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware*, consultabile su www.privacy.it all'indirizzo www.privacy.it/gruppracc199901.html.

²¹ 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.

²² "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).

"I *cookies* offrono, perciò, la possibilità di raccogliere informazioni sui siti visitati da un determinato soggetto, permettendo in questo modo di fabbricare una mappa dei gusti e delle preferenze dell'utente. Si tratta del processo definito, in gergo commerciale, di 'profilazione'.

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 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

Sono facilmente immaginabili, anche in questa ipotesi, le conseguenze di un uso distorto di tali strumenti, nati in origine per semplificare i compiti dell'utente che si connette, cui viene evitato di ridigitare ID e *password* ad ogni collegamento, cui potrebbe invece capitare di veder recapitare direttamente al proprio indirizzo (reale o virtuale che sia) proposte commerciali *ad hoc*, modellate sui suoi propri gusti e inclinazioni" (M.P. Berlingieri, *I rischi della navigazione in Internet* cit.).

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*²³.

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.*

²³ “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* cit.).

Sommario

5. 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* – recita il considerando 15 della direttiva 2002/58/CE – “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”.

I dati relativi al traffico, come definiti dal già esaminato art. 2, 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 elettroniche²⁴ disciplina i “dati sul traffico” prevedendo innanzitutto che tali dati,

²⁴ L'abrogata direttiva 97/66/CE prevedeva in proposito quanto segue (art. 6).

“1. I dati sul traffico relativi agli abbonati e agli utenti, trattati per inoltrare chiamate e memorizzati dal fornitore di una rete pubblica e/o di un servizio di telecomunicazione offerto al pubblico, devono essere cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei paragrafi 2, 3 e 4.

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).

Viene d'altra parte fatto salvo il disposto dell'art. 15, par. 1²⁵, 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

2. Ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento i dati indicati nell'allegato. Il trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

3. Ai fini della commercializzazione dei propri servizi di telecomunicazione il fornitore di un servizio di telecomunicazione offerto al pubblico può trattare i dati di cui al paragrafo 2 se l'abbonato ha dato il proprio consenso.

4. Il trattamento dei dati relativi al traffico e alla fatturazione deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori delle reti pubbliche di telecomunicazione e/o dei servizi di telecomunicazione offerti al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per i clienti, dell'accertamento di frodi e della commercializzazione dei servizi di telecomunicazione del fornitore, e deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività.

5. I paragrafi 1, 2, 3 e 4 si applicano fatta salva la possibilità per le autorità competenti di essere informate dei dati relativi alla fatturazione o al traffico in base alla normativa applicabile, ai fini della risoluzione delle controversie, in particolare di quelle attinenti all'interconnessione o alla fatturazione”.

²⁵ V. nota n. 19.

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).

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).

[Sommaro](#)

6. 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 precedente paragrafo.

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 poter comunque 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)²⁶.

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*

²⁶ La categoria dei "dati relativi all'ubicazione" non era contemplata specificamente dall'abrogata direttiva 97/66/CE.

L'art. 10, lett. b), della direttiva 2002/58/CE 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 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. 11.

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. 19).

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).

[Sommar](#)io

7. 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 della chiamata e gli elenchi di abbonati²⁷.

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).

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

²⁷ Per un confronto con la precedente disciplina si rimanda alle corrispondenti disposizioni della direttiva 97/66/CE.

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 *omesso un certo numero di cifre dei numeri chiamati* (considerando 33).

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)²⁸.

²⁸ “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

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).

Il paragrafo 1 dell'art. 8, sopra esaminato, si applica anche alle chiamate

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” (considerando 34).

“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” (considerando 36).

Sul campo di applicazione dell'art. 8 del provvedimento, v. nota n. 11.

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. 19).

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 pubblico²⁹:

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*.

²⁹ Sull'ambito di applicazione dell'art. 10 della direttiva 2002/58/CE, v. nota n. 11.

Trasferimento automatico della chiamata.

“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” (considerando 37).

L'art. 11 della direttiva sulle comunicazioni elettroniche dispone pertanto 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*³⁰.

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 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.

³⁰ Sul campo di applicazione dell'art. 11 del provvedimento, v. nota n. 11.

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)³¹.

[Sommar](#)io

³¹ 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'art. 11 della direttiva 97/66/CE prima dell'entrata in vigore delle disposizioni nazionali adottate conformemente alla direttiva 2002/58/CE (per l'Italia, come si vedrà, ciò vale a dire *anteriamente al primo gennaio 2004*) 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'art. 12 della direttiva in esame (art. 16, par. 2).

CAPITOLO II

IL CODICE DELLA PRIVACY

SOMMARIO: 1. [Premessa](#) – 2. [Definizioni](#) – 3. [Principi generali. Oggetto e ambito di applicazione](#) – 4. [Diritti dell'interessato](#) – 5. [Regole generali per il trattamento dei dati](#) – 6. [Segue: regole ulteriori per i soggetti pubblici](#) – 7. [Segue: il consenso dell'interessato](#) – 8. [Segue: Comunicazione e diffusione dei dati](#) – 9. [Segue: dati sensibili e semisensibili](#) – 10. [Soggetti che effettuano il trattamento](#) – 11. [Sicurezza dei dati e dei sistemi](#) – 11.1. [Misure minime per i trattamenti effettuati con strumenti elettronici](#) – 11.2. [Misure minime per i trattamenti effettuati senza l'ausilio di strumenti elettronici](#) – 12. [Adempimenti](#) – 13. [Trasferimento dei dati all'estero](#)

[INDICE](#)

1. Premessa

Come già si è avuto modo di accennare nel capitolo precedente, l'Italia ha dato attuazione alla direttiva 2002/58/CE sulle comunicazioni elettroniche con una disciplina inserita nel recente [Codice in materia di protezione dei dati personali](#) (D.L.vo 30 giugno 2003 n. 196)¹.

¹ GU 174 del 29 luglio 2003, Suppl. ord. 123. Il testo del provvedimento è consultabile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/codiceprivacy.htm. Cfr. art. 184, comma 1, del provvedimento.

Come può leggersi nella [relazione di accompagnamento al testo del Codice](#) (disponibile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/relazionecodiceprivacy.htm), “Nel 1996, dopo un lungo percorso normativo che ha interessato l’arco di più legislature, il Parlamento ha varato la prima legge italiana di carattere generale sulla tutela delle persone rispetto al trattamento dei dati personali, la n. 675, approvando contestualmente un’articolata legge delega – la n. 676 – per rendere possibile la successiva integrazione e, se necessario, modificazione delle relative disposizioni.

Con tale delega si è così individuato uno strumento risultato poi valido e che, nel corso degli ultimi sei anni, ha permesso di completare gradualmente l’impianto normativo già complesso della protezione dei dati, che è stato progressivamente allineato alla disciplina comunitaria cui si ispirava e a vari accordi e convenzioni internazionali. Ha consentito inoltre di apportare, in determinati casi, alcune correzioni necessarie per la migliore attuazione dei principi affermati nel 1996, anche alla luce dell’esperienza applicativa, significativa ed intensa, via via maturata.

Il Parlamento, il Governo e l’autorità di garanzia istituita in materia hanno cooperato attivamente negli ultimi anni per arricchire e specificare questi strumenti di garanzia e di tutela.

Dall’8 maggio 1997 in poi, tale processo si è sviluppato in particolare attraverso nove decreti legislativi e due dd.P.R., nonché tramite molte altre specifiche disposizioni, legislative e regolamentari, inserite in speciali provvedimenti, che hanno potenziato ulteriormente il congruo numero di norme vigenti in materia.

Il termine per adottare i decreti legislativi integrativi e correttivi della delega è poi scaduto il 31 dicembre 2001.

Tuttavia, il legislatore ha previsto opportunamente, nel 2001, la successiva adozione di un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni ‘connesse’, al fine di coordinarvi le norme vigenti e di apportarvi le integrazioni o modificazioni necessarie sia a tale coordinamento, sia ‘*per assicurarne la migliore attuazione*’ (art. 1, comma 4, legge 24 marzo 2001, n. 127).

Quest’ultimo riferimento alle possibili integrazioni o modificazioni apportabili alle norme riunite nel testo unico, al fine appunto di assicurarne la migliore attuazione (sia di quelle riferite direttamente e strettamente alla protezione dei dati personali, sia delle altre norme ‘connesse’ cui si è già accennato) corrisponde (e, per certi profili, è più ampio) all’analogo riferimento già presente nei criteri di delega per i decreti legislativi correttivi previsti dall’art. 2 della legge di delega n. 676/1996 e che ha permesso, negli ultimi anni, vari interventi di adeguamento su tutto l’arco delle disposizioni della legge n. 675/1996 (non solo sul piano del diritto sostanziale, ma anche sui profili sanzionatori – pene edittali; specificazione di nuovi illeciti – ed organizzativo-istituzionali relativi all’Ufficio del Garante).

Sulla base della nuova delega del 2001 il Governo ha pertanto iniziato un impegnativo processo di monitoraggio delle norme da riunire (direttamente relative alla protezione dei dati o ad essa connesse) sulla base della considerazione che la delega per la riunificazione della disciplina in materia presuppone non solo una ricognizione compilativa delle disposizioni vigenti, ma anche misurati e parziali interventi di armonizzazione e di adeguamento delle norme riunite in un unico testo, nel rispetto delle scelte di fondo già più volte ponderate dal Parlamento, dei connessi principi, del loro ambito applicativo e dell'impianto di garanzia derivante dall'attuale normativa.

Un'apposita commissione di studio costituita da numerosi esperti è stata pertanto istituita presso il Dipartimento per la funzione pubblica, autorevolmente presieduta dal prof. Cesare Massimo Bianca.

Il lavoro di ricognizione e di studio si è rivelato da subito più complesso del previsto e reso più impegnativo anche per effetto dell'intervento, *medio tempore*, di nuove convenzioni e direttive comunitarie – in particolare la n. 2002/58/CE del 12 luglio 2002 –, che ha reso necessario un breve differimento al 30 giugno 2003 del termine di delega (art. 26 della legge 3 febbraio 2003, n. 14).

Invertendo la linea di tendenza di precedenti testi unici 'misti' legislativo-regolamentari, il lavoro della commissione di studio si è poi orientato, da ultimo, verso la diversa prospettiva di un unico testo di rango legislativo, anziché misto, dovendosi (all'epoca della conclusione dei lavori e in futuro) tener conto dei nuovi orientamenti del disegno di legge di semplificazione 2001 (già approvato dalle Camere e attualmente in fase di nuovo esame dopo il rinvio da parte del Presidente della Repubblica: AS 776-B/bis), in tema di riassetto normativo e di codificazione, orientamenti applicabili per effetto di talune disposizioni transitorie anche a determinate deleghe legislative in corso.

Ciò spiega come oggi si proponga opportunamente di adottare un solo testo unico di matrice unicamente legislativa, con conseguente assorbimento o eliminazione di varie disposizioni di rango regolamentare non più necessarie, e con la contestuale previsione di un disciplinare tecnico per le c.d. misure minime di sicurezza, il quale potrà essere flessibilmente adeguato all'evoluzione del settore con decreti ministeriali non regolamentari.

L'adozione di un solo testo di rango legislativo, anziché anche regolamentare, si rivela tra l'altro assai più consono al rango dei diritti e delle libertà fondamentali tutelati dalla disciplina in questione. Permette inoltre di semplificare notevolmente l'impianto, l'articolazione e la 'leggibilità' delle norme che si intende inserire nel testo, essendosi eliminati dal testo delle norme riunite a livello legislativo i vari riferimenti alle disposizioni regolamentari di attuazione (e potendosi fare a meno, viceversa, dei corrispondenti richiami che figurano nelle norme regolamentari attualmente in applicazione).

L'integrazione delle vigenti norme legislative con alcuni dettagli attualmente disciplinati a livello regolamentare consente peraltro di ridurre e semplificare le norme di cui oggi si intende effettuare una riunione, con conseguenti ovvii benefici sul piano sistematico e per l'interprete.

Il testo unico di cui si propone la denominazione convenzionale di 'codice' (in sintonia con gli indirizzi del d.d.l. di semplificazione) recherà in allegato a scopo conoscitivo, nel rispetto di quanto stabilito da vari decreti legislativi già adottati in materia, gli esistenti codici di deontologia e di buona condotta (e quelli che verranno via via inseriti, una volta adottati), la cui allegazione (ritenuta indispensabile in ossequio all'art. 20, comma 4, del d.lg. n. 467/2001, nonché per esigenze di agevole conoscenza della materia) non fa mutare le caratteristiche giuridiche – non legislative – di questa nuova fonte.

Il rispetto delle disposizioni dei codici di deontologia e di buona condotta resta, per espressa previsione di rango legislativo introdotta da precedenti decreti legislativi, *'essenziale'* per determinare la liceità del trattamento dei dati personali ivi disciplinato, sebbene i codici continueranno a venire a giuridica esistenza – e ad essere eventualmente emendati – secondo i noti meccanismi procedurali non legislativi già osservati e che coinvolgono le entità maggiormente rappresentative del settore considerato.

Il *'codice'* reca anzitutto alcune nuove disposizioni direttamente connesse al quadro comunitario e internazionale, per aggiornare quanto già contenuto nel decreto legislativo n. 171/1998 alle nuove regole della direttiva n. 2002/58/CE e per completare o perfezionare il recepimento della direttiva n. 95/46/CE/CE (ad esempio, relativamente al principio di stabilimento e alla legge applicabile, o per taluni aspetti relativi ai flussi transfrontalieri di dati personali, ai numeri di identificazione personale e ai dati sensibili).

Il lavoro di ricognizione delle norme da riunire nel *'codice'* ha interessato molte altre disposizioni non modificate, integrate o aggiornate nel testo.

Ciò in quanto, pur ricorrendo i presupposti per un loro inserimento nel *'codice'*, si è ritenuto in linea generale – salvi specifici casi – proporzionato e ragionevole, e in sintonia con lo spirito della delega, non alterare la coerenza interna di altri testi normativi organici che, al loro interno, recano norme rilevanti in tema di tutela della riservatezza.

Ci si riferisce, in particolare, a disposizioni incriminative del codice penale, oppure a previsioni contenute in altri testi unici di cui non si è ravvisata necessaria una modifica e per le quali, dovendosi determinare la loro futura collocazione sistematica, è stata valutata l'esigenza di assicurare la contrapposta omogeneità o del testo unico di settore già vigente o in fase di preparazione (documentazione amministrativa; enti locali; pubblico impiego; igiene e sicurezza del lavoro; ecc.) oppure (in caso di stralcio da tali testi unici delle norme sulla *privacy* da collocare nell'odierno *'codice'*), del *'codice'* sulla protezione dei dati personali.

Sul piano sistematico, prima ancora di valutare la collocazione dei vari precetti, si è ritenuto doveroso porre in maggiore evidenza nella parte iniziale del *'codice'* le disposizioni generali riguardanti i diritti e le libertà fondamentali, le principali generali garanzie e le connesse sfere di responsabilità. Ciò tenendo conto dell'erronea tendenza registratasi in passato, volta ad enfatizzare – e, talvolta, a drammatizzare – i profili legati a taluni adempimenti a carico del titolare del trattamento.

Si è voluto così, come si vedrà a proposito dell'art. 2 del codice, valorizzare gli aspetti di garanzia della persona e burocratizzare, altresì, quelli concernenti gli adempimenti formali e le stesse modalità di esercizio dei diritti, che si è voluto entrambi ispirare meglio ai principi di semplificazione ed efficacia, senza pregiudizio alcuno per i livelli di garanzia.

Altre disposizioni non sono state poi riassorbite nell'alveo del codice in quanto (ad esempio, alcune norme della legge sull'AIDS) disciplinano taluni profili di tutela della riservatezza in stretta connessione con altri aspetti che non possono, *ratione materiae*, essere qui collocati. Analogamente, si è ritenuto inopportuno inserire nel codice specifici decreti di interesse *'interno'* di una sola, specifica amministrazione pubblica (es.: decreti o regolamenti di ricognizione dei dati sensibili) che, inglobati nel testo, avrebbero portato il *'codice'* a dimensioni elefantache, comprensive degli innumerevoli decreti adottati da tutte le amministrazioni pubbliche.

Si è voluto infine strutturare meglio la successione delle disposizioni applicabili da un lato ai soli soggetti pubblici e, dall'altro, ai privati – compresi i concessionari di pubblici servizi – e agli enti

Detto “testo unico”, entrato in vigore *il primo gennaio 2004*, abroga e sostituisce, tra l’altro, la nota [legge 675/1996](#) sulla privacy² nonché il già ricordato D.L.vo 171/1998 di attuazione della direttiva 97/66/CE.

L’art. 184 del provvedimento stabilisce infatti che “Quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31

pubblici economici, in modo da ridurre le possibili sviste nel considerare applicabili agli uni o agli altri disposizioni cogenti solo per taluni di essi.

L’attività di semplificazione ha permesso di ridurre di una buona percentuale, stimabile attorno al 30% circa, il numero delle disposizioni vigenti in materia (stima effettuata confrontando le vecchie e nuove disposizioni e tenendo conto delle molteplici norme del tutto innovative, nonché della frammentazione di attuali lunghi articoli in articoli composti di un solo comma).

Analoga semplificazione, anche in questo caso senza alcuna incidenza nei livelli di garanzia, è stata perseguita a proposito dell’illustrazione normativa delle varie ipotesi di esercizio dei diritti (art. 7), per i tempi per l’espressione di pareri (art. 154, comma 5), per la possibilità di esprimerli anche su schemi-tipo di provvedimento (es., art. 20, comma 2: in modo da facilitarne l’utilizzo da parte di più soggetti), sui modelli-tipo per la presentazione di reclami (art. 143, comma 3), ecc.

Da ultimo, sono stati apportati alcuni interventi sul ‘linguaggio’ del codice, laddove necessario e possibile in rapporto anche alla normativa comunitaria, tenuto conto, al contempo, dell’opposta esigenza di non innovare rispetto a nozioni ed espressioni da tempo entrate nell’applicazione quotidiana e nel linguaggio comune degli operatori”.

In generale, sul Codice della privacy si veda *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, a cura di R. Acciai, Rimini, Maggioli Editore, 2004; *Guida al Codice della privacy. La protezione dei dati personali alla luce del D.Lgs. 196/2003*, a cura di M. De Giorgi e A. Lisi, Napoli, Ed. Simone, 2003; G. Stumpo, *Il Testo Unico Privacy: analisi sintetica dei contenuti principali*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_privacy/stumpo.html; *Codice in materia di Protezione dei Dati Personali. Commentato per articolo*, a cura di M. Iaselli, in *Studiocelentano.it*, www.studiocelentano.it, www.studiocelentano.it/codici/privacy; G. Santaniello, *Il Codice italiano della privacy nella prospettiva europea*, in *InterLex*, www.interlex.it, www.interlex.it/675/santaniello8.htm; con particolare riferimento alla professione forense: G. Riem, *Brevi note in tema di adempimenti privacy nell’esercizio dell’attività forense dopo l’entrata in vigore del decreto legislativo 196/03*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6857; Atti dell’incontro sul tema “Privacy e studi legali. Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico”, organizzato dal Gruppo di Iniziativa Forense, Verona, 27 febbraio 2004, disponibili su www.iusondemand.com/ebook.

² 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 e successive modifiche (testo del provvedimento consultabile su www.iusreporter.it all’indirizzo www.iusreporter.it/Testi/legge675-1996.htm).

dicembre 1996, n. 675, e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice secondo la tavola di corrispondenza riportata in allegato”³.

Il Codice della privacy si compone di *tre parti*, che contengono, rispettivamente:

I) le *disposizioni generali* (artt. 1-45) riguardanti le regole "sostanziali" della disciplina del trattamento dei dati personali, *applicabili a tutti i trattamenti*, salvo eventuali *regole specifiche* per i trattamenti effettuati da soggetti pubblici o privati (art. 6);

II) *disposizioni particolari per specifici trattamenti* (artt. 46-140) *ad integrazione o eccezione alle disposizioni generali della parte I*;

III) le *disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio* (artt. 141-186)⁴.

Completano il testo normativo una serie di allegati:

- allegato A, relativo ai *codici di condotta*;
- allegato B, recante il *disciplinare tecnico in materia di misure minime di sicurezza*;
- allegato C, relativo ai *trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia* (peraltro non ancora pubblicato).

Il titolo X (“Comunicazioni elettroniche”) della parte II del Codice (artt. 121-134)

³ Restano d'altra parte ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali (art. 184, comma 3, del Codice).

⁴ Il titolo IV della parte III (artt. 173-186) reca “Disposizioni modificative, abrogative, transitorie e finali”.

contiene la disciplina di attuazione della direttiva 2002/58/CE⁵. Stante quanto sopra, alle *comunicazioni elettroniche* si applicheranno dunque le disposizioni generali contenute nella parte I del Codice salvo quanto per esse diversamente previsto nel titolo X della parte II.

Prima di esaminare le norme specificamente dettate per le comunicazioni elettroniche si rende pertanto indispensabile soffermarsi preliminarmente sulle disposizioni generali di cui alla prima parte del Codice della privacy.

[Sommaro](#)

2. Definizioni

Le *definizioni* valevoli *ai fini del Codice della privacy* vengono elencate come segue dall'art. 4 del provvedimento⁶.

a) *Trattamento*: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati.

Rispetto alla definizione accolta dalla previgente L. 675/1996, val la pena sottolineare che è stato precisato espressamente che nella nozione di trattamento

⁵ Salvo per quanto riguarda, come si vedrà, la materia della sicurezza, regolata dalla parte I.

⁶ Cfr. art. 2 [direttiva 95/46/CE](#); art. 1 L. 675/1996.

Segnala lo “scarso rigore definitorio adottato dal legislatore” A. Monti, *Decreto legislativo 196/03: l'internet non è una rete*, in *InterLex*, www.interlex.it, www.interlex.it/675/amonti69.htm.

devono essere fatte rientrare anche le operazioni relative a dati *non registrati in una banca dati*, come definita dalla successiva lettera p).

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.

Con riferimento ad Internet, possono dunque essere fatti rientrare nell'ampia nozione di "dato personale" rilevante ai fini del testo unico, ad esempio, il *domain name*, l'*indirizzo IP*, i *cookie*, il *nickname* e, come si vedrà meglio trattando di spamming, l'*account di posta elettronica*⁷.

c) *Dati identificativi*: i dati personali che permettono l'identificazione diretta dell'interessato⁸.

d) *Dati sensibili*: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale⁹.

e) *Dati giudiziari*: i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di

⁷ Cfr. A. Lisi, *La tutela della privacy in Internet* cit., p. 38 e s.

⁸ Cfr. art. 10, comma 5, D.L.vo 30 luglio 1999, n. 281, *Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica*, GU 191 del 16 agosto 1999.

⁹ Cfr. art. 22, comma 1, L. 675/1996.

indagato ai sensi degli articoli 60 e 61 del codice di procedura penale¹⁰.

f) *Titolare*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Rispetto alla definizione adottata dalla L. 675/1996, si prevede espressamente la possibilità che più soggetti siano *co-titolari* del medesimo trattamento.

g) *Responsabile*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

h) *Incaricati*: le *persone fisiche* autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile¹¹.

i) *Interessato*: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

l) *Comunicazione*: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

m) *Diffusione*: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

¹⁰ Cfr. art. 24, comma 1, L. 675/1996.

¹¹ Cfr. art. 19 L. 675/1996.

n) *Dato anonimo*: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

o) *Blocco*: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

p) *Banca di dati*: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

q) *Garante*: l'autorità di cui all'art. 153 del Codice, istituita dalla L. 675/1996.

Inoltre, come indicato nella relazione di accompagnamento al Codice, il secondo comma dell'art. 4 “contiene le definizioni necessarie per i trattamenti effettuati nell'ambito delle comunicazioni elettroniche (cfr. in particolare, Parte II, Titolo X), le quali riproducono pressoché pedissequamente le definizioni riportate nella direttiva n. 2002/58/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche, nonché quelle, espressamente richiamate, della direttiva ‘quadro’ n. 2002/21/CE in materia di reti e servizi di comunicazione elettronica. Al riguardo va rilevato che la definizione di ‘comunicazione’ di cui alla citata direttiva 2002/58 è riferita, nel testo, alla ‘comunicazione elettronica’ per distinguerla dalla ‘comunicazione’ tout court di cui al comma 1 dell'articolo in commento”.

Queste dunque le definizioni per le *comunicazioni elettroniche*¹².

¹² Cfr. art. 2 direttiva 2002/58/CE e art. 2 direttiva 2002/21/CE (cap. I, par. 2).

Il D.L.vo 171/1998 di attuazione della direttiva 97/66/CE forniva invece, all'art. 1, le definizioni che seguono.

“Ai fini del presente capo, si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini, si intende per:

a) *Comunicazione elettronica*: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile¹³.

b) *Chiamata*: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale.

c) *Reti di comunicazione elettronica*: i sistemi di trasmissione, 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

a) 'abbonato': 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;

b) 'utente': la persona fisica che utilizza uno o più servizi di telecomunicazioni accessibili al pubblico, indipendentemente dall'eventuale qualità di abbonato;

c) 'rete pubblica di telecomunicazioni': un sistema di trasmissione e, se del caso, le apparecchiature di commutazione o le altre risorse che permettono la trasmissione di segnali tra punti terminali di rete definiti, con mezzi a filo, radio, ottici o altri mezzi elettromagnetici utilizzati, in tutto o in parte, per fornire servizi di telecomunicazioni accessibili al pubblico;

d) 'servizio di telecomunicazioni': un servizio la cui fornitura consiste, in tutto o in parte, nella trasmissione e nell'instradamento di segnali su reti di telecomunicazioni, ivi compreso qualunque servizio interattivo anche se relativo a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi".

¹³ A proposito della definizione di "comunicazione elettronica" fornita dal Codice della privacy, in rapporto alla definizione di "comunicazione" di cui al medesimo provvedimento, è stato osservato che "sarebbe stato logico considerare la locuzione 'comunicazione elettronica' una specie del genere 'comunicazione'. Così concludendo che la comunicazione elettronica è quella comunicazione veicolata tramite una rete di comunicazione elettronica. Ma la lettura della norma evidenzia una scelta diversa del legislatore che – trasferendo nel testo normativo una comune ambiguità del linguaggio corrente – 'trasforma' il 'mezzo' in 'messaggio'. E così, l'aggiunta dell'aggettivo 'elettronica' al sostantivo 'comunicazione' trasforma il concetto risultante da azione pura e semplice (art. 4 comma 1 lett. l) nell'oggetto della stessa" (A. Monti, *Decreto legislativo 196/03: il senso delle parole*, in *InterLex*, www.interlex.it, www.interlex.it/675/amonti70.htm).

elettromagnetici, incluse 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 sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

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

e) *Servizio di comunicazione elettronica*: i servizi 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, nei limiti previsti dall'art. 2, lett. c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002¹⁴.

f) *Abbonato*: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate.

g) *Utente*: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

h) *Dati relativi al traffico*: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o

¹⁴ Sui limiti di cui alla direttiva 2002/21/CE, v. cap. I, par. 2.

della relativa fatturazione.

i) *Dati relativi all'ubicazione*: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.

l) *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.

m) *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.

Infine, e sempre ai fini del Codice, in materia di *sicurezza* si intende, altresì, per¹⁵:

a) *Misure minime*: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31.

b) *Strumenti elettronici*: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

¹⁵ Cfr. DPR 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. Il testo del provvedimento – abrogato dal Codice della privacy – è consultabile su www.privacy.it all'indirizzo www.privacy.it/dpr1999-318.html.

c) *Autenticazione informatica*: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

d) *Credenziali di autenticazione*: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

e) *Parola chiave*: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

f) *Profilo di autorizzazione*: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

g) *Sistema di autorizzazione*: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

[Sommaro](#)

3. Principi generali. Oggetto e ambito di applicazione

Il Codice della privacy pone innanzitutto il principio fondamentale, informatore di tutto il testo unico, secondo cui *chiunque ha diritto alla protezione dei dati personali che lo riguardano* (art. 1).

Come affermato nella relazione di accompagnamento al provvedimento, l'art. 1 introduce nell'ordinamento giuridico italiano il "*diritto alla protezione dei dati personali*", *diritto fondamentale della persona*, autonomo rispetto al più generale

diritto alla riservatezza già richiamato dall'art. 1 L. 675/1996, come chiarisce anche il successivo art. 2.

“Un diritto che tiene conto delle molteplici prerogative legate al trattamento dei dati personali, anche oltre quelle attinenti al riserbo e alla tutela della vita privata. In tal modo il legislatore italiano si adegua al quadro normativo comunitario che, nella Carta dei diritti del cittadino europeo, garantisce già tale diritto fondamentale (art. 8) che si accinge ad assumere una connotazione ancora più solenne nel quadro dei lavori della Convenzione europea”¹⁶.

In base all'art. 2 (“Finalità”), il Codice mira a garantire che il trattamento dei dati personali si svolga nel *rispetto dei diritti e delle libertà fondamentali*, nonché della *dignità dell'interessato*, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali¹⁷. Inoltre, il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui sopra nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento (*principio di semplificazione nell'elevata tutela*).

Secondo il *principio di necessità nel trattamento dei dati* introdotto dall'art. 3, *i sistemi informativi e i programmi informatici* devono essere configurati *riducendo*

¹⁶ L'art. 8 (“Protezione dei dati di carattere personale”) della *Carta dei diritti fondamentali dell'Unione europea* (www.europarl.eu.int/charter/pdf/text_it.pdf) prevede quanto segue.

“1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente”.

¹⁷ Cfr. art. 1 direttiva 95/46/CE; art. 1, comma 1, L. 675/1996.

al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Il principio introdotto integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati (cfr. art. 11). Si tratta di una regola di ordine generale, operante, benché non specificamente sanzionata, in specie per i sistemi e i programmi che verranno d'ora in poi predisposti¹⁸.

Con riguardo *all'oggetto e all'ambito di applicazione* del Codice della privacy, l'art. 5¹⁹ stabilisce che il testo unico disciplina il trattamento di dati personali, *anche detenuti all'estero*, effettuato da *chiunque è stabilito nel territorio dello Stato* o in un luogo comunque soggetto alla sovranità dello Stato.

Il Codice si applica anche al trattamento di dati personali effettuato da *chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici*, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.

In caso di applicazione del Codice, il titolare del trattamento deve designare un proprio *rappresentante stabilito nel territorio dello Stato* ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

¹⁸ Così la relazione di accompagnamento al testo del Codice.

¹⁹ Cfr. art. 4 direttiva 95/46/CE; artt. 2 e 6 L. 675/1996.

Il provvedimento conferma altresì che il *trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali* è soggetto all'applicazione del Codice solo se i dati sono destinati ad una *comunicazione sistematica o alla diffusione*. Si applicano d'altra parte anche al trattamento svolto per fini esclusivamente personali le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli artt. 15 e 31 del Codice²⁰.

Sommario

4. Diritti dell'interessato

Il titolo II della parte I (“Disposizioni generali”) del Codice della privacy (artt. 7-10) regola i *diritti dell'interessato*, come definito dal già esaminato art. 4.

In base all'art. 7 (“Diritto di accesso ai dati personali ed altri diritti”)²¹, comma 1, del provvedimento, l'interessato ha dunque, innanzitutto, *diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile*.

In base al secondo comma della medesima disposizione, l'interessato ha inoltre diritto di ottenere l'indicazione:

a) dell'origine dei dati personali che lo riguardano;

b) delle finalità e modalità del trattamento;

²⁰ Cfr. art. 3 direttiva 95/46/CE; art. 3 L. 675/1996.

Sugli artt. 15 (“Danni cagionati per effetto del trattamento”) e 31 (“Obblighi di sicurezza”) del Codice si veda quanto si dirà in proposito nei successivi paragrafi.

²¹ Cfr. art. 12 direttiva 95/46/CE; art. 13 L. 675/1996.

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Per quanto riguarda l'individuazione dei diritti dell'interessato, afferma la relazione di accompagnamento al Codice, rispetto alla normativa previgente l'art. 7, comma 1, lett. e) attribuisce, in più, all'interessato il diritto di conoscere i soggetti ai quali i dati possono essere comunicati o che ne possono comunque venire a conoscenza²².

L'interessato ha altresì diritto di ottenere (art. 7, comma 3):

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

²² “La norma dà attuazione all'art. 12, par. 1, lett. a), primo punto, della direttiva 95/46/CE e completa il quadro dei diritti dell'interessato in ordine al diritto di conoscere in sede di accesso i soggetti cui i dati possono essere comunicati, mentre la legge n. 675/1996 prevedeva soltanto il diritto di essere previamente informati sui soggetti ‘destinatari’ dei dati medesimi (art. 10, comma 1, lett. d), l. n. 675/1996 e analoga disposizione dell'art. 13 del codice)” (così la relazione di accompagnamento al Codice).

c) l'attestazione che le operazioni di cui alle precedenti lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha, infine, *diritto di opporsi*, in tutto o in parte (art. 7, comma 4):

a) per *motivi legittimi* al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) *al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale*²³.

I successivi articoli del titolo I regolano poi l'esercizio dei diritti riconosciuti dall'art. 7.

²³ L'art. 7 adegua pertanto alla direttiva 95/46/CE la disposizione che prevede il diritto dell'interessato di opporsi al trattamento dei propri dati personali effettuato per finalità di *marketing* o di *ricerche di mercato*, eliminando in questa sede l'ulteriore riferimento ad essere informato del medesimo trattamento, ridondante rispetto alla direttiva comunitaria e all'obbligo di informativa già previsto a carico del titolare.

Inoltre, rileva la relazione di accompagnamento al Codice, dal testo è stato espunto il riferimento alle *informazioni commerciali*, inconfidente rispetto allo specifico profilo in esame (art. 7, comma 4, lett. b), del Codice, già art. 13, lett. e), L. 675/1996).

In tema di diritti dell'interessato, si ricorda altresì quanto disposto dall'art. 14 del Codice ("Definizione di profili e della personalità dell'interessato").

"1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17".

Secondo quanto previsto dall'art. 8 ("Esercizio dei diritti"), dunque, i diritti di cui all'art. 7 appena esaminato sono esercitati con *richiesta rivolta senza formalità al titolare o al responsabile del trattamento*, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo²⁴.

D'altra parte, i diritti di cui all'art. 7 *non* possono essere esercitati con richiesta al titolare o al responsabile o con ricorso al Garante ai sensi dell'art. 145 del Codice²⁵, se i trattamenti di dati personali sono effettuati nei casi elencati dal secondo comma dell'art. 8.

Tra le ipotesi ivi previste, vi è in particolare quella del trattamento effettuato da *fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata*, salvo che possa derivarne un *pregiudizio effettivo e concreto*²⁶ per lo svolgimento delle investigazioni

²⁴ Cfr. art. 13 direttiva 95/46/CE; art. 14 L. 675/1996; art. 17 DPR 31 marzo 1998, n. 501, *Regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'articolo 33, comma 3, della L. 31 dicembre 1996, n. 675*, GU Serie gen. 25 dell'1 febbraio 1999. Il testo del provvedimento può essere consultato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/dpr501-1998.htm.

²⁵ Sui ricorsi al Garante si veda il cap. V.

²⁶ "Un'importante chiarimento riguarda la nozione di 'pregiudizio' richiamata dall'art. 14 della legge n. 675/1996 in relazione ai limiti all'esercizio dei diritti dell'interessato. In base a tale disposizione, infatti, il pregiudizio è rilevante al duplice fine:

a) di 'differire' l'accesso ai dati personali in caso di pregiudizio per lo svolgimento di investigazioni difensive o per l'esercizio di un diritto;

b) di consentire, viceversa, il medesimo accesso ai dati relativi a chiamate in entrata (altrimenti non accessibili), in presenza di un pregiudizio riguardante lo svolgimento delle medesime indagini.

L'art. 8, nel confermare tale disciplina, ha precisato che il pregiudizio deve essere 'effettivo e concreto'. Il chiarimento è il frutto dell'esperienza applicativa di questi primi anni, che ha visto verificarsi tentativi di applicazione della norma in disarmonia con quanto previsto da alcune disposizioni del d.lg. n. 171/1998 che tutelano l'utente chiamante e quello chiamato, e risponde ad una prassi interpretativa già sperimentata e applicata anche dal Garante nell'ambito di vari procedimenti instaurati con ricorso" (così la relazione di accompagnamento al Codice).

difensive di cui alla legge 7 dicembre 2000, n. 397²⁷.

L'esercizio dei diritti di cui all'art. 7, quando *non riguarda dati di carattere oggettivo*, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento (art. 8, comma 4).

L'art. 9 ("Modalità di esercizio")²⁸ del Codice prevede che la richiesta rivolta al titolare o al responsabile *ex art. 8* possa essere trasmessa anche mediante *lettera raccomandata, telefax o posta elettronica*. Il Garante può d'altra parte individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche.

Quando riguarda l'esercizio dei diritti di cui all'art. 7, commi 1 e 2, sopra esaminati, la richiesta può essere formulata anche *oralmente* e in tal caso è *annotata sinteticamente* a cura dell'incaricato o del responsabile.

Nell'esercizio dei diritti di cui all'art. 7, l'interessato può conferire, *per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi*. L'interessato può, altresì, *farsi assistere da una persona di fiducia*.

L'identità dell'interessato deve essere verificata sulla base di *idonei elementi di valutazione*, anche mediante atti o documenti disponibili o esibizione o

²⁷ Il Garante, anche su segnalazione dell'interessato, in siffatta ipotesi provvede nei modi di cui agli artt. 157, 158 e 159 del Codice.

²⁸ Cfr. art. 13 L. 675/1996; art. 17 DPR 501/1998.

allegazione di copia di un documento di riconoscimento (art. 9, comma 4)²⁹. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

La richiesta di cui all'art. 7, commi 1 e 2, sopra esaminati, deve essere formulata *liberamente e senza costrizioni* e può essere *rinnovata*, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Al fine di garantire l'effettivo esercizio dei diritti di cui all'art. 7, il titolare del trattamento è tenuto ad adottare *idonee misure* volte, in particolare (art. 10, comma 1)³⁰:

- a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
- b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero

²⁹ La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.

³⁰ Cfr. art. 13 L. 675/1996; art. 17 DPR 501/1998.

alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato deve comprendere *tutti i dati personali* che riguardano l'interessato *comunque trattati* dal titolare³¹.

Sommario

³¹ Quando l'estrazione dei dati risulti particolarmente difficoltosa, l'art. 10, comma 4, consente che il riscontro alla richiesta dell'interessato possa avvenire *anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti*.

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda *dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato* (art. 10, comma 5).

La comunicazione dei dati è effettuata in *forma intelligibile* anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle devono essere forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato (art. 10, comma 6).

Quando, a seguito della richiesta di cui all'art. 7, commi 1 e 2, lettere a), b) e c) *non risulta confermata l'esistenza di dati* che riguardano l'interessato, può essere chiesto un *contributo spese* non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico. Detto contributo non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato. Il contributo è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e *comunque non oltre quindici giorni da tale riscontro* (art. 10, commi 7 e 8).

5. Regole generali per il trattamento dei dati

Il titolo III della parte I del D.L.vo 196/2003 detta le *regole generali per il trattamento dei dati*, distinguendo tra *regole per tutti i trattamenti* (capo I), *regole ulteriori per i soggetti pubblici* (capo II), *regole ulteriori per privati ed enti pubblici economici* (capo III)³².

Modalità del trattamento e requisiti dei dati.

Con riguardo alle regole valide per tutti i trattamenti contenute nel capo I, l'art. 11, conformemente alla legge 675/1996³³, stabilisce innanzitutto che i dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

³² In ordine alle sanzioni riconnesse dal Codice alla violazione di alcune delle norme che si vanno ad illustrare, si rimanda al cap. V.

³³ Cfr. art. 6 direttiva 95/46/CE; art. 9 L. 675/1996.

L'ultimo comma della disposizione in esame introduce il *divieto di utilizzare – in qualsiasi modo – i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali*.

Codici di deontologia e di buona condotta.

L'art. 12 disciplina i *codici di deontologia e di buona condotta*³⁴.

Al Garante viene infatti affidato il compito di promuovere, nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, nonché di verificare la conformità di detti codici alle leggi e ai regolamenti, anche attraverso l'esame di osservazioni di soggetti interessati e di contribuire a garantirne la diffusione e il rispetto.

Si prevede che *l'osservanza delle disposizioni contenute nei codici di deontologia e di buona condotta costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici*³⁵.

Il ricorso ai codici di deontologia e di buona condotta pone dunque alcune rilevanti e delicate questioni. Tra queste, quella relativa all'applicabilità dei

³⁴ Cfr. art. 27 direttiva 95/46/CE; art. 31 L. 675/1996; art. 20 [D.L.vo 28 dicembre 2001, n. 467](#), *Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della legge 24 marzo 2001, n. 127*, GU 13 del 16 gennaio 2002 (il testo del provvedimento può essere consultato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/doc-privacy-467-2001.htm).

³⁵ I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del Codice della privacy (il quale attualmente reca i codici di deontologia relativi al trattamento di dati personali nell'esercizio dell'attività giornalistica, per scopi storici e per scopi statistici in ambito SISTAN).

suddetti codici anche nei confronti di coloro che non li hanno sottoscritti³⁶.

Informativa.

Per ciò che concerne l'*informativa* che deve essere fornita all'interessato, l'art. 13 del Codice³⁷ stabilisce che quest'ultimo o la persona presso la quale sono raccolti i dati personali devono essere *previamente informati oralmente o per iscritto* circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

³⁶ “Se, infatti, il codice deontologico vincolasse soltanto gli aderenti allora si creerebbe una inaccettabile ‘doppia misura’ della responsabilità penale. Che vedrebbe favoriti (o penalizzati) coloro che non accettano di conformarsi allo stato di fatto.

Se, al contrario, il codice deontologico avesse validità *erga omnes* allora non si capirebbe la ragione del garantire a un gruppo ristretto di aziende private una vera e propria potestà legislativa in materia penale. Creando, ancora una volta, disparità di trattamento e, con buona probabilità, un serio sconvolgimento di quei principi penalistici che, fino a oggi, sembravano oramai *jus receptum*”.

Così A. Monti, *Codici deontologici: se chi ruba i dati può scrivere le regole*, in *InterLex*, www.interlex.it, www.interlex.it/675/amonti68.htm.

³⁷ Cfr. art. 10 direttiva 95/46/CE; art. 10 L. 675/1996.

“Nell'art. 13, comma 1, che riguarda l'informativa all'interessato, il diritto di quest'ultimo di venire a conoscenza dell'ambito di comunicazione dei dati che lo riguardano è conformato alla ‘nuova’ definizione di comunicazione di cui si è detto sopra (art. 13, comma 1, lett. d)) e sono chiarite, per dirimere ogni eventuale altro dubbio interpretativo, le modalità con le quali deve essere indicato il responsabile del trattamento, ove designato (art. 13, comma 1, lett. f)).

Inoltre, si prevede che il Garante possa individuare modalità semplificate per l'informativa all'interessato, in particolare quando essa è resa da *call-center*. Tale previsione tiene conto dell'avvertita esigenza di assicurare, in maniera agevole, il rispetto dell'obbligo di fornire l'informativa anche per trattamenti in cui il contatto diretto con l'interessato non vede quest'ultimo fisicamente presente.

Al comma 4, in attuazione di una specifica previsione della direttiva europea n. 95/46, si è previsto che, quando l'informativa riguarda dati non raccolti presso l'interessato, essa deve contenere anche le ‘*categorie di dati trattati*’ (art. 11, par. 1, lett. c), dir. 95/46/CE).

Al comma 5, si è precisato che il Garante può prescrivere misure appropriate a garanzia dell'interessato quando l'informativa non è dovuta perché comporta un impiego di mezzi che il Garante stesso giudichi manifestamente sproporzionati o risulti impossibile (come è avvenuto ad esempio in caso di cartolarizzazione)” (così la relazione di accompagnamento).

- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'art. 7 esaminati nel paragrafo precedente;
- f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'art. 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando altresì il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, è indicato tale responsabile³⁸.

Se i dati personali *non* sono raccolti presso l'interessato, l'informativa, *comprensiva delle categorie di dati trattati*, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre

³⁸ L'informativa di cui nel testo deve contenere anche gli ulteriori elementi eventualmente previsti da specifiche disposizioni del Codice e *può non comprendere* (art. 13, comma 2):

- gli elementi già noti alla persona che fornisce i dati
- o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Il Garante può individuare con proprio provvedimento *modalità semplificate* per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

la prima comunicazione (art. 13, comma 4)³⁹.

In ambito Internet, è utile richiamare anche, quale ausilio interpretativo, la raccomandazione 2/2001 relativa ai *requisiti minimi per la raccolta di dati on-line nell'Unione europea* adottata dal Gruppo europeo per la tutela delle persone con riguardo al trattamento dei dati personali⁴⁰.

Danni cagionati per effetto del trattamento.

L'art. 15 del Codice⁴¹ disciplina l'importante aspetto dei *danni cagionati per effetto del trattamento di dati personali*, prevedendo che, come già disposto dalla previgente L. 675/1996, "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile".

Come è noto, l'art. 2050 cod. civ. disciplina la responsabilità extracontrattuale per l'esercizio di *attività pericolose*, addossando a colui che voglia andare esente da responsabilità risarcitoria l'arduo onere di provare *di avere adottato tutte le*

³⁹ La disposizione di cui al comma 4 dell'art. 13, richiamata nel testo, *non si applica* quando (art. 13, comma 5):

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

⁴⁰ Il testo della raccomandazione può essere consultato su www.privacy.it all'indirizzo www.privacy.it/grupriracc200102.html.

⁴¹ Cfr. art. 23 direttiva 95/46/CE; art. 18 L. 675/1996.

misure idonee a evitare il danno.

Infatti, il danneggiato avrà in questo caso soltanto l'onere di provare l'esistenza di un danno ed il nesso di causalità tra questo ed il comportamento del soggetto che si assume lo abbia provocato.

Problemi si pongono allorché si voglia stabilire in cosa consista effettivamente la prova liberatoria richiesta dall'art. 2050 cod. civ. con riferimento al trattamento di dati personali⁴².

Viene altresì confermata⁴³ dalla disposizione del Codice in esame la risarcibilità, oltre che del danno patrimoniale (danno emergente e lucro cessante), anche del *danno non patrimoniale* in caso di violazione dell'art. 11 sopra illustrato.

Cessazione del trattamento.

In caso di *cessazione, per qualsiasi causa, del trattamento*, l'art. 16, comma 1, del Codice prevede che i dati debbano essere⁴⁴:

a) distrutti;

⁴² Si veda in proposito M.P. Berlingieri, *La responsabilità civile derivante dal trattamento dei dati personali: natura giuridica, conseguenze, oneri probatori*, in *Privacy.it*, www.privacy.it, www.privacy.it/berlingieri04.html.

⁴³ Cfr. art. 29, comma 9, L. 675/1996.

⁴⁴ Cfr. art. 19 direttiva 95/46/CE; art. 16 L. 675/1996.

“All'art. 16, è stato opportunamente precisato che in caso di cessazione dei trattamenti i dati possono essere ceduti ad altro titolare, purché destinati ad un trattamento ‘*in termini compatibili*’ agli scopi originariamente perseguiti, e non più ‘*per finalità analoghe*’, così omologando la disposizione a quanto previsto per il trattamento effettuato da un unico titolare in base al principio di compatibilità del trattamento dei dati (art. 11, comma 1, lett. b), già 9, comma 1, lett. b), l. n. 675/1996)” (così la relazione di accompagnamento).

b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'art. 12.

La cessione dei dati in violazione di quanto previsto dal comma 1, lett. b), dell'art. 16 o di altre disposizioni rilevanti in materia di trattamento dei dati personali è *priva di effetti* (art. 16, comma 2).

[Sommaro](#)

6. *Segue*: regole ulteriori per i soggetti pubblici

Le disposizioni successive (artt. 18-22) dettano alcune *regole ulteriori per i trattamenti effettuati da soggetti pubblici*. Le disposizioni riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

L'art. 18 pone innanzitutto alcuni *principi applicabili a tutti i trattamenti di dati personali effettuati da soggetti pubblici*⁴⁵.

Come già previsto dalla precedente disciplina, qualunque trattamento di dati personali da parte di soggetti pubblici è consentito *soltanto per lo svolgimento delle funzioni istituzionali* (art. 18, comma 2). Nel trattare i dati il soggetto

⁴⁵ Cfr. art. 27 L.675/1996.

pubblico osserva i presupposti e i limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

Salvo quanto previsto nella parte II del Codice della privacy per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, viene espressamente sancito che *i soggetti pubblici non devono richiedere il consenso dell'interessato*. Si osservano d'altra parte le disposizioni di cui all'art. 25 del testo unico in tema di comunicazione e diffusione dei dati⁴⁶.

L'art. 19⁴⁷ pone poi alcuni *principi applicabili al solo trattamento di dati diversi da quelli sensibili e giudiziari*, ai quali, come si vedrà, è riservata una disciplina apposita.

Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è dunque consentito, fermo restando quanto previsto dall'art. 18, comma 2 (svolgimento delle funzioni istituzionali), *anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente*⁴⁸.

L'art. 20 del Codice detta i *principi applicabili al trattamento di dati sensibili* da parte di soggetti pubblici⁴⁹, sancendo che detto trattamento è *consentito solo se*

⁴⁶ Sulla comunicazione e diffusione dei dati, v. par. 8.

⁴⁷ Cfr. art. 7, par. 1, lett. e), direttiva 95/46/CE; art. 27 L. 675/1996.

⁴⁸ La *comunicazione* da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono invece ammesse unicamente quando sono previste da una norma di legge o di regolamento.

⁴⁹ Sulla definizione di *dati sensibili* si rimanda al par. 2. Cfr. art. 8 direttiva 95/46/CE; art. 22 L. 675/1996; art. 5 D.L.vo 135/1999, *Disposizioni integrative della legge 31 dicembre 1996, n. 675*,

*autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite*⁵⁰.

Con riguardo al *trattamento di dati giudiziari da parte di soggetti pubblici*, l'art. 21⁵¹ prevede che esso sia consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

L'art. 22 detta infine alcuni *principi applicabili sia al trattamento di dati sensibili che al trattamento di dati giudiziari*⁵².

I soggetti pubblici devono conformare il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

sul trattamento di dati sensibili da parte dei soggetti pubblici, GU 206 del 9 maggio 1998 (oggi abrogato).

⁵⁰ Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'art. 22 del Codice, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'art. 154, comma 1, lett. g), anche su schemi tipo (art. 20, comma 2).

Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'art. 26, comma 2, il trattamento dei dati sensibili (art. 20, comma 3).

Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2 sopra esaminato.

L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 dell'art. 20 sopra illustrati è aggiornata e integrata periodicamente.

⁵¹ Cfr. art. 8, par. 5, direttiva 95/46/CE; art. 24 L. 675/1996; art. 5 D.L.vo 135/1999.

⁵² Cfr. D.L.vo 135/1999; art. 23, comma 4, L. 675/1996.

Nel fornire l'informativa di cui all'art. 13 del Codice, esaminata nel paragrafo precedente, i soggetti pubblici devono fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

I soggetti pubblici possono trattare solo i dati sensibili e giudiziari *indispensabili per svolgere attività istituzionali* che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

In applicazione dell'art. 11, comma 1, lett. c), d) ed e), sopra illustrato, i soggetti pubblici sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa⁵³.

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, *devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.*

⁵³ Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui sopra anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

I dati idonei a rivelare lo stato di salute *non possono essere diffusi.*

Rispetto ai dati sensibili e giudiziari indispensabili ai sensi delle norme illustrate, i soggetti pubblici sono autorizzati ad effettuare unicamente le *operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito*, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'art. 14⁵⁴, sono effettuati solo previa annotazione scritta dei motivi.

In ogni caso, le operazioni e i trattamenti di cui sopra, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge⁵⁵.

[Sommar](#)io

⁵⁴ Sull'art. 14 v. nota n. 23.

⁵⁵ Le disposizioni di cui all'art. 22 in esame recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

7. *Segue*: il consenso dell'interessato

Il capo III (artt. 23-27) del titolo III della parte I del Codice, come già accennato, reca *regole ulteriori per i privati ed enti pubblici economici*⁵⁶.

L'art. 23 conferma innanzitutto il principio secondo cui, normalmente, il trattamento di dati personali da parte di privati od enti pubblici economici non può che avvenire in base al *consenso espresso dell'interessato*⁵⁷.

In ambito Internet, ciò comporta in primo luogo il problema di stabilire se la manifestazione del consenso attraverso la compilazione di un *form on-line*, con pressione del tasto "accetto" o simile (meccanismo del c.d. *point and click*), possa essere considerata quale comportamento *espresso* del soggetto o, al contrario, debba essere considerata un semplice *comportamento concludente*.

A questo proposito, come visto nel capitolo I, la direttiva 2002/58/CE (considerando n. 17) precisa che 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".

⁵⁶ "Il capo III contiene, in maniera pressoché speculare a quello che precede (riguardante i soggetti pubblici), la disciplina specifica del trattamento effettuato da soggetti privati, riguardante sia i dati 'comuni', sia i dati sensibili o giudiziari. Per quanto riguarda i dati comuni, l'art. 23 (già 11 della legge n. 675/1996) chiarisce meglio, anche in accoglimento di quanto espressamente richiesto in sede di parere dalla Commissione giustizia del Senato, che il consenso al trattamento dei dati personali deve essere '*espresso liberamente e specificamente in riferimento al trattamento chiaramente individuato,*' e non solo reso 'in forma specifica', in linea con quanto richiesto dalla direttiva europea (art. 2, par. 1, lett. h, dir. n. 95/46/CE)" (così la relazione di accompagnamento).

⁵⁷ Cfr. art. 7, par. 1, lett. a) direttiva 95/46/CE; artt. 11, 20 e 22 L. 675/1996.

Pare dunque ragionevole ritenere, allo stato attuale, la comunicazione “via bit” un *segno di linguaggio*, come tale idonea a configurare una *dichiarazione espressa* di volontà⁵⁸. Altrettanto può dirsi per un consenso manifestato nel testo di una e-mail, che dovrà considerarsi “espresso” ai fini della normativa sulla privacy.

Come già previsto dalla previgente disciplina, il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il consenso è validamente prestato solo se è *espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato*, se è *documentato per iscritto*, e se sono state rese all'interessato le *informazioni di cui all'art. 13*, sopra illustrato (art. 23, comma 3). Il consenso deve essere manifestato *in forma scritta* quando il trattamento riguarda *dati sensibili* (art. 23, comma 4).

L'art. 24 del provvedimento in esame si occupa d'altra parte dei *casi nei quali il trattamento di dati comuni può essere effettuato a prescindere dal consenso dell'interessato*, riprendendo in buona parte quanto già disposto dalla L.

⁵⁸ In questo senso, A. Lisi, *Tutela della privacy in Internet* cit., pp. 47 e ss.

Sull'ulteriore questione se il consenso manifestato on-line possa o meno considerarsi “documentato per iscritto” come richiesto in relazione ai dati comuni, come subito si vedrà, dall'art. 23 o “in forma scritta” come richiesto dall'art. 26 per i dati sensibili, v. *ibidem* nonché Filippi, *Il trattamento dei dati personali*, in *Il diritto della nuova economia*, a cura di F. Maschio, Padova, 2002, pp. 345 s.

Il Tribunale di Cuneo, con provvedimento del 15/12/2003, ha accolto un *ricorso per decreto ingiuntivo* fondato sull'asserita rilevanza di una *e-mail quale documento informatico sottoscritto con firma elettronica “leggera”*. Sul punto si vedano A. Lisi, *L'e-mail dal commercio elettronico alle aule di giustizia*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6882; M. Cammarata e E. Maccarone, *Un messaggio e-mail non è “prova scritta”*, in *InterLex*, www.interlex.it, www.interlex.it/docdigit/provascritta.htm; A. Lisi, *L'e-mail è “forma scritta”?*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=250; F. Sarzana di S. Ippolito, *Profili giuridici delle firme elettroniche*, in *Punto Informatico*, <http://punto-informatico.it/p.asp?i=46847>; S. Camerini, *Provider ed e-mail probatorie*, in *Studium Fori*, www.studiumfori.it, www.studiumfori.it/visallex.php?id=1491; L.M. De Grazia, *Firma Elettronica Non Avanzata. Una personale opinione sulla c.d. “firma elettronica debole”*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/firma_elettronica.pdf.

675/1996, con alcune novità di rilievo⁵⁹.

⁵⁹ Cfr. art. 7 direttiva 95/46/CE; artt. 12 e 20 L. 675/1996; art. 7 D.L.vo 281/1999.

“Nell’art. 24 sono state riunite, in ragione della sostanziale omogeneità della disciplina, le disposizioni che autorizzano il trattamento di dati personali anche in assenza del consenso, unificando, in sostanza, i previgenti articoli 12 e 20 della legge n. 675/1996. L’art. 24 fa salve le specificità riconosciute, in alcuni casi, per la comunicazione e, soprattutto, per la diffusione dei dati (lett. c), f) e g)). La disciplina risulta ora più chiara, essendo state eliminate alcune duplicazioni ed apportate talune opportune precisazioni.

In particolare, fra l’altro:

a) in relazione alle lettere a) e b), è stato meglio specificato, in conformità a quanto previsto dalla direttiva europea (art. 7, par. 1, lett. c), dir. 95/46/CE), il presupposto di liceità del trattamento relativo alla sussistenza di un obbligo legale, riferita ora correttamente alla necessità di adempiere comunque ad un obbligo previsto dalla legge, e non più solo al caso di ‘dati raccolti e detenuti’ in base al medesimo obbligo. Inoltre, in sintonia con il diritto vivente, si è chiarito che il trattamento è consentito quando è comunque necessario per adempiere, prima della conclusione del contratto, a specifiche richieste dell’interessato e non solo per eseguire ‘misure’ precontrattuali su richiesta del medesimo interessato. Quest’ultimo intervento, ripetuto in maniera speculare nell’articolo 43 (già 28 della legge n. 675/1996), in relazione al trasferimento di dati all’estero, completa l’allineamento alla direttiva europea delle disposizioni concernenti trattamenti effettuati in relazione a rapporti precontrattuali, già avviato con il decreto legislativo n. 467/2001 (art. 7, par. 1, lett. b), dir. 95/46/CE);

b) alla lettera e), si è chiarito che il presupposto di liceità del trattamento riferito all’esigenza di salvaguardare la vita o l’incolumità di un terzo è comunque applicabile anche fuori dei precedenti casi in cui veniva specificato che l’interessato non può, per incapacità o altri motivi, prestare il proprio consenso. Inoltre, in relazione al caso in cui la medesima finalità riguardi la vita o l’incolumità dell’interessato, la disciplina è stata allineata a quella vigente in ambito sanitario in relazione al trattamento di dati idonei a rivelare lo stato di salute per finalità di cura della persona, che in base alle disposizioni previgenti risultava più rigorosa rispetto a quella del trattamento di dati comuni o sensibili effettuato da soggetti diversi da quelli sanitari. La disciplina prevede, ora, che anche in questi ultimi casi, se manca il consenso della persona incapace o altrimenti impossibilitata a prestarlo è necessario acquisire il consenso dei prossimi congiunti o familiari, e si può procedere al trattamento dei dati personali dell’interessato solo se sia impossibile acquisire anche il consenso di tali soggetti o vi è rischio grave ed imminente per la salute della persona, purché il consenso sia acquisito successivamente (art. 82, comma 2);

c) è stato soppresso l’ormai inutile riferimento specifico alla comunicazione effettuata nell’ambito di gruppi bancari o fra società controllate o collegate, in quanto la disposizione era legata al generalizzato sistema delle notificazioni di trattamenti correlati che il codice ha sostanzialmente eliminato (cfr. art. 37 – *Notificazione del trattamento*). La medesima esigenza, peraltro, può essere comunque efficacemente soddisfatta in applicazione dell’istituto del bilanciamento degli interessi del titolare con i diritti dell’interessato (art. 24, comma 1, lett. g);

d) si è esteso l’esonero dall’obbligo di acquisire il consenso ai trattamenti in ambito ‘interno’ effettuati da organismi ‘no-profit’ anche in relazione a dati comuni, in conformità a quanto già previsto per i dati sensibili, a condizione che le modalità di utilizzo dei dati siano esplicitate in un’apposita determinazione resa nota agli associati con l’informativa (analoga condizione è stata inserita per i trattamenti di dati sensibili all’art. 26, comma 4, lett. a));

Il consenso non è dunque richiesto, oltre che nei casi specificamente previsti nella parte II del Codice, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato⁶⁰;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, *fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati*⁶¹;

e) la lettera i) reca un miglior coordinamento con la disciplina in materia di trattamenti per scopi storici, statistici o scientifici” (così la relazione di accompagnamento).

⁶⁰ L'art. 12, lett. b), L. 675/1996, così come modificato dal D.L.vo 467/2001, faceva riferimento all'“esecuzione di misure precontrattuali” adottate su richiesta dell'interessato.

In proposito, con riguardo al Web, si veda A. Lisi e M. De Giorgi, *Cambiano le leggi ma rimane illegittimo il trattamento dei dati personali nel web*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6816.

⁶¹ L'ultima parte, evidenziata in corsivo, è stata aggiunta dal Codice rispetto alla formulazione di cui alla previgente legge sulla privacy.

L'esclusione in parola aveva suscitato infatti diverse questioni applicative, con riferimento soprattutto ai dati (indirizzo e-mail, fax...) rinvenuti su siti web o newsgroup e utilizzati per l'invio di messaggi promozionali non richiesti.

Con diversi provvedimenti, il Garante aveva comunque stabilito il principio, più volte riaffermato, secondo cui la previsione della lettera c) dell'art. 12 L. 675/1996 non doveva intendersi come riferita a qualunque dato personale di fatto consultabile da una pluralità di persone, bensì ai soli dati personali che, oltre ad essere desunti da registri, elenchi, atti o documenti “pubblici”, fossero sottoposti anche ad un regime giuridico di piena conoscibilità, da parte di chiunque.

Si veda in proposito quanto si dirà nel capitolo III in materia di spamming.

d) riguarda *dati relativi allo svolgimento di attività economiche*, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale⁶²;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo⁶³;

f) *con esclusione della diffusione*, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, *nel rispetto della vigente normativa in materia di segreto aziendale e industriale*;

g) *con esclusione della diffusione*, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, *anche in riferimento all'attività di gruppi bancari e di società controllate o collegate*, qualora non prevalgano i

⁶² La corrispondente disposizione dell'abrogata L. 675/1996 (art. 12, comma 1, lett. f)) faceva espresso riferimento anche ai dati relativi allo svolgimento di attività economiche raccolti ai fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva.

Con provvedimento del 25/06/2002 (www.iusreporter.it/Testi/osservaspamming.htm) il Garante per la protezione dei dati personali ha avuto modo di affermare che l'espressione "dati relativi allo svolgimento di attività economiche" (cfr. provvedimento del 16/02/1999, in *Bollettino*, n. 7) *non ricomprende le informazioni ed i dati di carattere puramente personale come un indirizzo di posta elettronica ad uso privato*.

Nel vigore della precedente disciplina, considerato il tenore letterale della norma, allorché si rientrasse nel campo di applicazione della L. 675/1996, pare in ogni caso che potesse essere utilmente invocata l'ipotesi di esclusione del consenso in parola al fine di andare esenti da responsabilità per trattamento illecito di dati personali nel caso di invio di *e-mail pubblicitarie non richieste* (sullo *spamming* si veda, più approfonditamente, quanto si dirà nel capitolo III nonché, con riguardo alle sanzioni, nel capitolo V).

⁶³ Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica in questo caso la disposizione di cui all'art. 82, comma 2, del Codice.

diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) *con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'art. 13⁶⁴;*

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A) del Codice, per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'art. 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

[Sommar](#)

8. Segue: comunicazione e diffusione dei dati

La comunicazione e la diffusione dei dati trattati sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria (art. 25)⁶⁵ e salvi particolari divieti previsti dalla legge:

⁶⁴ Una simile ipotesi di esclusione del consenso era prima espressamente prevista dall'art. 22 L. 675/1996 con riferimento ai soli dati sensibili.

⁶⁵ Cfr. art. 21 L. 675/1996.

L'art. 20 L. 675/1996, contrariamente a quanto oggi accade, elencava i casi in cui la comunicazione e la diffusione dei dati erano *ammesse*. Sulle definizioni di comunicazione e diffusione accolte dal Codice, v. par. 2.

a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'art. 11, comma 1, lett. e), vale a dire “un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati”;

b) per finalità diverse da quelle indicate nella notificazione⁶⁶ del trattamento, ove prescritta.

E' fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2 del Codice, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Sommario

9. Segue: dati sensibili e semisensibili

L'art. 26, comma 1, del Codice della privacy, confermando sostanzialmente la disciplina previgente, dispone che i *dati sensibili* possono essere oggetto di trattamento solo con il *consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti*⁶⁷.

⁶⁶ Sulla notificazione si veda il par. 12.

⁶⁷ Cfr. art. 8 direttiva 95/46/CE; artt. 22 e 23 L. 675/1996.

“Per quanto riguarda il trattamento dei dati sensibili, si segnalano alcuni interventi di razionalizzazione del sistema e per il pieno adeguamento della normativa alla direttiva 95/46/CE (art. 26).

Anzitutto, conformemente a quanto previsto per i soggetti pubblici, si è nuovamente ricordato che anche i soggetti privati nel trattare dati sensibili devono altresì rispettare i presupposti ed i limiti stabiliti dal codice, da disposizioni di legge o di regolamento.

Un importante intervento di razionalizzazione della disciplina, riguarda il trattamento di dati sensibili effettuati da confessioni religiose.

L'art. 8, par. 2, lett. d), della dir. 95/46/CE prevede che i trattamenti effettuati da associazioni o altri organismi senza scopo di lucro operanti in ambito religioso, filosofico, politico o sindacale sono consentiti anche senza il consenso degli interessati, se effettuati in base a '*garanzie adeguate*' e purché siano utilizzati - all'interno' degli organismi - i soli dati degli aderenti o delle persone che hanno contatti abituali con gli organismi stessi nell'ambito delle loro finalità lecite. Il particolare regime si giustifica in ragione del fine perseguito dagli organismi (in ogni caso non di lucro) e del 'limite' rappresentato dalla circolazione dei dati solo all'interno degli organismi.

Per quanto riguarda l'ambito religioso, il decreto legislativo n. 135/1999, in materia di trattamento di dati sensibili da parte di soggetti pubblici, ha dato una prima attuazione a tale disciplina in riferimento alle confessioni religiose i cui rapporti con lo Stato sono regolati da accordi o intese (art. 22, comma 1-bis, l. n. 675/1996, introdotto dal d. lg. n. 135/1999), 'autorizzando' le stesse a trattare i dati in questione anche senza il consenso degli interessati e senza l'obbligo di rispettare l'autorizzazione del Garante, nel rispetto, tuttavia, di idonee garanzie da adottare in relazione ai trattamenti effettuati. Successivamente il decreto legislativo n. 467/2001 ha integrato il medesimo articolo 22 della legge n. 675/1996 prevedendo che tutti gli organismi senza scopo di lucro, anche a carattere religioso, possono trattare i dati sensibili senza il consenso dell'interessato, ma nel rispetto dell'autorizzazione del Garante. L'art. 26, comma 3, lett. a) del codice completa, ora, l'intervento normativo, armonizzando meglio la disciplina normativa delle confessioni religiose, anche in riferimento alla giurisprudenza costituzionale e alle garanzie di cui le medesime confessioni si dotano nel rispetto dei principi contenuti in un'autorizzazione del Garante. Un'apposita disposizione transitoria (art. 181, comma 6) consente, in ogni caso, alle confessioni religiose che, prima dell'entrata in vigore del codice, abbiano già determinato e adottato le garanzie richieste nell'ambito del rispettivo ordinamento, di proseguire le attività di trattamento nel rispetto delle medesime.

Per quanto riguarda i casi in cui il trattamento è consentito anche senza il consenso dell'interessato, previa autorizzazione del Garante, si evidenzia:

a) la disciplina dei trattamenti effettuati da organismi senza scopo di lucro – analogamente a quanto sopra descritto in relazione al trattamento di dati comuni – è stata adeguata ad un criterio di maggiore garanzia e trasparenza prevedendo che tali organismi individuino con espressa determinazione le modalità di utilizzo dei dati, rendendola nota agli interessati all'atto dell'informativa (art. 26, comma 4, lett. a));

b) è stato apportato un intervento analogo a quello già descritto per il trattamento di dati comuni necessario per salvaguardare la vita o l'incolumità di un terzo o dell'interessato (art. 26, comma 4, lett. b));

c) in relazione al diritto di 'rango pari' a quello dell'interessato – presupposto di liceità del trattamento di dati idonei a rivelare lo stato di salute per finalità di esercizio di un diritto – è stato precisato, in conformità alla giurisprudenza e al diritto vivente, che tale diritto è relativo ad un diritto della personalità o ad un altro diritto o libertà fondamentale e inviolabile; tale precisazione normativa ricorre, ovviamente, in ogni altro caso in cui nel codice si fa riferimento ad un diritto di rango pari (artt. 60, 71 e 92) (art. 26, comma 4, lett. c));d) in attuazione di una specifica

Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro *quarantacinque giorni*, decorsi i quali *la mancata pronuncia equivale a rigetto*.

Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere *misure e accorgimenti a garanzia dell'interessato*, che il titolare del trattamento è tenuto ad adottare.

L'art. 26, comma 1, del Codice, appena illustrato, non si applica al trattamento:

a) dei *dati relativi agli aderenti alle confessioni religiose*⁶⁸ e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. D'altra parte il Codice prevede che le confessioni religiose determinino *idonee garanzie* relativamente ai trattamenti effettuati, *nel rispetto dei principi indicati al riguardo con autorizzazione del Garante*;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

La disposizione in esame elenca altresì un'altra serie di ipotesi in cui i dati sensibili possono essere oggetto di trattamento *anche senza consenso*, ma *previa*

disposizione della direttiva europea (art. 8, par. 2, lett. b), dir. 95/46/CE), è stato introdotto un ulteriore presupposto di liceità del trattamento in relazione a ciò che è necessario per adempiere a specifici obblighi previsti dalla normativa, anche comunitaria, in materia di gestione del rapporto di lavoro, nei limiti previsti dall'autorizzazione del Garante e ferme restando le disposizioni del codice di deontologia e di buona condotta (art. 26, comma 4, lett. d)" (così la relazione di accompagnamento).

Sulle *autorizzazioni*, v. par. 12.

⁶⁸ Il previgente art. 22 L. 675/1996 si riferiva invece alle sole "confessioni religiose i cui rapporti con lo Stato siano regolati da accordi o intese ai sensi degli articoli 7 e 8 della Costituzione".

autorizzazione del Garante; ciò precisamente accade:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, *per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo*, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini *idonee garanzie* relativamente ai trattamenti effettuati, *prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'art. 13 del Codice*;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. *Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'art. 82, comma 2⁶⁹*;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o

⁶⁹ La norma contenuta nel Codice, innovando rispetto al passato, prevede dunque che in caso di impossibilità o di incapacità riguardante l'interessato la necessità di ricevere il consenso per il trattamento dei dati permane; consenso che dovrà essere acquisito da uno dei soggetti espressamente indicati, salva comunque l'applicabilità dell'art. 82, comma 2, con riguardo ai dati riguardanti lo stato di salute.

Come sopra visto, anche in relazione ai dati comuni è oggi prevista un'analoga ipotesi di esclusione del consenso (v. par. 7).

difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento⁷⁰;

d) *quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice*⁷¹.

L'ultimo comma dell'art. 26 prevede infine un generale *divieto di diffusione per i dati idonei a rivelare lo stato di salute*.

Con riguardo alla categoria dei *dati semisensibili*, introdotta nell'ordinamento dal D.L.vo 461/2001, l'art. 17⁷² del Codice ("Trattamento che presenta rischi specifici") dispone inoltre che "il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti".

Le misure e gli accorgimenti di cui sopra sono prescritti dal Garante in applicazione dei principi sanciti dal Codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate

⁷⁰ Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, *ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile*.

⁷¹ Tale ultima categoria di ipotesi, relativa alla gestione del rapporto di lavoro, non era contemplata dalla previgente disciplina.

⁷² Cfr. art. 20 direttiva 95/46/CE; art. 24bis L. 675/1996.

categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare⁷³.

Sommario

10. Soggetti che effettuano il trattamento

Il titolo IV (artt. 28-30) della parte I del Codice della privacy detta alcune norme per i *soggetti che effettuano il trattamento*: titolare, responsabile e incaricato del trattamento, così come previamente definiti dall'art. 4 del provvedimento⁷⁴.

Viene innanzitutto specificato che, quando il trattamento è effettuato da una *persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo*, titolare del trattamento è *l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza* (art. 28).

Ai sensi dell'art. 29, il *responsabile del trattamento*⁷⁵, la cui nomina da parte del titolare rimane facoltativa, se designato, deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

⁷³ Per quanto concerne le *garanzie per i dati giudiziari*, l'art. 27 del testo unico prevede che "Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili".

⁷⁴ V. par. 2.

⁷⁵ Cfr. art. 16 direttiva 95/46/CE; art. 8 L. 675/1996.

Viene espressamente previsto che i compiti affidati al responsabile siano *analiticamente specificati per iscritto dal titolare*.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui sopra e delle proprie istruzioni.

L'art. 30 stabilisce infine che le operazioni di trattamento possono essere effettuate solo da *incaricati*⁷⁶ che operino sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

La designazione degli incaricati deve essere effettuata per iscritto e individuare puntualmente l'ambito del trattamento consentito. Viene specificato che si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

[Sommaro](#)

11. Sicurezza dei dati e dei sistemi

Il titolo V della parte I del Codice della privacy ("Sicurezza dei dati e dei sistemi", artt. 31-36) detta le disposizioni relative alle *misure di sicurezza* volte a proteggere i dati personali oggetto di trattamento⁷⁷.

⁷⁶ Cfr. art. 17, par. 3, direttiva 95/46/CE; artt. 8 e 19 L. 675/1996.

⁷⁷ 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; T. Minella, *La Privacy. Guida all'applicazione della legge 675/1996*, Napoli, Ed. Simone, 2001, pp. 369 ss.; S. Sutti, *La*

L'art. 31, nel riprodurre la previgente normativa, pone innanzitutto fondamentali *obblighi di sicurezza* in capo al soggetto che effettua il trattamento di dati personali⁷⁸.

Secondo la disposizione infatti, i dati personali oggetto di trattamento sono 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.

sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., pp. 837 ss.; F. Tommasi, *La sicurezza dei sistemi informativi ed il documento programmatico sulla sicurezza* cit., pp. 853 ss.; D. De Gaetano, *Il documento programmatico sulla sicurezza*, in *La privacy in Internet* cit., pp. 115 ss.; con particolare riferimento alla professione forense, E. Ancona e M. Bonanno, *Sicurezza e professione forense. Aspetti deontologici e norme tecniche nell'uso della rete*, in *La privacy in Internet* cit., pp. 135 ss.

Con riguardo all'*entrata in vigore* delle disposizioni del Codice concernenti le misure di sicurezza, l'art. 180 stabilisce quanto segue.

“1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 30 giugno 2004.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro un anno dall'entrata in vigore del codice”.

In ordine alle *sanzioni* riconnesse alla violazione delle norme sulla sicurezza che ci si appresta ad analizzare si rimanda sin d'ora al cap. V.

⁷⁸ Cfr. art. 17 direttiva 95/46/CE; art. 15, comma 1, L. 675/1996.

L'art. 32 del Codice detta poi alcune disposizioni specifiche per "particolari titolari". Il riferimento va oggi, in attuazione della direttiva 2002/58/CE, ai *fornitori di un servizio di comunicazione elettronica accessibile al pubblico*⁷⁹.

Con riguardo alle *misure minime di sicurezza* che devono essere adottate, l'art. 33⁸⁰ del Codice prevede innanzitutto che, *nel quadro dei più generali obblighi di*

⁷⁹ Dette disposizioni saranno analizzate nel cap. III unitamente alle altre norme di attuazione della direttiva 2002/58/CE.

⁸⁰ Cfr. art. 15, comma 2, L. 675/1996.

"Il capo II individua le note misure 'minime' di sicurezza demandando la determinazione delle modalità di applicazione alle disposizioni contenute nel Disciplinare tecnico allegato al codice (allegato B).

Rispetto alle disposizioni contenute nel d.P.R. 28 luglio 1999, n. 318, emanato in attuazione dell'art. 15 della legge n. 675/1996, il sistema delle misure minime di sicurezza viene semplificato e aggiornato sulla base dell'esperienza applicativa degli ultimi tre anni e dell'evoluzione tecnologica.

Si segnalano, in particolare, alcuni aspetti caratterizzanti il nuovo sistema.

Ai fini dell'applicazione delle misure minime richieste, si conferma la distinzione fra trattamenti effettuati con strumenti elettronici e trattamenti 'cartacei', mentre, per quanto riguarda i primi, si evidenzia la diversa configurazione della distinzione, presente a determinati effetti nel d.P.R. 318/1999, tra trattamenti effettuati con elaboratori non accessibili da altri elaboratori o terminali e trattamenti con elaboratori 'accessibili' in rete, e, tra questi ultimi, dell'ulteriore distinzione tra l'accessibilità attraverso reti disponibili o non disponibili al pubblico.

Non ha più una sua espressa rilevanza formale la figura dell'*amministratore di sistema*, mentre viene confermato l'obbligo di provvedere alla custodia di copie delle parole chiave per l'autenticazione, qualora sia tecnicamente indispensabile per garantire l'accesso ai dati in caso di impedimento di un incaricato.

Per il trattamento con strumenti elettronici si prevede l'obbligo di adottare l'autenticazione informatica dell'utente, anche mediante l'utilizzo di eventuali sistemi biometrici, e adeguate procedure di gestione delle relative credenziali di autenticazione.

Il titolare deve curare l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, la tenuta di un aggiornato documento programmatico sulla sicurezza e l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Per i casi residuali in cui la limitatezza tecnologica degli strumenti in uso o la loro obsolescenza non consentano di attuare completamente il dettato normativo, si prevede l'obbligo da parte del

sicurezza di cui all'art. 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate dalle disposizioni che si vanno ad illustrare (artt. 34-36) o ai sensi dell'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Il rispetto delle prescrizioni sulle misure minime di sicurezza, come si vedrà meglio nel prosieguo, eviterà al titolare del trattamento di incorrere nel *reato* di cui all'art. 169 del Codice.

Deve rilevarsi d'altra parte che, per evitare anche una eventuale responsabilità risarcitoria sul piano civile, il titolare non dovrà limitarsi all'osservanza delle norme relative alle misure minime, ma dovrà altresì dimostrare di avere adottato tutte le "idonee e preventive misure di sicurezza" di cui all'art. 31 del testo unico, sopra illustrato, tali da *ridurre al minimo* i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta⁸¹.

titolare di descrivere in un documento a data certa, da custodire presso la propria struttura, gli impedimenti tecnici che hanno reso impossibile o parziale l'immediata applicazione delle misure minime di sicurezza. Viene inoltre introdotto, in relazione alla possibile inadeguatezza di alcuni elaboratori a consentire l'applicazione delle misure minime, un termine di un anno per dare tempo ai titolari di adeguare la propria dotazione tecnologica in modo da consentire l'applicazione delle misure minime di sicurezza (art. 180).

Per quanto riguarda le modalità di applicazione delle misure minime di sicurezza da adottare, sono state apportati gli adeguamenti richiesti dalla Commissione giustizia della Camera.

In particolare, nel Disciplinare tecnico che reca tali modalità, sono state stabilite due scadenze periodiche (semestrale e annuale) per gli adempimenti a carico del titolare del trattamento e uniformate le scadenze rispondenti a finalità omogenee (punti 14 e 15 del Disciplinare). E' stato infine determinato il termine di aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito agli incaricati (punto 27 del Disciplinare)" (così la relazione di accompagnamento al Codice).

Sulla disciplina delle misure minime di sicurezza introdotta dal Codice della privacy, si veda C. Giustozzi, *Dati al sicuro, non ci sono più scuse*, in *InterLex*, www.interlex.it, www.interlex.it/675/corrado10.htm; A. Gelpi, *Misure minime, qualche passo avanti*, in *InterLex*, www.interlex.it, www.interlex.it/675/gelpi7.htm.

⁸¹ Sul risarcimento del danno v. par. 5; si veda anche M.P. Berlingieri, *La responsabilità civile derivante dal trattamento dei dati personali: natura giuridica, conseguenze, oneri probatori* cit.,

La nuova disciplina va a sostituire pertanto quella di cui al precedente art. 15, comma 2, L. 675/1995 e relativa normativa di attuazione, contenuta nell'altrettanto noto e discusso DPR 318/1999.

La nuova normativa, analogamente alla precedente, distingue tra *trattamenti effettuati con strumenti elettronici* e *trattamenti effettuati senza l'ausilio di strumenti elettronici*.

11.1. Misure minime per i trattamenti effettuati con strumenti elettronici

Con riferimento ai *trattamenti effettuati con strumenti elettronici*, occorre rilevare innanzitutto che scompare nel Codice della privacy la non felice distinzione tra elaboratori non accessibili da altri elaboratori o terminali ed elaboratori accessibili in rete⁸².

L'art. 34 prevede che *il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B)*⁸³ del Codice, *le seguenti misure minime*⁸⁴:

secondo cui "La sicurezza, pertanto, non potrà mai avere i caratteri dell'assolutezza e della staticità: in quanto processo essenzialmente dinamico (perché così è stato concepito dal legislatore, che lo ha ancorato al criterio estremamente variabile del progresso tecnico), la sicurezza impone una continua ponderazione degli interessi in gioco, tra il costo dell'adozione di tutte le misure ed il costo potenziale derivante da una sicurezza inadeguata.

La prova positiva da fornire è necessariamente una prova critica, di carattere organizzativo, sull'esistenza delle misure più opportune in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento. Tale valutazione andrà fatta con riferimento al momento in cui il danno si è verificato: non è ammissibile, infatti, che un titolare del trattamento possa liberarsi dalla responsabilità civile di cui si tratta dimostrando che le misure disposte avevano il carattere della 'idoneità' al momento della loro adozione".

⁸² Questi ultimi a loro volta distinti, dal previgente DPR 318/1999, in elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico e elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico (cfr. artt. 2 e 3 DPR 318/1999).

⁸³ Ai sensi dell'art. 36, il disciplinare tecnico di cui all'allegato B) del Codice, relativo alle misure minime, deve essere aggiornato periodicamente con decreto del Ministro della giustizia di concerto

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione⁸⁵;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Le *modalità tecniche* relative alle misure minime di sicurezza nel caso di trattamento con strumenti elettronici, da adottarsi a cura del titolare, del

con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

⁸⁴ Per le relative *definizioni*, si rimanda a quanto già illustrato, con riferimento all'art. 4 del Codice, nel par. 2 del presente capitolo.

⁸⁵ Sulla distinzione tra sistemi di *autenticazione* e sistemi di *autorizzazione* informatica si veda C. Giustozzi, *Dati al sicuro, non ci sono più scuse* cit.

responsabile ove designato e dell'incaricato⁸⁶, vengono dunque poi specificate come segue nell'allegato B) del Codice della privacy.

Sistema di autenticazione informatica.

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di *credenziali di autenticazione* che consentano il superamento di una *procedura di autenticazione* relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono:

- in un *codice per l'identificazione* dell'incaricato associato a una *parola chiave riservata* conosciuta solamente dal medesimo oppure
- in un *dispositivo di autenticazione* in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure
- in una *caratteristica biometrica* dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave⁸⁷.

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la *segretezza* della componente riservata della credenziale e la *diligente custodia* dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La *parola chiave*, quando è prevista dal sistema di autenticazione, è composta da *almeno otto caratteri* oppure, nel caso in cui lo strumento elettronico non lo

⁸⁶ Su tali soggetti v. par. 10.

⁸⁷ Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

permetta, da un numero di caratteri pari al massimo consentito; *essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi*. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Il *codice per l'identificazione*, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono *disattivate*, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Sono *impartite istruzioni* agli incaricati per non lasciare *incustodito e accessibile lo strumento elettronico durante una sessione di trattamento*⁸⁸.

Le disposizioni sul sistema di autenticazione di cui sopra e quelle sul sistema di autorizzazione di cui appresso *non si applicano ai trattamenti dei dati personali destinati alla diffusione*⁸⁹.

Sistema di autorizzazione.

⁸⁸ Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

⁸⁹ Come definita dall'art. 4 del Codice, v. par. 2.

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso deve essere utilizzato un *sistema di autorizzazione*.

I *profili di autorizzazione*, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, *in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento*.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza.

Nell'ambito dell'*aggiornamento periodico con cadenza almeno annuale* dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Con riguardo alla protezione dai *virus informatici*, si prevede che i dati personali debbano essere *protetti contro il rischio di intrusione e dell'azione di tali programmi, di cui all'art. 615quinquies del codice penale*⁹⁰, mediante l'attivazione di *idonei strumenti elettronici* (anti-virus) da aggiornare con cadenza *almeno semestrale*.

⁹⁰ L'art. 615quinquies del codice penale ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico") prevede quanto segue.

"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a Euro 10.329".

Si prevede inoltre che gli *aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti* (c.d. *patch*) debbano essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale⁹¹.

Infine, con riguardo al *back-up* dei dati, si prevede che siano impartite istruzioni organizzative e tecniche che contemplino il *salvataggio dei dati con frequenza almeno settimanale*.

Documento programmatico sulla sicurezza.

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari è tenuto a redigere anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- 1) l'elenco dei trattamenti di dati personali;
- 2) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- 3) l'analisi dei rischi che incombono sui dati;
- 4) le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e

⁹¹ “Credo sia evidente a tutti che avere l'antivirus aggiornato ogni 6 mesi è assolutamente inutile [...] Sul problema degli antivirus il testo si è completamente dimenticato di quei sistemi (Linux ad esempio o i mainframe IBM) dove il problema dei virus non esiste [...] Identico problema si trova nell'articolo successivo dove si precisa che l'installazione di correttivi ai programmi (le famose *patch*) deve essere fatta almeno una volta l'anno, salvo il caso di trattamenti di dati sensibili o giudiziari, nel qual caso il limite è di soli, si fa per dire, sei mesi” (A. Gelpi, *Misure minime, qualche passo avanti* cit.).

accessibilità;

5) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

6) la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare⁹²;

7) la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;

8) per i dati personali idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari e gli esercenti le professioni sanitarie, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Il documento programmatico sulla sicurezza è dunque un resoconto delle misure di sicurezza adottate dal titolare del trattamento di dati personali al fine di ridurre al minimo il verificarsi di qualsiasi tipo di evento dannoso o pericoloso a carico degli stessi dati personali⁹³.

⁹² La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

⁹³ A. Lisi, *Documento Programmatico per la Sicurezza: rompicapo o risorsa aziendale? Sono questi i nuovi rebus che le imprese dovranno risolvere con l'entrata in vigore a gennaio del nuovo Codice per la privacy!*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6869.

La nuova normativa (artt. 33 e ss. del Codice e relativo all. B) pone problemi interpretativi con riguardo ai *soggetti* tenuti alla redazione del documento programmatico sulla sicurezza.

Mentre infatti l'art. 34 del Codice prevede la tenuta di un aggiornato documento programmatico per i *trattamenti effettuati con strumenti elettronici* – senza distinguere tra dati comuni e dati sensibili – l'all. B ora in esame prevede l'adozione del documento soltanto per coloro che effettuano trattamenti di *dati sensibili o giudiziari*⁹⁴.

A parere di chi scrive, la lettura congiunta dell'art. 34 del Codice e dell'all. B) consente di affermare che, in base alla normativa in vigore dal primo gennaio 2004, tenuti alla redazione del documento programmatico sulla sicurezza siano i *titolari di trattamenti di dati sensibili o giudiziari effettuati con l'ausilio di strumenti elettronici*.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari.

I dati sensibili o giudiziari devono essere protetti contro l'*accesso abusivo*, di cui all' art. 615^{ter} del codice penale, mediante l'utilizzo di idonei strumenti elettronici⁹⁵.

Sono inoltre impartite *istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili* su cui sono memorizzati i dati, al fine di evitare accessi non autorizzati e trattamenti non consentiti.

⁹⁴ Sul punto, v. A. Lisi, *Documento Programmatico per la Sicurezza: rompicapo o risorsa aziendale?* cit.

⁹⁵ L'art. 615^{ter} del codice penale punisce l'*accesso abusivo ad un sistema informatico o telematico* prevedendo al primo comma che “chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni”.

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Sono infine adottate idonee misure per garantire il *ripristino dell'accesso ai dati* in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni⁹⁶.

Misure di tutela e garanzia.

Il titolare che adotta misure minime di sicurezza avvalendosi di *soggetti esterni alla propria struttura*, per provvedere alla esecuzione deve ricevere dall'installatore una *descrizione scritta dell'intervento effettuato*, che ne attesti la conformità alle disposizioni del disciplinare tecnico in esame.

Il titolare deve riferire, nella *relazione accompagnatoria del bilancio d'esercizio*, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

11.2. Misure minime per i trattamenti effettuati senza l'ausilio di strumenti elettronici

⁹⁶ Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei *dati idonei a rivelare lo stato di salute e la vita sessuale* contenuti in elenchi, registri o banche di dati con le modalità di cui all'art. 22, comma 6, del Codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

I *dati relativi all'identità genetica* sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Per quanto riguarda i *trattamenti effettuati senza l'ausilio di strumenti elettronici*, l'art. 35 del Codice prescrive che detta tipologia di trattamento è *consentita solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime*:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Ancora una volta dunque, le specifiche modalità di adozione delle misure minime, a cura del titolare, del responsabile, ove designato, e dell'incaricato, vengono poi dettate dall'allegato B) del Codice, il quale stabilisce in proposito quanto segue.

Agli incaricati devono essere impartite *istruzioni scritte* finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Quando gli atti e i documenti contenenti *dati personali sensibili o giudiziari* sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i

medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

[Sommaro](#)

12. Adempimenti

Il titolo VI della parte I del Codice della privacy (artt. 37-41) disciplina gli “adempimenti” posti a carico del titolare del trattamento di dati personali.

Notificazione.

Innanzitutto, in ordine alla *notificazione del trattamento*, deve rilevarsi che l'intento di semplificazione perseguito dal legislatore ha condotto all'inversione della regola rispetto alla normativa precedente⁹⁷.

⁹⁷ Cfr. art. 18 direttiva 95/46/CE; artt. 7 e 28 L. 675/1996; art. 13 DPR 501/1998.

“Gli articoli 37 e 38 completano l'intervento di semplificazione e razionalizzazione del sistema delle notificazioni già avviato dal decreto legislativo n. 467/2001, rivelatosi, sulla base dell'esperienza, per alcuni aspetti non indispensabile rispetto alle reali finalità di trasparenza perseguite dalla direttiva comunitaria. Con le modifiche apportate, si snelliscono gli adempimenti in favore sia di soggetti privati, sia della pubblica amministrazione. Si prevede, infatti,

L'art. 37, comma 1, del testo unico in esame sancisce infatti l'obbligo per il titolare di notificare al Garante il trattamento di dati personali cui intende procedere *solo allorché il trattamento riguardi una delle ipotesi tassativamente elencate dalla medesima disposizione*⁹⁸.

Tra queste, si ricordano in particolare quelle relative a:

- *dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica* (art. 37, comma 1, lett. a));
- *dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti*

l'individuazione di un elenco 'in positivo' di un numero più ristretto di categorie di trattamenti soggetti a notificazione, modificando il precedente impianto della normativa che, com'è noto, prevedeva un obbligo più ampio di effettuare la notificazione e individuava, poi, alcuni casi di esonero dall'obbligo o forme semplificate di notificazione. Il codice, completando, come si è detto, l'intervento normativo avviato dal d.lg. n. 467/2001, che aveva individuato le linee generali del nuovo sistema e demandato ad un regolamento governativo la determinazione dei casi e della modalità della notificazione, individua in positivo le tipologie dei trattamenti oggetto di notificazione al Garante in quanto suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato" (così la relazione di accompagnamento al Codice).

⁹⁸ Oltre alle ipotesi di cui nel testo, si tratta di:

- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

(art. 37, comma 1, lett. d)).

Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'art. 17 del Codice.

Con analogo provvedimento pubblicato sulla Gazzetta ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui sopra, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.

Il Garante inserisce le notificazioni ricevute in un *registro dei trattamenti* accessibile a chiunque e determina le modalità per la sua *consultazione gratuita per via telematica*, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio⁹⁹. Le notizie accessibili tramite la consultazione del registro possono essere trattate per *esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali*.

Con riguardo alle *modalità* con le quali deve essere eseguita la notificazione del trattamento, ove richiesta, l'art. 38 prevede che essa sia presentata al Garante *prima dell'inizio del trattamento ed una sola volta*, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno

⁹⁹ Il *registro dei trattamenti* è disponibile per via telematica nel sito del Garante all'indirizzo <https://web.garanteprivacy.it/rgt/NotificaTelematica.php>. Nello stesso sito è presente altresì il *modello per la notificazione telematica* di cui appresso nel testo.

o più trattamenti con finalità correlate¹⁰⁰.

La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione¹⁰¹. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

Una nuova notificazione è richiesta solo *anteriamente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.*

Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.

Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'art. 37 sopra esaminato è in ogni caso tenuto a fornire le notizie contenute nel modello di cui sopra a chiunque ne faccia richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque¹⁰².

¹⁰⁰ Cfr. art. 19 direttiva 95/46/CE; artt. 7 e 16 L. 675/1996; art. 12 DPR 501/1998.

¹⁰¹ Sulla *firma digitale* si veda G. Briganti, *Le firme elettroniche*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/doc-firme.htm e successivi aggiornamenti.

¹⁰² L'art. 39 del Codice disciplina inoltre gli *obblighi di comunicazione* al Garante posti a carico del titolare di particolari trattamenti.

Il titolare del trattamento è tenuto infatti a *comunicare previamente al Garante* le seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

Autorizzazioni.

Come già previsto, ai sensi dell'art. 40, le disposizioni del Codice che prevedono un'*autorizzazione del Garante* sono applicate anche mediante il rilascio di autorizzazioni relative a *determinate categorie di titolari o di trattamenti*, pubblicate nella Gazzetta ufficiale della Repubblica italiana (c.d. *autorizzazioni generali*)¹⁰³.

Ai sensi del successivo art. 41¹⁰⁴, il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'art. 40 *non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni*. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'art. 40 il Garante può provvedere comunque sulla richiesta, se le specifiche modalità del

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'art. 110, comma 1, primo periodo.

I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione, salvo diversa determinazione anche successiva del Garante.

¹⁰³ Cfr. art. 41 L. 675/1996; art. 14 DPR 501/1998.

Con deliberazione del 24 giugno 2003 (GU 191 del 19 agosto 2003), in vista dell'entrata in vigore del Codice, il Garante della privacy ha disposto la proroga al *30 giugno 2004* dell'efficacia delle sei autorizzazioni generali per il trattamento dei dati sensibili e di quella per il trattamento dei dati giudiziari rilasciate il 31 gennaio 2002 (GU 83 del 9 aprile 2002, Suppl. ord.).

Le autorizzazioni, il cui testo può essere consultato su www.privacy.it all'indirizzo www.privacy.it/garautor2002.html, concernono: il trattamento dei dati sensibili nei rapporti di lavoro (1/2002); il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (2/2002); il trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni (3/2002); il trattamento dei dati sensibili da parte dei liberi professionisti (4/2002); il trattamento dei dati sensibili da parte di diverse categorie di titolari (5/2002); il trattamento di dati sensibili da parte degli investigatori privati (6/2002); il trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici (7/2002).

¹⁰⁴ Cfr. art. 14 DPR 501/1998.

trattamento lo giustificano¹⁰⁵.

Sommario

13. Trasferimento dei dati all'estero

Il titolo VII della parte I del Codice della privacy (artt. 42-45) reca la disciplina del *trasferimento dei dati all'estero*¹⁰⁶.

¹⁰⁵ L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'art. 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni di cui all'art. 26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

¹⁰⁶ Cfr. artt. 25 e 26 direttiva 95/46/CE.

“Il titolo VII reca la disciplina del trasferimento dei dati all'estero (già contenuta nell'art. 28 della legge n. 675/1996), riportata, ora, nel codice in maniera più chiara ed organica con la formulazione di tre distinte disposizioni.

In sintesi, gli interventi di razionalizzazione tendono nuovamente, in linea con la direttiva 95/46/CE:

a) a semplificare il sistema del trasferimento dei dati verso Paesi non appartenenti all'Unione europea, con l'esclusione dell'obbligo di notificare specificamente al Garante il trasferimento dei dati (l'obbligo è adempiuto, una tantum, con l'unica notifica eventualmente dovuta ai sensi dell'art. 37) e con la conseguente soppressione dell'obbligo di attendere il decorso del termine originariamente prima di poter procedere al trasferimento dei dati (art. 28, comma 2, l. n. 675/1996);

b) ad assicurare la piena simmetria della disciplina del trattamento dei dati personali effettuato a fini di trasferimento dei dati all'estero con quella relativa al trattamento sul territorio nazionale (art. 43, comma 1, lett. b) e d))” (così la relazione di accompagnamento).

Più approfonditamente, in argomento si veda, con riferimento alla previgente disciplina, M. De Giorgi, *Le problematiche relative al trasferimento dei dati all'estero*, in *La privacy in Internet* cit., pp. 79 ss. e autori ivi citati; M. Bellabarba, *Gli sviluppi dei trasferimenti transfrontalieri dei dati*

Con riferimento alla Rete, è interessante notare preliminarmente come, secondo quanto precisato dalla Corte di Giustizia Europea con sentenza 6 novembre 2003 (C-101/01), *l'inserimento da parte di una persona che si trovi in uno Stato membro di dati personali in una pagina Internet, caricata presso un web hosting stabilito nello Stato stesso o in un altro Stato membro, così da rendere accessibili detti dati a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi, non costituisce un "trasferimento verso un paese terzo di dati" ai sensi dell'art. 25 della direttiva 95/46/CE*¹⁰⁷.

Ciò premesso, l'art. 42 del Codice della Privacy stabilisce, con riferimento ai *trasferimenti all'interno dell'Unione europea*, che le disposizioni del testo unico non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso Codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Il successivo art. 43 enuncia invece quali sono i *trasferimenti consentiti rispetto a Paesi non appartenenti all'Unione europea*¹⁰⁸.

Ai sensi della norma citata, *il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito solo quando:*

a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati

personali dopo l'adozione delle "standard contractual clauses", in www.privacy.it, www.privacy.it/bellabarba02.html.

¹⁰⁷ Il testo integrale della pronuncia richiamata è disponibile su www.altalex.com all'indirizzo www.altalex.com/index.php?idnot=4870.

¹⁰⁸ Cfr. artt. 26 e 28 L. 675/1996; art. 7 D.L.vo 281/1999.

sensibili, in forma scritta;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli artt. 20 e 21;

d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo¹⁰⁹;

e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici

¹⁰⁹ Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'art. 82, comma 2.

presso archivi privati dichiarati di notevole interesse storico ai sensi dell'art. 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

Inoltre, in base all'art. 44¹¹⁰, il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito *quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato*:

a) individuate dal Garante anche in relazione a garanzie prestate con un contratto;

b) individuate con le decisioni previste dagli artt. 25, par. 6, e 26, par. 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Fuori dei casi di cui agli artt. 43 e 44 sopra esaminati, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato *quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato*. Sono valutate a questo proposito anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza (art. 45)¹¹¹.

¹¹⁰ Cfr. art. 28 L. 675/1996.

¹¹¹ Cfr. art. 28 L. 675/1996.

Sommario

CAPITOLO III

LA DISCIPLINA DI ATTUAZIONE DELLA DIRETTIVA 2002/58/CE SULLE COMUNICAZIONI ELETTRONICHE

SOMMARIO: 1. [Premessa. Ambito di applicazione e definizioni](#) – 2. [Sicurezza](#) – 3. [Riservatezza delle comunicazioni](#) – 4. [Dati relativi al traffico](#) – 5. [Fatturazione dettagliata](#) – 6. [Identificazione della linea](#) – 7. [Dati relativi all'ubicazione](#) – 8. [Chiamate di disturbo e di emergenza](#) – 9. [Trasferimento automatico della chiamata](#) – 10. [Elenchi di abbonati](#) – 11. [Comunicazioni indesiderate e spamming](#) – 11.1. [Le comunicazioni indesiderate \(unsolicited communications\) nella direttiva 2002/58/CE](#) – 11.2. [La disciplina contenuta nel D.L.vo 171/1998 di attuazione della direttiva 97/66/CE](#) – 11.3. [L'art. 13 della direttiva 2002/58/CE](#) – 11.4. [L'art. 130 del Codice della privacy](#) – 11.5. [Codice di deontologia e di buona condotta per il marketing diretto](#) – 11.6. [Altre norme rilevanti in materia di spamming](#) – 12. [Segue: il provvedimento generale sullo spamming del Garante per la protezione dei dati personali](#) – 13. [Segue: le regole della Netiquette, l'attività della Naming Authority; iniziative e responsabilità dei provider](#) – 14. [Informazioni ad abbonati e utenti](#) – 15. [Conservazione di dati di traffico per altre finalità](#) – 16. [Internet e reti telematiche](#) – 17. [Videosorveglianza](#)

[INDICE](#)

1. Premessa. Ambito di applicazione e definizioni

Come già rilevato, in base all'art. 6 del [Codice della privacy](#), le disposizioni contenute nella parte I del provvedimento, illustrate nel precedente capitolo, sono destinate a trovare applicazione rispetto a *tutti i trattamenti di dati personali*, fatte

salve le disposizioni integrative o modificative della parte II relative a determinati trattamenti.

Per quel che qui interessa, occorre pertanto prendere ora in esame le norme del testo unico dettate specificamente per la materia delle *comunicazioni elettroniche*¹.

Il titolo X della parte II del Codice (artt. 121-134) reca infatti la disciplina italiana di attuazione della [direttiva 2002/58/CE](#) sulle comunicazioni elettroniche, esaminata nel capitolo I; disciplina che sostituisce, come più volte ricordato, quella già contenuta nel previgente [D.L.vo 171/1998](#) di attuazione dell'abrogata direttiva 97/66/CE².

Ai sensi dell'art. 121 del provvedimento ("Servizi interessati"), le disposizioni del

¹ Per quanto riguarda le *forme di tutela dell'interessato* e le *sanzioni* riconnesse alla violazione di alcune delle norme che ci appresta ad illustrare, si rimanda sin d'ora a quanto si dirà nel capitolo V.

² "Le disposizioni del presente titolo danno attuazione alla direttiva 2002/58 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, secondo quanto previsto dall'articolo 26 della legge 3 febbraio 2003, n. 14 (legge comunitaria 2002) che ha prorogato il termine per l'adozione del presente codice anche al fine del previo recepimento della predetta direttiva.

Com'è noto, la direttiva 2002/58 ha sostituito la precedente direttiva 97/66/CE del 15 dicembre 1997, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni, recepita nel nostro ordinamento con il decreto legislativo 13 maggio 1998, n. 171 e con alcuni mirati interventi di completamento apportati al medesimo d.lg. n. 171/1998 dal decreto legislativo n. 467/2001 (artt. 21, 22 e 23, in materia di modalità di pagamento alternative alla fatturazione, di informazione al pubblico sull'identificazione della linea chiamante e collegata, nonché in materia di chiamate di emergenza).

Il titolo in commento, pertanto, nel 'riportare' nel codice le disposizioni previgenti contenute nel d. lg. n. 171/1998, le modifica ed integra al fine di attuare le disposizioni della direttiva n. 2002/58 innovative o specificative della precedente direttiva.

La corrispondenza degli articoli del codice con gli articoli del d. lg. n. 171/1998, può agevolmente essere confrontata ricorrendo alla tavola sinottica allegata al codice, dove, per ulteriore chiarezza, sono state riportate anche le pertinenti disposizioni della direttiva 2002/58" (così la relazione di accompagnamento al Codice).

titolo X della parte II *si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni*³.

Con riferimento alle *definizioni* vevoli ai fini della disciplina, si rimanda a quanto già detto nel capitolo precedente⁴. Una precisazione deve però essere fatta a proposito delle “reti di comunicazione elettronica”, definite dall’art. 4 del Codice come “i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via

³ Cfr. art. 3 direttiva 2002/58/CE (cap. I, par. 2).

Si ricorda che per *servizi di comunicazione elettronica* devono intendersi 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’art. 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica.

⁴ V. cap. II, par. 2.

Per un confronto con la previgente disciplina, si riportano le definizioni contenute nell’art. 1 del D.L.vo 171/1998:

“1. Ai fini del presente capo, si applicano le definizioni elencate nell’articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini, si intende per:

- a) ‘abbonato’: 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;
- b) ‘utente’: la persona fisica che utilizza uno o più servizi di telecomunicazioni accessibili al pubblico, indipendentemente dall’eventuale qualità di abbonato;
- c) ‘rete pubblica di telecomunicazioni’: un sistema di trasmissione e, se del caso, le apparecchiature di commutazione o le altre risorse che permettono la trasmissione di segnali tra punti terminali di rete definiti, con mezzi a filo, radio, ottici o altri mezzi elettromagnetici utilizzati, in tutto o in parte, per fornire servizi di telecomunicazioni accessibili al pubblico;
- d) ‘servizio di telecomunicazioni’: un servizio la cui fornitura consiste, in tutto o in parte, nella trasmissione e nell’instradamento di segnali su reti di telecomunicazioni, ivi compreso qualunque servizio interattivo anche se relativo a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi”.

radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse 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 sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato”.

È stato infatti osservato in proposito che “La definizione è particolarmente ampia tanto da ricomprendere elementi tecnicamente attestati su livelli diversi e che sembra difficile poter equiparare in termini normativi. Così vengono messi sullo stesso piano gli apparati di trasmissione, le apparecchiature di commutazione o instradamento e le infrastrutture. Queste ultime distinte ancora in ‘sistemi di trasmissione’ e ‘reti’ *tout-court*. Inoltre, nell’elenco delle reti oggetto di attenzione legislativa viene inclusa – con seria perplessità dell’interprete – anche l’internet” (A. Monti)⁵.

Dalla lettura della norma definitoria sopra richiamata pare dunque di capire che per il legislatore Internet (più propriamente: l’internet) sarebbe un mezzo di trasmissione analogo a reti a commutazione di circuito o di pacchetto; cosa che però non corrisponde alla realtà, considerato che l’internet non è una rete fisica bensì una *suite* di protocolli, come tale utilizzabile su di una pluralità di reti tecnologicamente diverse⁶.

[Somario](#)

⁵ A. Monti, *Decreto legislativo 196/03: l’internet non è una rete* cit.

La definizione accolta dal Codice della privacy riproduce d’altra parte pedissequamente quella di cui alla direttiva 2002/21/CE, richiamata dalla direttiva 2002/58/CE (cap. I, par. 2).

⁶ *Ibidem*.

2. Sicurezza

Contrariamente agli altri aspetti della disciplina oggetto della direttiva 2002/58/CE, la *sicurezza* in materia di comunicazioni elettroniche viene specificamente regolata già dalla parte I del Codice, nell'ambito delle disposizioni sulla "sicurezza dei dati e dei sistemi" valide per tutti i trattamenti, esaminate nel capitolo precedente (artt. 31-36 del Codice e relativo disciplinare tecnico)⁷.

Con particolare riferimento, dunque, ai *fornitori di un servizio di comunicazione elettronica accessibile al pubblico*, l'art. 32⁸ prevede che costoro siano tenuti ad adottare, ai sensi dell'art. 31, *idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei loro servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita*.

Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico deve adottare tali misure *congiuntamente con il*

⁷ Cap. II, parr. 11 e ss.

⁸ Cfr. art. 4 direttiva 2002/58/CE (cap. I, par. 3).

L'art. 2 ("Sicurezza") dell'abrogato D.L.vo 171/1998 prevedeva quanto segue.

"1. Il fornitore di un servizio di telecomunicazioni accessibile al pubblico adotta le misure tecniche e organizzative di cui all'articolo 15, comma 1, della legge 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".

fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente (art. 32, comma 2).

Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico è tenuto inoltre ad *informare gli abbonati e, ove possibile, gli utenti, dell'eventuale sussistenza di un particolare rischio di violazione della sicurezza della rete*, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi delle disposizioni sopra illustrate, *tutti i possibili rimedi e i relativi costi presumibili*. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni (art. 32, comma 3).

L'art. 32 ripropone dunque, pressoché integralmente, salvo per la terminologia che è adeguata alla direttiva 2002/58/CE, l'art. 2 dell'abrogato D.L.vo 171/1998. La norma, in attuazione della specifica previsione contenuta nella direttiva sulle comunicazioni elettroniche, prevede inoltre, come sopra visto, che le misure debbano essere adottate *anche per salvaguardare l'integrità dei dati trattati e delle comunicazioni elettroniche contro il rischio di intercettazione o altra abusiva cognizione ed utilizzazione*⁹.

[Sommaro](#)

3. Riservatezza delle comunicazioni

Ai sensi dell'art. 122 ("Informazioni raccolte nei riguardi dell'abbonato o

⁹ Cfr. art. 5 direttiva 2002/58/CE (cap. I, par. 4).

dell'utente")¹⁰, comma 1, del Codice, salvo quanto previsto dal successivo comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

Al codice di deontologia di cui all'art. 133 del Codice¹¹ è demandato poi il compito di individuare i presupposti e i limiti entro i quali l'uso della rete nei modi di cui sopra, *per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente*, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il *consenso* sulla base di una *previa informativa* ai sensi dell'art. 13¹² che indichi analiticamente, in modo chiaro e preciso, *le finalità e la durata del trattamento* (art. 122, comma 2).

Si ricorda che, secondo quanto previsto dall'art. 12 del testo unico¹³, il rispetto delle disposizioni contenute nei codici di deontologia e buona condotta costituisce

¹⁰ Cfr. art. 5 direttiva 2002/58/CE (cap. I, par. 4).

Per un confronto con la disciplina previgente, si riporta il testo dell'art. 3 ("Riservatezza nelle comunicazioni") del D.L.vo 171/1998.

"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 a 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".

¹¹ Sul quale si veda *infra*, par. 16.

¹² Cap. II, par. 5.

¹³ Cap. II, par. 5.

condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti pubblici e privati.

Con l'articolo in parola, il legislatore italiano ha inteso dunque dare attuazione alla corrispondente disposizione contenuta nell'art. 5 della direttiva 2002/58/CE avente ad oggetto, in particolare, come visto nel capitolo I, *web bugs*, *cookies* e *spyware*.

Occorre però sin d'ora evidenziare, come si vedrà meglio nel prosieguo, che la violazione dell'art. 122 del Codice è sprovvista di sanzione, di tipo amministrativo o penale, ferma restando l'eventuale responsabilità civile in ordine al risarcimento del danno, ai sensi dell'art. 15 del testo unico, in capo al titolare del trattamento, da valutarsi anche con riferimento al previsto codice di deontologia¹⁴.

[Sommaro](#)

4. Dati relativi al traffico

Con parere del 29/01/2003, il *Gruppo europeo di lavoro per la tutela dei dati personali*, preso atto che “Sono emerse indicazioni dell'esistenza di divergenze nella prassi seguita dalle società di comunicazioni elettroniche negli Stati membri riguardo ai periodi di memorizzazione dei dati relativi al traffico”, rilevava che “è quindi importante adottare misure per interpretare in maniera armonizzata il periodo limitato durante il quale i fornitori di servizi di telecomunicazioni sono autorizzati a trattare i dati relativi al traffico a fini di fatturazione e di pagamenti di interconnessione”.

¹⁴ Con possibilità di ottenere il risarcimento anche dei danni non patrimoniali (cap. II, par. 5).

Il Gruppo ritiene pertanto che un'interpretazione ragionevole delle direttive in tema di tutela dei dati è quella secondo la quale un *periodo di memorizzazione normale ai fini della fatturazione dura un massimo di 3-6 mesi, fatta eccezione per casi particolari di controversie in cui i dati possono essere sottoposti a trattamento per un periodo più lungo*. Inoltre, prosegue il Gruppo, possono essere sottoposti a trattamento soltanto i *dati relativi al traffico che sono adeguati, pertinenti e non eccedenti ai fini della fatturazione e dei pagamenti di interconnessione*. Gli altri dati relativi al traffico devono essere cancellati¹⁵.

Secondo quanto sancito dall'art. 123 ("Dati relativi al traffico")¹⁶, comma 1, del

¹⁵ Il testo integrale del parere può essere consultato su www.europa.eu.int/comm/privacy.

¹⁶ Cfr. art. 6 direttiva 2002/58/CE (v. cap. I, par. 5).

L'art. 4 ("Dati relativi al traffico e alla fatturazione del servizio") dell'abrogato D.L.vo 171/1998 prevedeva quanto segue.

"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;
- 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.

Codice della privacy, i dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico devono essere cancellati o resi anonimi quando non più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei successivi commi 2, 3 e 5.

Il comma 2 della disposizione richiamata prevede che il trattamento dei dati relativi al traffico *strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione*, è consentito al fornitore, *a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi*, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

Ai sensi del successivo comma tre, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui sopra anche nella misura e per la durata necessarie a fini di *commercializzazione di servizi di comunicazione elettronica* o per la *fornitura di servizi a valore aggiunto*, a condizione che l'abbonato o l'utente cui i dati si riferiscono abbiano manifestato il proprio *consenso*, che rimane, in ogni caso, revocabile in ogni momento.

Come spiega la relazione di accompagnamento, rispetto alla previgente disposizione (art. 4, comma 3, D.L.vo 171/1998), il comma 3 è integrato con la

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”.

previsione che il consenso espresso dall'abbonato o dall'utente al trattamento dei dati personali a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, può essere *revocato in ogni momento*.

Si prevede inoltre che nel fornire l'informativa di cui all'art. 13 del Codice¹⁷ il fornitore del servizio informi l'abbonato o l'utente sulla *natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento* ai fini di cui ai commi 2 e 3 sopra illustrati (comma 4).

Come si legge nella relazione di accompagnamento, il comma 4, interamente innovativo, introduce una specifica garanzia di trasparenza per l'abbonato o per l'utente, precisando che nel fornire l'informativa di cui all'art. 13, il fornitore del servizio, in relazione ai trattamenti appena descritti, *deve informare espressamente l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata dei medesimi trattamenti* (cfr. art. 6, par. 4, direttiva 2002/58/CE).

Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'art. 30¹⁸ sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche

¹⁷ V. cap. II, par. 5.

¹⁸ V. cap. II, par. 10.

mediante un'operazione di interrogazione automatizzata (art. 123, comma 5).

L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione (comma 6).

[Sommaro](#)

5. Fatturazione dettagliata

Secondo quanto previsto dall'art. 124 ("Fatturazione dettagliata")¹⁹, comma 1, del Codice, l'abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, *la dimostrazione degli elementi che compongono la fattura* relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti

¹⁹ Cfr. art. 7 direttiva 2002/58/CE (cap. I, par. 7).

Si riporta il testo della corrispondente disposizione dell'abrogato D.L.vo 171/1998.

"Art. 5. *Modalità di pagamento e fatturazione dettagliata.* 1. I fornitori di servizi di telecomunicazioni accessibili al pubblico sono tenuti a predisporre ogni misura idonea affinché i servizi richiesti e le chiamate effettuate da qualsiasi terminale possano essere pagate con modalità alternative alla fatturazione, anche anonime, quali le carte di pagamento o prepagate.

1bis. I fornitori di cui al comma 1 sono tenuti a documentare al Garante, entro il 30 giugno 2002, le misure predisposte. In caso di mancata documentazione si applica la sanzione amministrativa prevista dall'articolo 39, comma 1, della legge 31 dicembre 1996, n. 675. In mancanza di idonee misure il Garante provvede altresì ai sensi dell'articolo 31, comma 1, lettere c) ed l), della medesima legge.

2. Nella documentazione relativa alle chiamate effettuate inviate agli abbonati non vengono evidenziati i servizi e le chiamate di cui al comma 1.

3. Gli abbonati hanno diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo, alla località, alla durata, al numero di scatti addebitati per ciascuna conversazione. In ogni caso nella documentazione fornita all'abbonato non sono evidenziate le ultime tre cifre del numero chiamato".

addebitati per ciascuna conversazione.

Il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto inoltre ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di *modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate* (art. 124, comma 2). Nella documentazione inviata all'abbonato relativa alle comunicazioni effettuate non sono evidenziati i servizi e le comunicazioni di cui sopra, né le comunicazioni necessarie per attivare le modalità alternative alla fatturazione.

Nella fatturazione all'abbonato *non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati*, è d'altra parte previsto il diritto per l'abbonato di richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

Il Garante per la protezione dei dati personali, accertata l'effettiva disponibilità delle modalità alternative di cui all'esaminato art. 124, comma 2, può *autorizzare* il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

L'art. 124 del testo unico, dunque, conferma la previsione del "mascheramento" sulle fatture delle ultime tre cifre dei numeri chiamati, ma in linea con il progressivo adeguamento dei fornitori alla previsione comunitaria, a seguito dell'ampia diffusione in Italia dei mezzi di pagamento alternativi, prevede altresì che il Garante, accertata l'effettiva disponibilità di tali mezzi, possa autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

[Sommaro](#)

6. Identificazione della linea

Ai sensi dell'art. 125 ("Identificazione della linea")²⁰, comma 1, del Codice della privacy, se è disponibile la *presentazione dell'identificazione della linea chiamante*, il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto ad *assicurare all'utente chiamante la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.*

Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico *deve*

²⁰ Cfr. art. 8 direttiva 2002/58/CE (cap. I, par. 7).

L'art. 6 ("Identificazione della linea") dell'abrogato D.L.vo 171/1998 prevedeva in proposito quanto segue.

"1. Se è disponibile la presentazione dell'identificazione della linea chiamante, l'utente chiamante deve avere la possibilità di eliminare, gratuitamente e mediante una funzione semplice, la presentazione della identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere la stessa possibilità linea per linea.

2. Se è disponibile la presentazione dell'identificazione della linea chiamante, l'abbonato chiamato deve avere la possibilità, gratuitamente e mediante una funzione semplice, di impedire la presentazione dell'identificazione delle chiamate entranti.

3. Se è disponibile la presentazione della linea chiamante e tale identificazione è presentata prima che la comunicazione sia stabilita, l'abbonato chiamato deve avere la possibilità, gratuitamente e 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.

4. Se è disponibile la presentazione dell'identificazione della linea collegata, l'abbonato chiamato deve avere la possibilità di eliminare, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano alle chiamate dirette verso altri Paesi; quelle di cui ai commi 2, 3 e 4 si applicano anche alle chiamate in arrivo da altri Paesi.

6. Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore di una rete di telecomunicazioni pubblica o di un servizio di telecomunicazioni accessibili al pubblico deve informare gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità, previste ai commi 1, 2, 3 e 4".

assicurare inoltre all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti (art. 125, comma 2).

Se è disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto altresì ad assicurare all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante (art. 125, comma 3).

Se è invece disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico deve assicurare all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante (art. 125, comma 4).

Le disposizioni di cui all'art. 125, comma 1, sopra esaminate si applicano anche alle chiamate dirette verso Paesi non appartenenti all'Unione europea. Le disposizioni di cui ai successivi commi 2, 3 e 4 si applicano anche alle chiamate provenienti da tali Paesi.

Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, si prevede infine che il fornitore del servizio di comunicazione elettronica accessibile al pubblico sia tenuto ad *informare gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità previste ai sensi delle disposizioni dell'art. 125 sopra illustrate.*

L'art. 125 riproduce dunque pressoché pedissequamente l'art. 6 del D.L.vo 171/1998, come integrato dall'art. 22 del D.L.vo 467/2001.

Sommario

7. Dati relativi all'ubicazione

L'art. 126 (“Dati relativi all'ubicazione”)²¹ del Codice della privacy, con una previsione innovativa, stabilisce che *i dati relativi all'ubicazione diversi dai dati relativi al traffico*²², riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato abbia manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

Il fornitore del servizio, prima di richiedere il consenso, *deve informare* gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al 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 (art. 126, comma 2).

L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, *conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per*

²¹ Cfr. art. 9 direttiva 2002/58/CE (cap. I, par. 6).

Il D.L.vo 171/1998 non si occupava espressamente di tale specifica categoria di dati personali.

²² Giova ricordare che, come già visto, ai sensi dell'art. 4 del Codice della privacy per *dato relativo all'ubicazione* deve intendersi “ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico”.

ciascuna trasmissione di comunicazioni (art. 126, comma 3).

Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi delle norme appena illustrate, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'art. 30²³, sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

[Sommaro](#)

8. Chiamate di disturbo e di emergenza

Ai sensi dell'art. 127 (“Chiamate di disturbo e di emergenza”)²⁴, comma 1, del

²³ Cap. II, par. 10.

²⁴ Cfr. art. 10 direttiva 2002/58/CE (cap. I, par. 7).

L'art. 7 (“Chiamate di disturbo e di emergenza”) del previgente D.L.vo 171/1998 stabiliva in proposito quanto segue.

“1. L'abbonato che riceve chiamate di disturbo può richiedere, a proprie spese e anche telefonicamente in caso di urgenza, che il fornitore del servizio di telecomunicazioni accessibile al pubblico renda inefficace la soppressione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta nei soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. L'istanza formulata per iscritto dall'abbonato deve specificare le modalità di ricezione delle chiamate di disturbo e, nel caso in cui sia preceduta da una richiesta telefonica, deve essere inviata entro ventiquattro ore.

2bis. Il fornitore di una rete di telecomunicazioni pubblica o di un servizio di telecomunicazioni accessibili al pubblico deve predisporre procedure adeguate e trasparenti per garantire, linea per

Codice della privacy, l'abbonato che riceve *chiamate di disturbo* può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico *renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante*²⁵ e *conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.*

La richiesta deve essere formulata per iscritto dall'abbonato e specificare le modalità di ricezione delle chiamate di disturbo. Nel caso in cui sia preceduta da una richiesta telefonica, detta richiesta scritta deve essere inoltrata nelle successive quarantotto ore.

I dati conservati in virtù di quanto sopra possono essere *comunicati all'abbonato che dichiara di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo*. Per i servizi oggetto della disposizione in esame, inoltre, il fornitore è tenuto ad assicurare *procedure trasparenti* nei confronti degli abbonati e può richiedere un *contributo spese* non superiore ai costi effettivamente sopportati.

Con riguardo alle *chiamate di emergenza*, l'art. 127, comma 4, prevede che il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predisponga *procedure trasparenti* per garantire, linea per linea, *l'inefficacia della soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione*²⁶, *nonostante il rifiuto o il mancato consenso temporanei*

linea, l'annullamento della soppressione dell'identificazione della linea chiamante da parte dei servizi abilitati a ricevere chiamate d'emergenza”.

²⁵ Ove disponibile la presentazione del numero chiamante. V. par. 6.

²⁶ V. parr. 6 e 7.

dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. Detti servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante per la protezione dei dati personali e l'Autorità per le garanzie nelle comunicazioni.

L'art. 127 conferma dunque le analoghe previsioni già contenute nell'art. 7 del D.L.vo 171/1998 (come modificato dall'art. 23 D.L.vo 467/2001), introducendo altresì alcune precisazioni finalizzate a rendere più agevole l'applicazione della norma.

[Sommaro](#)

9. Trasferimento automatico della chiamata

Con riguardo al *trasferimento automatico della chiamata*, l'art. 128 del Codice della privacy, confermando quanto già stabilito dal D.L.vo 171/1998, prescrive al fornitore di un servizio di comunicazione elettronica accessibile al pubblico di adottare *le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi*²⁷.

[Sommaro](#)

²⁷ Cfr. art. 11 direttiva 2002/58/CE (cap. I, par. 7).

Si riporta il testo dell'art. 8 dell'abrogato D.L.vo 171/1998.

“Art. 8. *Trasferimento automatico della chiamata*. 1. Il fornitore di un servizio di telecomunicazioni accessibile al pubblico deve adottare le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico verso la propria linea delle chiamate da parte dei terzi”.

10. Elenchi di abbonati

L'art. 129 (“Elenchi di abbonati”)²⁸ del Codice della privacy, nel confermare quanto già previsto, attribuisce al Garante per la protezione dei dati personali il compito di individuare con proprio *provvedimento*, in cooperazione con l’Autorità per le garanzie nelle comunicazioni²⁹, *le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico*, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del Codice.

Il provvedimento di cui sopra individua altresì idonee modalità per la *manifestazione del consenso all’inclusione negli elenchi e, rispettivamente, all’utilizzo dei dati per le finalità di cui all’art. 7, comma 4, lett. b)*, in base al *principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell’abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri*.

L’art. 7, comma 4, lett. b), richiamato dall’art. 129, come visto nel capitolo II, concerne il trattamento di dati personali *a fini di invio di materiale pubblicitario o*

²⁸ Cfr. art. 12 direttiva 2002/58/CE (cap. I, par. 7).

L’art. 9 (“Elenco degli abbonati”) del previgente D.L.vo 171/1998 prevedeva in proposito quanto segue.

“1. I dati personali relativi agli abbonati contenuti in elenchi cartacei o su supporti magnetici od ottici a disposizione del pubblico od ottenibili attraverso i servizi che forniscono informazioni sugli elenchi sono limitati agli elementi necessari per identificare un determinato abbonato, salvo il caso in cui l’abbonato abbia prestato il proprio consenso espresso alla diffusione di ulteriori dati personali. L’abbonato ha diritto, gratuitamente e con richiesta documentata per iscritto, di non essere incluso negli elenchi, di ottenere che il suo indirizzo sia in parte omesso e, se ciò è fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso.

2. Le disposizioni di cui al comma 1 non si applicano agli elenchi cartacei o su altri supporti pubblicati prima della entrata in vigore del presente decreto legislativo”.

²⁹ Ai sensi dell’art. 154, comma 3, del testo unico e in conformità alla normativa comunitaria.

di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale³⁰.

Sommario

11. Comunicazioni indesiderate e spamming

Il termine *spamming*, come noto, viene usato per indicare l'invio di *comunicazioni elettroniche non richieste ad un lungo elenco di destinatari*³¹.

Il contenuto dei messaggi elettronici in questione può essere vario. Essi hanno per lo più *carattere pubblicitario*, ma non solo: possono avere anche, ad esempio, *finalità di propaganda politica o di proselitismo religioso*.

In particolare, i messaggi pubblicitari di posta elettronica inviati con la tecnica dello *spamming* sono definiti anche UCE, acronimo di *Unsolicited Commercial e-*

³⁰ Cfr. deliberazione Autorità per le Garanzie nelle comunicazioni del 13 giugno 2002 n. 180, *Regole e modalità organizzative per la realizzazione e l'offerta di un servizio di elenco telefonico generale: disposizioni attuative* (Deliberazione n. 180/02/CONS; GU 159 del 9 luglio 2002).

³¹ *Spam* era, in origine, il marchio di una carne in scatola nota negli Stati Uniti per la sua scadente qualità. Il linguaggio comune si è poi appropriato del termine per indicare tutto ciò che è di pessima qualità, ed oggi l'uso è invalso su Internet per indicare il genere di e-mail "spazzatura" di cui nel testo. Ciò grazie – pare – a uno sketch comparso nella serie televisiva americana *Monthy Python's Flying Circus*. Per maggiori notizie si rimanda alla pagina web www.collinelli.net/antispam/.

Per un approfondimento in tema di spamming si veda, con riferimento alla previgente disciplina, G. Briganti, *Spamming e diritto*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/doc-spamming.htm e autori ivi citati. Nello stesso sito, si veda inoltre l'*Osservatorio sullo spamming*, all'indirizzo www.iusreporter.it/Testi/osservaspmming.htm. Si veda altresì G. Sisto, *La sollecitazione commerciale nell'e-commerce. Il problema dello spamming*, in *Il commercio via Internet*, a cura di G. Cassano, Piacenza, CELT, 2002, pp.165 ss.; A. Lisi, *Tutela della privacy in Internet* cit. pp. 64 ss.; M.P. Berlingieri, *L'informazione commerciale non desiderata e lo spamming*, in *Privacy.it*, www.privacy.it, www.privacy.it/berlingieri06.html.

mail (e-mail non richieste di carattere commerciale)³².

Lo *spamming* usa diversi canali: quello preferenziale è la posta elettronica, ma può impiegare anche qualsiasi altro mezzo che consenta di raggiungere un alto numero di destinatari (ad esempio newsgroup, chat, mailing list, SMS).

I c.d. *spammer*, coloro che inviano questo genere di messaggi-spaZZatura a grandi liste di destinatari, reperiscono gli indirizzi e-mail necessari all'operazione con diversi metodi: acquistando "pacchetti" di indirizzi da siti che richiedono la registrazione dell'utente; acquisendoli da elenchi presenti in rete, dai vari newsgroup e forum o da siti sulle cui pagine figurano indirizzi e-mail.

L'invio di grandi quantità di e-mail non sollecitate comporta dispendi di tempo e di denaro per chi lo subisce. Nel caso del c.d. *mail bombing*, inoltre, può prodursi il rallentamento o perfino il blocco dei sistemi degli *Internet Service Provider*³³.

Le norme giuridiche italiane rilevanti in materia sono oggi, innanzitutto, quelle contenute nel [Codice della privacy](#), in particolare nel suo art. 130 di attuazione dell'art. 13 della [direttiva 2002/58/CE](#); in secondo luogo, quelle contenute nel [D.L.vo 185/1999](#) concernente i contratti a distanza conclusi dai consumatori nonché nel [D.L.vo 70/2003](#) di attuazione della direttiva europea sul commercio elettronico³⁴.

Un cenno dovrà infine, con riguardo alla Rete, essere fatto anche alle regole di *Netiquette* e all'attività della *Naming Authority italiana* volta ad assicurarne

³² Si parla anche di *junk e-mail*.

³³ Si parla di *mail bombing* quando l'invio di grandi quantità di e-mail è finalizzato appunto a causare il rallentamento od il blocco di sistemi informatici.

³⁴ Sul D.L.vo 70/2003 si rimanda a quanto si dirà nel prossimo capitolo. Con riguardo alla tutela accordata all'interessato ed alle sanzioni previste in materia di spamming si veda il cap. V.

l'applicazione, nonché alle iniziative prese in relazione al fenomeno spamming da alcuni provider.

11.1. Le comunicazioni indesiderate (unsolicited communications) nella direttiva 2002/58/CE

Il considerando 40 della direttiva europea 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 2002/58/CE detta dunque una disciplina specifica delle comunicazioni indesiderate, in luogo di quella già contenuta, come visto nel capitolo I, nell'abrogata direttiva 97/66/CE attuata in Italia con il D.L.vo 171/1998.

11.2. La disciplina contenuta nel D.L.vo 171/1998 di attuazione della direttiva

97/66/CE

Entro il proprio ambito di applicazione³⁵, l'art. 10 ("Chiamate indesiderate"), comma 1, del previgente D.L.vo 171/1998, con riguardo alla *tutela della vita privata nel settore delle telecomunicazioni*, stabiliva 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 di ricerche di mercato o di comunicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato"³⁶.

Ai fini del provvedimento richiamato, per *abbonato* doveva 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)³⁷.

³⁵ V. G. Briganti, *Spamming e diritto* cit.

³⁶ L'art. 12 ("Chiamate indesiderate") della direttiva 97/66/CE prevedeva in proposito quanto segue.

"1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata) o di telefax (telecopia) per scopi di invio di materiale pubblicitario può essere consentito soltanto nei confronti degli abbonati che hanno dato preventivamente il loro consenso.

2. Gli Stati membri adottano le misure appropriate per garantire che, gratuitamente, le chiamate indesiderate a scopo di invio di materiale pubblicitario, con mezzi diversi da quelli di cui al paragrafo 1, non siano permesse o senza il consenso dell'abbonato interessato o nei confronti di abbonati che non desiderino ricevere questo tipo di chiamate; la scelta tra queste due possibilità è stabilita dalla normativa nazionale.

3. I diritti di cui ai precedenti paragrafi 1 e 2 si applicano agli abbonati che sono persone fisiche. Gli Stati membri garantiscono, inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela dei legittimi interessi degli abbonati che sono persone fisiche, relativamente alle chiamate indesiderate".

³⁷ Per la definizione di *servizio di telecomunicazioni* si veda l'art. 1, lett. d), del D.L.vo 171/1998 (nota n. 4).

Come sopra visto (cap. I, par. 2; cap. II, par. 2), la direttiva 2002/58/CE così come la relativa normativa italiana di attuazione fanno oggi riferimento non più al "servizio di telecomunicazioni" bensì al "servizio di comunicazione elettronica".

La disposizione prevedeva inoltre che le chiamate effettuate per le medesime finalità di cui sopra, ma con mezzi diversi da quelli ivi indicati, fossero consentite ai sensi degli artt. 11 e 12 della [L. 675/1996](#) (art. 10, comma 2, D.L.vo 171/1998).

In caso di violazione dell'art. 10, l'art. 11 D.L.vo 171/1998 stabiliva l'applicazione delle sanzioni penali di cui all'art. 35 L. 675/1996 ("Trattamento illecito di dati personali").

La disposizione in esame riguardava 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 veniva effettuata per scopi diversi, l'art. 10 D.L.vo 171/1998 non poteva dunque, in nessun caso, trovare applicazione³⁸.

Il comma 1 dell'articolo in parola non menzionava 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* poteva ricomprendersi anche l'invio di e-mail per i fini contemplati dalla norma.

In caso di risposta affermativa avrebbe trovato infatti applicazione il comma 1 dell'art. 10 D.L.vo 171/1998, mentre in caso di risposta negativa, stante il richiamo operato dal comma 2, ci si sarebbe dovuti rifare agli artt. 11 e 12 L.

³⁸ Potevano 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* cit.

675/1996³⁹.

11.3. 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 automatici di chiamata), del *telefax* o della *posta elettronica a fini di commercializzazione diretta (direct marketing)* è 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, secondo la direttiva, al *preliminare consenso dell'abbonato*, vale a dire, come visto nel capitolo I, 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 (c.d. *opt-in*).

Fatto salvo il paragrafo 1 dell'art. 13, appena illustrato, nell'ambito di una *relazione di clientela già esistente*, la direttiva prevede inoltre che quando una persona fisica o giuridica ottiene 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).

³⁹ Il Garante per la protezione dei dati personali pare avesse accolto la soluzione negativa. Si veda in proposito G. Briganti, *Spamming e privacy*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/spamming1.htm.

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 esprimono 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 ora in parola 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 destinatario⁴⁰.

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 applicazione⁴¹.

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 fisiche⁴².

Occorre rilevare altresì 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.

⁴⁰ V. cap. IV.

⁴¹ Analogamente a quanto accadeva, come sopra visto, con l'art. 10 D.L.vo 171/1998.

⁴² 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 (v. cap. IV).

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, l'art. 15, par. 2, del provvedimento stabilisce che le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità ed alle sanzioni si applichino relativamente alle disposizioni nazionali adottate in base alla direttiva in esame e con riguardo ai diritti individuali risultanti dalla stessa.

11.4. L'art. 130 del Codice della privacy

L'art. 13 della direttiva 2002/58/CE, come già si è avuto modo di rilevare, ha trovato attuazione in Italia con l'art. 130 del Codice della privacy ("Comunicazioni indesiderate").

Nell'ambito di applicazione del titolo X della parte II del Codice⁴³, la suddetta disposizione prevede dunque innanzitutto che l'uso di *sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato*.

Si prevede espressamente, altresì, che la norma di cui sopra si applichi anche alle comunicazioni elettroniche *effettuate per le finalità ivi indicate mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo* (art. 130, comma 2)⁴⁴.

⁴³ V. par. 1.

⁴⁴ Vale la pena notare che la disposizione in esame va a colpire ogni singola comunicazione elettronica indesiderata, *indipendentemente dal numero dei suoi destinatari*.

Rispetto alla previsione dell'art. 13 della direttiva 2002/58/CE, risulta dunque più ampio l'ambito di applicazione della regola dell'*opt-in* di cui al comma 1 dell'art. 130 del Codice, il quale finisce col riferirsi, oltre che a dispositivi automatici di chiamata, fax, e-mail, MMS e SMS anche a qualunque "messaggio di altro tipo".

Confrontando inoltre il testo della norma ora in esame con quello del previgente 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 consenso dell'interessato. La nuova disposizione pare dunque destinata a risolvere gli accennati problemi interpretativi relativi al campo di applicazione del comma 1 dell'abrogato art. 10 D.L.vo 171/1998.

Da notare altresì che l'art. 130 si riferisce, in generale, agli *interessati*, mentre nella direttiva 2002/58/CE, così come anche nel D.L.vo 171/1998, il riferimento andava ai soli *abbonati*⁴⁵.

Fuori dei casi di cui ai commi 1 e 2 dell'art. 130, appena illustrati, ulteriori comunicazioni *per le finalità di cui ai medesimi commi* ma effettuate *con mezzi*

Con riferimento a MMS e privacy si ricorda anche il parere espresso dal Garante per la protezione dei dati personali in data 12/03/2003 (www.iusreporter.it/Testi/agg-privacy.htm).

⁴⁵ Giova in proposito ricordare che, come visto nel capitolo II, l'art. 4 del testo unico definisce *interessato* "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali". L'art. 2 della direttiva 2002/58/CE, nel richiamare la direttiva 2002/21/CE, definisce invece *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" (cap. I, par. 2). Ai sensi dell'abrogato D.L.vo 171/1998, infine, per *abbonato* doveva 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".

Nella nozione di *interessato* rilevante ai fini dell'art. 130 del testo unico ricadono dunque anche *persone giuridiche, enti ed associazioni*. L'art. 13, par. 5, della direttiva 2002/58/CE, come visto nel capitolo I, si limita invece a imporre agli Stati membri di garantire "un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche", senza pertanto richiedere per tali soggetti diversi dalle persone fisiche la necessaria adozione di un regime di *opt-in* in ordine alle comunicazioni commerciali.

diversi da quelli ivi indicati si prevede siano consentite ai sensi degli artt. 23 e 24 del Codice, relativi rispettivamente al consenso dell'interessato ed ai casi in cui è possibile procedere a trattamento a prescindere da detto consenso (art. 130, comma 3)⁴⁶.

Fatto salvo quanto previsto nel comma 1 dell'art. 130, inoltre, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni (art. 130, comma 4). L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui sopra, deve essere informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

E' vietato, in ogni caso, l'invio di comunicazioni per le finalità di cui al comma 1 dell'art. 130 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'art. 7 del Codice⁴⁷ (art. 130, comma 5).

Infine, in caso di *reiterata violazione* delle disposizioni di cui all'articolo in

⁴⁶ V. cap. II, par. 7.

⁴⁷ Sui diritti di cui all'art. 7 del Codice, v. cap. II, par. 4.

In ordine alla questione se l'invio di una prima e-mail contenente la mera richiesta di consenso all'invio di successive comunicazioni commerciali via posta elettronica possa ritenersi ricompreso nell'ambito di applicazione dell'art. 130 del Codice, e quindi vietato, si rimanda a quanto si dirà nel capitolo V, par. 4.

esame, il Garante può⁴⁸ prescrivere a *fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono state inviate le comunicazioni* (art. 130, comma 6).

Il Codice della privacy stabilisce dunque che, a tutela degli interessati, il Garante possa imporre agli stessi *provider* l'obbligo di adottare le necessarie misure contro gli *spammer*, sebbene soltanto in presenza di "reiterate violazioni".

11.5. Codice di deontologia e di buona condotta per il marketing diretto

L'art. 140 del Codice della privacy, collocato nel titolo XIII della parte II, attribuisce al Garante per la protezione dei dati personali il compito di promuovere⁴⁹ *la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato⁵⁰, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.*

Come in più occasioni sottolineato, il rispetto delle disposizioni di un siffatto codice costituirà, quando emanato, condizione essenziale per la liceità e la

⁴⁸ Provvedendo ai sensi dell'art. 143, comma 1, lett. b), del Codice (v. cap. V).

⁴⁹ Ai sensi dell'art. 12 del testo unico, sul quale v. cap. II, par. 5.

⁵⁰ Nell'ambito di applicazione del testo unico, quali sono oggi i casi in cui il trattamento dei dati a fini di marketing diretto *non* presuppone necessariamente il consenso dell'interessato? Si tratta delle ipotesi di cui ai commi 3 e 4 dell'art. 130, sopra esaminati.

correttezza del trattamento dei dati personali (art. 12, comma 4)⁵¹.

11.6. Altre norme rilevanti in materia di spamming

Come sopra visto, l'ambito di applicazione dell'art. 130 del Codice della privacy è circoscritto all'invio di materiale pubblicitario o di vendita diretta o al compimento di ricerche di mercato o di comunicazione commerciale in relazione al trattamento di dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni (art. 121).

Al di fuori del campo di applicazione dell'art. 130 – ad esempio nel caso di invio di comunicazioni di propaganda politica o di proselitismo religioso o nel caso di invio di materiale per posta – troveranno dunque applicazione le disposizioni generali della parte I del Codice per quanto concerne, in particolare, il consenso dell'interessato (art. 23) ed i casi in cui il trattamento dei dati può essere effettuato a prescindere da detto consenso (art. 24)⁵². Tali ultime norme sono richiamate

⁵¹ Si ricorda il *Codice Europeo di Condotta e di Autodisciplina per l'Uso dei Dati Personali nelle Attività di Direct Marketing* (FEDMA), il cui testo può essere consultato su www.privacy.it all'indirizzo www.privacy.it/fedmacodeont.html. Nello stesso sito, si veda inoltre il parere 3/2003 *sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto* espresso dal Gruppo europeo per la tutela delle persone con riguardo al trattamento dei dati personali (www.privacy.it/grupripareri200303.html).

⁵² “Con un provvedimento generale l'Autorità garante (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan) ha indicato a partiti, organismi politici, sostenitori di liste e candidati i principi e i criteri per raccogliere ed utilizzare correttamente i dati personali dei cittadini che intendono contattare a fini di comunicazione e propaganda elettorale.

La comunicazione elettorale, che costituisce un momento particolarmente significativo della partecipazione alla vita democratica, deve infatti tener conto dei diritti e delle libertà fondamentali delle persone.

Alla luce delle novità introdotte dal Codice in materia di protezione dei dati personale, entrato in vigore il 1 gennaio 2004, il Garante ha fornito precise indicazioni alle quali partiti e candidati devono attenersi.

Dati tratti da elenchi pubblici come liste elettorali ed elenchi telefonici

Chi effettua propaganda elettorale tramite posta ordinaria, può farlo, senza consenso, solo se utilizza dati estratti da fonti 'pubbliche', cioè registri, elenchi, atti, documenti conoscibili da chiunque.

Deve però informare i cittadini sull'uso che verrà fatto dei loro dati personali.

Sono fonti pubbliche le liste degli aventi diritto al voto detenute dai Comuni, le liste degli elettori italiani residenti all'estero, gli elenchi dei telefoni fissi, così pure gli elenchi degli iscritti ad albi e collegi professionali e alcuni registri delle Camere di commercio.

Se la comunicazione elettorale è telefonica e il numero è tratto da un elenco pubblico l'operatore deve specificare all'inizio della telefonata chi sta chiamando, perché e quali diritti ha la persona che risponde.

E' comunque illecito effettuare propaganda elettorale telefonica, senza consenso specifico dell'abbonato, quando si usano sistemi automatizzati che effettuano chiamate vocali preregistrate.

Dati non pubblici: necessario il consenso dell'interessato

Chi effettua propaganda elettorale tramite fax, telefono cellulare, e-mail ha l'obbligo di dare l'informativa ai cittadini e acquisirne il consenso prima di qualsiasi comunicazione.

L'uso dei numeri dei cellulari per l'invio di messaggi Sms e Mms è vietato senza il consenso preventivo e informato dell'abbonato o del reale utilizzatore della scheda prepagata.

Allo stesso regime sottostanno gli indirizzi e-mail i quali, come sottolineato più volte dal Garante, non rientrano tra le fonti pubbliche utilizzabili liberamente ma recano dati personali da trattare nel rispetto della normativa sulla privacy.

E' quindi illecito il loro uso senza consenso preventivo dell'abbonato, indipendentemente dalle modalità del reperimento degli indirizzi di posta elettronica in Internet (forum, newsgroup, software automatici).

Il consenso deve essere specifico e manifestato liberamente, non è sufficiente un consenso generico, espresso magari per scopi di tipo commerciale.

Il candidato o l'organismo politico che acquisisce dati da un privato ha l'onere di verificare che gli interessati siano stati informati in modo specifico e abbiano espresso il loro consenso.

La violazione di questi principi rende illecito il trattamento e inutilizzabili i dati.

Dati che non si possono utilizzare

In nessun caso possono essere usate le liste elettorali di sezione già utilizzate nei seggi e sulle quali sono stati annotati dati relativi alle persone che hanno votato.

E' illecita la compilazione da parte di scrutatori e rappresentanti di lista di elenchi di persone che si sono astenute dal voto.

I titolari di cariche elettive, politiche e amministrative, che nell'esercizio del loro mandato hanno potuto accedere a dati personali, non possono usare tali informazioni a fini di propaganda elettorale.

espressamente dallo stesso art. 130, comma 3, in relazione alle comunicazioni commerciali effettuate con mezzi diversi da quelli indicati – con ampia definizione – dal primo comma della disposizione.

Con riguardo ad alcune questioni applicative relative agli artt. 23 e 24 del Codice in materia di spamming si rimanda a quanto si dirà nel paragrafo successivo a proposito del provvedimento generale sullo spamming adottato dal Garante per la protezione dei dati personali nel maggio 2003.

Occorre ora invece accennare ad altre disposizioni rilevanti in materia.

I Comuni non possono fornire ai privati elenchi degli iscritti nelle anagrafi della popolazione, anche se il richiedente è un amministratore locale o il titolare di una carica elettiva.

E' illecita la prassi di utilizzare indirizzi di iscritti ad associazioni no-profit, sportive, di categoria a fini di propaganda elettorale senza consenso degli interessati, anche per sostenere candidati interni.

Temporanea sospensione dell'informativa ai cittadini

Quando i partiti politici e i candidati impegnati nelle prossime consultazioni elettorali inviano solo materiale propagandistico di dimensioni ridotte (i cosiddetti "santini"), fino al 30 giugno 2004 non saranno tenuti all'informativa, purché utilizzino dati estratti da pubblici registri, elenchi, atti conoscibili da chiunque e solo per finalità elettorali.

In questo caso, i partiti politici e candidati potranno conservare questi dati solo se informeranno, anche in modo semplice e sintetico, tutti gli interessati entro il 30 settembre 2004.

Altrimenti entro tale termine dovranno distruggere i dati.

Garanzie per i cittadini

Il cittadino può opporsi all'ulteriore invio di materiale elettorale anche se in precedenza si era dichiarato disponibile a riceverlo.

Se nei casi previsti il cittadino non è chiamato a esprimere il consenso o non ricevere l'informativa può avvalersi delle tutele previste dal Codice sulla privacy e chiedere al partito o al candidato di avere accesso ai dati personali che lo riguardano.

Se partiti o candidati non forniscono un riscontro idoneo il cittadino può rivolgersi all'autorità giudiziaria o presentare un reclamo o un ricorso al Garante.

Partiti, movimenti o comitati elettorali devono adottare idonee misure di sicurezza per la salvaguardia dei dati dei cittadini" (Garante per la protezione dei dati personali, comunicato stampa del 13 febbraio 2004).

In *rapporto di specialità* con le disposizioni del Codice della privacy dovrebbe infatti continuare a porsi l'art. 10 del [D.L.vo 185/1999](#) relativo ai *contratti a distanza conclusi dai consumatori*⁵³.

Per *contratto a distanza* deve intendersi, secondo la definizione fornita dall'art. 1, lett. a), del D.L.vo 185/1999, “il contratto avente per oggetto beni o servizi stipulato tra un fornitore e un consumatore nell'ambito di un sistema di vendita o di prestazione di servizi a distanza organizzato dal fornitore che, per tale contratto, impiega esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto, compresa la conclusione del contratto stesso”.

Ai sensi dell'art. 1, lett. b), D.L.vo 185/1999, *consumatore* è la *persona fisica* che in relazione ai contratti a distanza agisce per *scopi non riferibili all'attività professionale eventualmente svolta*. Per *fornitore* deve intendersi invece, secondo la definizione fornita dall'art. 1, lett. c), del provvedimento, la *persona fisica o giuridica* che nei contratti a distanza agisce *nel quadro della sua attività professionale*.

Entro tale ambito di applicazione, l'art. 10 del D.L.vo 185/1999 (“Limiti all'impiego di talune tecniche di comunicazione a distanza”) dispone dunque che l'impiego da parte di un fornitore del *telefono*, della *posta elettronica*, di *sistemi automatizzati di chiamata* senza l'intervento di un operatore o di *fax*, richiede il *consenso preventivo del consumatore*.

⁵³ 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 (consultabile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/dlvo185-1999.htm).

In argomento si veda G. Briganti, *Spamming e diritto* cit. ed autori ivi citati. Sul D.L.vo 185/1999, v. *La disciplina del commercio elettronico e delle altre forme di contrattazione a distanza. Commento al d.lg. 22 maggio 1999, n. 185*, a cura di M. Atelli, Torino, 2001; A. Fraternali, *I contratti a distanza*, Milano, 2002.

D'altra parte, si prevede che tecniche di comunicazione a distanza diverse da quelle di cui sopra, *qualora consentano una comunicazione individuale*, possano essere impiegate dal fornitore *se il consumatore non si dichiara esplicitamente contrario* ^(opt-out)⁵⁴.

L'art. 10 D.L.vo 185/1999 riguarda pertanto il *consumatore* quale parte di un *contratto a distanza* e, stante il summenzionato rapporto di specialità con le disposizioni del Codice della privacy, sarà esso a prevalere sul testo unico nel proprio ambito applicativo.

Restano invece fuori dal campo di applicazione della norma in esame le comunicazioni che avvengono nel c.d. B2B (*Business to Business*), poiché tali comunicazioni non coinvolgono appunto i consumatori, intesi come coloro che agiscono per scopi estranei ad attività imprenditoriale o professionale. Tali fattispecie saranno pertanto disciplinate dalle norme precedentemente analizzate.

⁵⁴ Si veda anche l'art. 10 ("Comunicazioni non richieste") della recente [direttiva 2002/65/CE](#) del 23 settembre 2002, *concernente la commercializzazione a distanza di servizi finanziari ai consumatori e che modifica la direttiva 90/619/CEE del Consiglio e le direttive 97/7/CE e 98/27/CE*, GUCE L 271 del 9 ottobre 2002 (disponibile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/direttiva2002-65-ce.htm), secondo cui:

"1. L'utilizzazione da parte di un fornitore delle seguenti tecniche di comunicazione a distanza richiede il previo consenso del consumatore:

a) sistemi automatizzati di chiamata senza intervento di un operatore (dispositivo automatico di chiamata);

b) fax (telecopia).

2. Gli Stati membri adottano le misure appropriate affinché le tecniche di comunicazione a distanza diverse da quelle indicate al paragrafo 1, quando consentono una comunicazione individuale:

a) non siano autorizzate se non è stato ottenuto il consenso del consumatore interessato; o

b) possano essere utilizzate solo in assenza di una manifesta opposizione del consumatore.

3. Le misure di cui ai paragrafi 1 e 2 non comportano costi per i consumatori".

La violazione dell'art. 10 del D.L.vo 185/1999 comporta l'applicazione delle sanzioni di cui all'art. 12 del medesimo provvedimento⁵⁵.

Un cenno merita infine l'art. 660 cod. pen. ("Molestia o disturbo alle persone") il quale punisce chiunque, in un luogo pubblico o aperto al pubblico, ovvero *col mezzo del telefono*, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo.

Secondo alcuni tale reato potrebbe perfezionarsi anche tramite l'*invio di messaggi di posta elettronica*. Deve però osservarsi che il principio di tassatività vigente in materia penale non consente alcuna interpretazione estensiva della fattispecie con riguardo al mezzo del telefono ivi contemplato⁵⁶.

[Sommaro](#)

12. Segue: il provvedimento generale sullo spamming del Garante per la protezione dei dati personali

In data 29 maggio 2003, anteriormente dunque alla pubblicazione sulla Gazzetta ufficiale del Codice della privacy, il Garante per la protezione dei dati personali è intervenuto in materia di *spamming effettuato tramite posta elettronica* con un *provvedimento di carattere generale*⁵⁷.

⁵⁵ Sulle quali si rimanda a quanto si dirà nel capitolo V.

⁵⁶ Si veda D. Minotti, *I reati commessi mediante Internet*, in *INTERNET. Nuovi problemi e questioni controverse*, a cura di G. Cassano, Milano, Giuffrè, 2001, p. 472 s.

Con riguardo allo spamming effettuato su *newsgroup* e *mailing list* v. G. Sisto, *La sollecitazione commerciale nell'e-commerce. Il problema dello spamming* cit., p. 177.

⁵⁷ Il testo del provvedimento generale è consultabile sul sito del Garante all'indirizzo www.garanteprivacy.it/garante/document?ID=272587. In data 2 dicembre 2003 sullo stesso sito è

Il provvedimento, pur non avendo, naturalmente, portata normativa, può costituire un utile riferimento per l'interprete, sebbene emanato nella vigenza della precedente disciplina. Il pensiero ivi espresso dall'Autorità non è d'altra parte certamente esente da critiche, soprattutto, come si vedrà, in merito alla rilevanza penale della condotta consistente nell'invio di e-mail indesiderate di carattere commerciale.

Secondo l'Autorità, l'intervento si è reso necessario a seguito di “diverse centinaia di reclami e segnalazioni da parte di utenti di reti telematiche e di associazioni per la tutela dei diritti di utenti e consumatori, che contestano la ricezione di messaggi di posta elettronica per scopi promozionali, pubblicitari, di informazione commerciale o di vendita diretta, inviati senza che gli interessati abbiano manifestato in precedenza il proprio consenso informato”.

Il Garante rileva inoltre che “Numerosi interessati espongono anche ulteriori disagi derivanti dalla costante ripetizione di analoghi messaggi da parte di uno stesso mittente titolare del trattamento, dai vani tentativi esperiti per ottenere sia la cancellazione del proprio indirizzo di posta elettronica presso i mittenti, sia l'interruzione di altri messaggi. Altre segnalazioni riguardano gli inconvenienti che derivano dalla ricezione di e-mail anonime o prive dell'indicazione di un indirizzo, oppure delle coordinate veritiere di un reale mittente”.

“Nella prevalenza dei casi” – prosegue il provvedimento – “agli interessati non è stato previamente richiesto, come dovuto, uno specifico consenso preceduto da un'idonea informativa che illustri adeguatamente le modalità e le caratteristiche dei messaggi.

In altri casi i messaggi sono inviati da imprese – anche in questo caso senza

stata inoltre pubblicata una “scheda informativa” sullo spamming raggiungibile all'indirizzo www.garanteprivacy.it/garante/doc.jsp?ID=432448.

consenso – per promuovere, presso clienti, prodotti o servizi analoghi a quelli forniti in un rapporto contrattuale, oppure per offrire altri tipi di prodotti o servizi distribuiti anche da terzi”.

Con il provvedimento generale in esame l’Autorità ha inteso dunque, con riferimento al quadro giuridico previgente, “indicare le misure che gli operatori del settore devono adottare al fine di conformarsi alla disciplina generale sull’uso dei dati personali, specie nel settore delle comunicazioni (in particolare, alla legge 31 dicembre 1996, n. 675, al decreto legislativo 13 maggio 1998, n. 171 e al decreto legislativo 22 maggio 1999, n. 185)”⁵⁸.

Invio lecito di posta elettronica pubblicitaria.

Come può leggersi nel provvedimento del Garante, “Gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia”⁵⁹.

La loro utilizzazione per *scopi promozionali e pubblicitari*, prosegue dunque il Garante, è possibile *solo se il soggetto cui si riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato*.

Il consenso, rileva l’Autorità, è necessario anche quando gli indirizzi sono *formati*

⁵⁸ I provvedimenti emanati dal Garante in materia di spamming in relazione a casi specifici sono consultabili sul sito dell’Autorità, all’indirizzo www.garanteprivacy.it. Si veda anche www.iusreporter.it/Testi/osservaspmming.htm.

⁵⁹ Art. 1, comma 2, lett. c), L. 675/1996; cfr., oggi, art. 4, comma 1, lett. b), del Codice della privacy (cap. II, par. 2).

In passato, era stato da alcuni posto in discussione che l’indirizzo e-mail fosse idoneo a ricadere nella nozione di “dato personale” accolta dalla normativa sulla privacy. Si veda in proposito A. Monti, *Spam e indirizzi e-mail. Quando la 675 è impotente*, in *InterLex*, www.interlex.it, www.interlex.it/675/amonti44.htm; G. Sisto, *La sollecitazione commerciale nell’e-commerce. Il problema dello spamming* cit., p. 175 e s.

ed utilizzati automaticamente con un software senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

“Questo assetto, basato su una scelta dell'interessato c.d. di *opt-in*, è stato ribadito nel 1998 (con il d.lg. n. 171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea (n. 2002/58/CE in fase di recepimento in Italia, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002)”.

In più di un'occasione il Garante ha infatti avuto modo di ribadire che *la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari*⁶⁰.

In particolare, i dati dei singoli utenti che prendono parte a *gruppi di discussione* in Internet sono resi conoscibili in rete *per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico*⁶¹. Ad analoga conclusione, secondo il Garante, deve pervenirsi per gli indirizzi di posta elettronica compresi nella *lista “anagrafica” degli abbonati ad un Internet provider* (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure *pubblicati su siti web di soggetti pubblici per fini istituzionali*.

Tali considerazioni, prosegue l'Autorità, valgono anche con riferimento ai *messaggi pubblicitari inviati a gestori di siti web – anche di soggetti privati –*

⁶⁰ Cfr. provvedimento dell'11 gennaio 2001, in *Bollettino del Garante*, n. 16. In proposito, si veda G. Briganti, *Spamming e diritto cit.*; G. Briganti, *Spamming e privacy cit.*

⁶¹ Art. 9, comma 1, lett. a) e b), L. 675/1996; cfr., oggi, art. 11, comma 1, lett. a) e b) del Codice della privacy (cap. II, par. 5).

utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio. “In quest’ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n. 675) e non anche a rendere l’interessato disponibile all’invio di messaggi pubblicitari”⁶².

⁶² “I Garanti Ue indicano le regole per l’uso degli elenchi con i nomi dei responsabili dei domini web. Gli elenchi che contengono i nomi dei responsabili dei domini web non possono essere resi pubblici in maniera indiscriminata o resi accessibili a chiunque. L’utilizzazione di tali elenchi per finalità di marketing non è ammissibile.

I Garanti europei hanno adottato lo scorso 13 giugno un parere (2/2003) relativo ai problemi posti, in termini di protezione dati, dai cosiddetti ‘database Whois’, consultabili sulla Rete, che contengono le informazioni per contattare i responsabili dei domini o delle reti Internet.

I Garanti hanno indicato l’inopportunità di rendere indiscriminatamente pubblici ed accessibili a chiunque i dati contenuti in tali elenchi, e la necessità di distinguere fra dati assolutamente necessari e dati opzionali.

Inoltre, l’utilizzazione massiva di tali registri o elenchi per finalità di marketing non è ammissibile alla luce della direttiva europea sulla protezione dei dati personali (Direttiva 95/46/CE), in quanto non è conforme agli scopi per i quali essi sono stati istituiti.

Gli elenchi consultabili attraverso i servizi Whois contengono dati personali relativi, in particolare, alla persona da contattare in caso di problemi con i servizi forniti nell’ambito di un determinato dominio (spesso chi ha registrato il dominio oppure le figure tecniche preposte alle gestione dei servizi di rete): numero di telefono, indirizzo e-mail, altri dati personali.

La finalità per cui questi elenchi sono stati costituiti, e vengono tuttora gestiti, da un ente denominato ICANN (*International Corporation for Assigned Names and Numbers*) è chiaramente di tipo tecnico.

Negli ultimi anni si sono verificati però numerosi casi di utilizzazione impropria di tali dati, soprattutto per finalità di marketing, anche perché alcuni soggetti ai quali ICANN ha delegato l’assegnazione di nomi di dominio e la tenuta di registri ‘regionali’ hanno ritenuto di poter mettere in vendita tali registri al migliore offerente (v. sul punto Newsletter 18-24 giugno 2001).

Dal 22 al 26 giugno si tiene a Montreal, in Canada, un’importante conferenza di ICANN che ha fra i propri obiettivi la definizione delle modalità di gestione di questi registri.

I Garanti europei hanno ritenuto opportuno segnalare ai partecipanti a tale Conferenza che i principi di protezione dati trovano applicazione anche in questo contesto e devono essere adeguatamente rispettati.

In tutti questi casi, “l’utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad

Queste le indicazioni dei Garanti: in primo luogo, i Garanti sottolineano come il fatto che dati personali siano accessibili al pubblico non significhi che essi siano sottratti alle garanzie previste dalla legislazione in materia di protezione dati.

Pertanto, gli interessati (titolari dei nomi di dominio e/o amministratori di sistema) conservano tutti i diritti previsti dalla normativa in materia.

E’ necessario che ICANN definisca chiaramente quali sono le finalità di Whois e quali attività sono compatibili con tali finalità.

Sinora l’apposita task force costituita da ICANN non è riuscita nell’intento.

In base alla direttiva europea (ed alle leggi nazionali di recepimento), i dati devono essere ‘pertinenti e non eccedenti’ rispetto alle finalità del trattamento.

E’ dunque necessario limitare la quantità dei dati personali inseriti nel registro, e soprattutto distinguere fra la registrazione di nomi di dominio effettuata da singoli e quella effettuata da imprese o altre persone giuridiche.

Nel primo caso, infatti, non è necessario che i dati personali (indirizzo, numero di telefono) utili per contattare il titolare del dominio siano resi pubblici.

I Garanti consigliano un approccio simile a quello adottato in alcuni Paesi europei (ad esempio, in Francia attraverso l’AFNIC – *Association Française pour le Nommage d’Internet en Coopération*): i dati personali del titolare sono noti ai fornitori dei servizi di registrazione, che provvedono eventualmente a contattarlo qualora insorgano problemi relativamente al sito.

Il principio di proporzionalità impone, inoltre, di limitare l’accesso ai dati disponibili nel registro senza renderli indiscriminatamente di dominio pubblico.

Si può pensare, dunque, a meccanismi di filtro da inserire nelle interfacce con le quali si accede ai singoli registri Whois.

L’utilizzazione dei dati contenuti nei registri Whois per scopi di marketing diretto non è compatibile con le finalità di tali registri; inoltre, anche in base alla direttiva 2002/58 in materia di privacy e comunicazioni elettroniche, l’utilizzazione di indirizzi di posta elettronica (presenti nei registri Whois) per fini di marketing diretto deve basarsi sul previo consenso espresso dell’interessato (opt-in)” (Garante per la protezione dei dati personali, *Newsletter* n. 175 del 16-22 giugno 2003, www.garanteprivacy.it).

adottare ‘filtri’, a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico.

Il fenomeno interessa anche piccole e grandi imprese destinatarie di un elevato numero di messaggi, le quali devono farsi carico di misure interne e di costi anche organizzativi per contrastarlo.

Questo ingiustificato riversamento sugli utenti dei costi pubblicitari si verifica anche relativamente a messaggi inviati da singole persone fisiche che, in vari casi esaminati, non si limitano ad una comunicazione episodica, ma intraprendono una comunicazione sistematica per fini personali o, addirittura, una diffusione di dati cui è applicabile la disciplina in materia di protezione dei dati personali⁶³.

Il quadro giuridico su informativa e consenso.

Il Garante prosegue poi ricostruendo, secondo quella che è l’opinione dell’Autorità, il quadro giuridico su informativa e consenso in relazione allo spamming.

Innanzitutto, osserva il Garante, è la legge ad individuare il contenuto dell’informativa agli interessati, nonché i casi in cui è necessario il consenso espresso dell’interessato o è possibile prescindere⁶⁴.

Al riguardo, rileva nuovamente il Garante, non può farsi a meno del consenso ritenendo che i dati personali relativi all’indirizzo di posta elettronica – e all’indirizzo in particolare – siano “pubblici” in quanto conoscibili da chiunque.

⁶³ Art. 3 L. 675/1996; cfr., oggi, art. 5, comma 3, del Codice della privacy (cap. II, par. 3).

⁶⁴ Artt. 10, 11, 12 e 20 L. 675/1996; cfr., oggi, artt. 13, 23 e 24 del Codice della privacy (cap. II, parr. 5 e 7).

Le disposizioni normative che si riferiscono a questo aspetto sono infatti applicabili, prosegue l’Autorità con argomentazioni condivisibili, solo quando vi è un *pubblico registro, elenco, atto o documento conoscibile da chiunque perché vi è una specifica disciplina che ne impone la conoscibilità indifferenziata da parte del pubblico, e non anche quando i dati personali sono conoscibili da chiunque per mere circostanze di fatto* (si pensi, oltre ai casi già richiamati di raccolta su siti web o di messaggi trasmessi su newsgroup o su mailing list, *agli indirizzi di posta elettronica raccolti in rete tramite appositi software o mediante comuni motori di ricerca*)⁶⁵.

“Il principio del consenso è quindi già operante nel nostro ordinamento prima ancora di essere affermato senza eccezioni su scala europea, dalla menzionata direttiva n. 2002/58 in fase di recepimento, a tutta la posta elettronica comunque inviata per fini di commercializzazione diretta (si vedano in particolare l’art. 13 e il considerando n. 40)”.

Il quadro evidenziato, secondo il Garante, trova d’altra parte conferma nella disciplina sulla protezione dei consumatori nei contratti a distanza di cui al D.L.vo 185/1999 che, in riferimento al rapporto sottostante ai fini del quale si procede al trattamento di dati personali, vieta ai fornitori l’impiego della posta elettronica in mancanza del consenso preventivo del consumatore, *in relazione a determinati scopi tra i quali rientrano anche quelli pubblicitari*.

Il Garante omette però di considerare l’altra ipotesi di esclusione del consenso suscettibile di venire in rilievo con riguardo all’invio di e-mail indesiderate di carattere commerciale: quella concernente i “dati relativi allo svolgimento di attività economiche” di cui all’art. 12, comma 1, lett. f), dell’abrogata L.

⁶⁵ Cfr. art. 12, comma 1, lett. c), L. 675/1996 e la nuova formulazione della norma contenuta nell’art. 24, comma 1, lett. c), del Codice della privacy (cap. II, par. 7).

675/1996⁶⁶.

Afferma inoltre l’Autorità che “per gli aspetti relativi alla protezione dei dati personali non devono essere peraltro considerate le disposizioni del recente decreto legislativo 9 aprile 2003, n. 70, sul commercio elettronico, dichiarate in proposito espressamente inapplicabili (art. 1, comma 2, lett. b) d.lg. n. 70 cit.)”.

D’altra parte, se è vero che il decreto legislativo di attuazione della direttiva europea sul commercio elettronico lascia espressamente impregiudicata la disciplina in materia di protezione dei dati personali, ciò però non può significare che le norme del D.L.vo 70/2003 non debbano trovare applicazione, con riferimento all’invio di comunicazioni commerciali, nell’ambito considerato dal suddetto provvedimento⁶⁷.

Il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell’inoltro dei messaggi⁶⁸.

Tale disciplina, afferma il Garante, non può essere elusa inviando una *prima e-mail che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario⁶⁹, oppure riconoscendo solo un diritto di tipo c.d. “opt-out” al fine di non ricevere più messaggi dello tesso tenore.*

“Al contrario, è opportuna e va incoraggiata la prassi di alcuni fornitori i quali,

⁶⁶ V. cap. II, par. 7; cap. V, par. 4.

⁶⁷ Sul quale si veda il capitolo IV.

⁶⁸ Art. 11 L. 675/1996; cfr., oggi, art. 23 del Codice della privacy (cap. II, par. 7).

⁶⁹ La precisazione del Garante riguarda dunque solo i casi in cui alla prima e-mail possa essere comunque riconosciuto un *contenuto promozionale oppure pubblicitario*. Si veda in proposito quanto si dirà, con riferimento all’attuale disciplina, nel cap. V, par. 4.

dopo aver ottenuto realmente un valido consenso dei destinatari, danno semplice conferma della sua manifestazione, attraverso un messaggio volto unicamente ad annunciare il successivo inoltro di materiale pubblicitario. Tale prassi, se utilizzata correttamente, consente tra l'altro di verificare l'effettiva corrispondenza dell'indirizzo di posta elettronica ai soggetti che avevano espresso il consenso, nonché di accertare il permanere di tale volontà”.

Sulla base delle premesse illustrate, l'Autorità conclude affermando che l'insieme dei diritti riconosciuti dalla legge agli utenti determina, in caso di loro violazione, un *trattamento illecito dei dati* che:

- è già *vietato direttamente dalla legge*, senza che sia necessario adottare uno specifico provvedimento interdittivo;
- determina, a seconda dei casi, l'applicazione di *sanzioni amministrative pecuniarie*, in particolare per omessa informativa od omessa notificazione⁷⁰;
- comporta il *rimborso delle spese e dei diritti* relativi al procedimento attivato da un fondato ricorso al Garante, oppure da un'azione dinanzi al giudice civile, come pure il *risarcimento dei danni*, specie di tipo patrimoniale, che derivino dai fatti illeciti e siano comprovati dall'interessato in relazione ai disagi sopra illustrati;
- rende applicabile anche una *sanzione penale* qualora il trattamento illecito dei dati sia effettuato *al fine di trarne per sé o per altri un profitto o per arrecare ad altri un danno*, con la pena accessoria della pubblicazione della sentenza di condanna.

Tale ultima conclusione tratta dal Garante ha suscitato notevoli perplessità in dottrina. Prima dell'entrata in vigore del Codice della Privacy – si è sostenuto

⁷⁰ Sulle sanzioni si veda il capitolo V.

infatti con argomentazioni in larga parte condivisibili – con riferimento all’invio di e-mail indesiderate di carattere commerciale doveva ritenersi operante l’ipotesi di esclusione del consenso di cui all’art. 12, comma 1, lett. f), L. 675/1996, concernente, come si è visto, il trattamento di dati relativi allo svolgimento di attività economiche. Ipotesi di esclusione del consenso che l’Autorità ha però omesso, come già rilevato, di considerare nel provvedimento in parola.

Conseguentemente, “Tale riscontro, in uno con l’introduzione nel novello d.l.vo 196/03 di una specifica disciplina in materia di comunicazioni indesiderate basata sul principio del consenso preventivo (cfr., art. 130), consentono di affermare che solo a partire dal 1° gennaio 2004 nel nostro ordinamento troverà applicazione in materia di ‘spamming’ il c.d. principio dell’*opt-in* la cui violazione integrerà per espressa previsione legislativa responsabilità penali” (C. Blengino e M.A. Senior)⁷¹.

Messaggi pubblicitari a propri clienti.

Afferma il Garante, con riferimento alla disciplina anteriore al Codice della privacy, che “Per effetto del recepimento della direttiva 2002/58/CE sarà peraltro possibile integrare, nel prossimo futuro, la disciplina sopra illustrata, permettendo a talune società di far conoscere a propri clienti prodotti o servizi analoghi a quelli per i quali si è già stabilito un rapporto, con i medesimi clienti, di vendita di prodotti o servizi”.

In tali casi, “la società titolare del trattamento (dopo aver informato

⁷¹ C. Blengino e M.A. Senior, *Lo spamming a fini di profitto non costituisce reato*, in *Penale.it*, www.penale.it, www.penale.it/commenti/blengino_senor_01.htm; v. anche L. Pulito, *Spamming: profili penali e prospettive future*, in *La pratica forense*, www.lapraticaforense.it, www.lapraticaforense.it/articolo.php?idart=223.

Per il reato di “spamming” secondo la disciplina introdotta dal Codice della privacy, v. cap. V, parr. 3.2 e 4.

preventivamente e adeguatamente il cliente) potrà procedere all'invio del messaggio pubblicitario, offrendo però al cliente, in modo chiaro e distinto (sia al momento della raccolta dei suoi dati, sia in occasione di ciascun messaggio) il diritto di rifiutare sin dall'inizio tale uso dei dati o di obiettare, gratuitamente e in maniera agevole, anche successivamente (art. 13, par. 2, direttiva n. 2002/58/CE cit.)⁷².

Messaggi per conto terzi e acquisto di banche dati.

In alcuni casi portati all'attenzione del Garante, *l'invio di messaggi pubblicitari era stato effettuato, per conto di terzi committenti, da società specializzate che utilizzano indirizzi di posta elettronica contenuti in proprie banche dati.*

Tali società, da considerarsi *titolari* o *contitolari* del trattamento dei dati a seconda del rapporto che si instaura con il committente e delle modalità di concreta utilizzazione dei dati, sono, secondo il Garante, *tenute a rispettare le disposizioni in tema di informativa e specifico consenso, anche per quanto riguarda l'eventuale comunicazione di dati personali ai committenti medesimi e le relative finalità.*

Ciò comporta un quadro di obblighi e possibili responsabilità anche penali che gli operatori devono verificare con attenzione, anche quando la società specializzata incaricata sia stabilita fuori dell'Unione europea.

Dall'esame dei reclami e delle segnalazioni pervenuti al Garante è risultato, altresì, che alcuni dei soggetti che hanno utilizzato la posta elettronica per l'invio di messaggi pubblicitari *avevano acquisito da terzi le banche dati contenenti gli indirizzi dei destinatari.* In questi casi, secondo l'Autorità, *chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito alla*

⁷² Cfr. art. 130, comma 4, Codice privacy (par. 11.4).

comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario; al momento in cui registra i dati deve poi inviare in ogni caso, a tutti gli interessati, un messaggio di informativa che precisi gli elementi indicati oggi nell'art. 13 del Codice della privacy⁷³, comprensivi di un riferimento di luogo – e non solo di posta elettronica – presso cui l'interessato possa esercitare i diritti riconosciuti dalla legge.

Diritti degli interessati.

Si legge nel provvedimento del Garante in esame che “Indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi, chi detiene i dati deve assicurare in ogni caso agli interessati la possibilità di far valere in ogni momento i diritti riconosciuti dalla legge, i quali sono spesso esercitati per conoscere da quale fonte sono stati tratti i dati, o per far interrompere gratuitamente la loro ulteriore utilizzazione ai fini commerciali-pubblicitari, oppure per far cancellare i dati trattati in violazione di legge”⁷⁴.

I diritti vanno esercitati direttamente presso l'indirizzo conoscibile del titolare o del responsabile del trattamento, riservando solo ad un eventuale momento successivo l'instaurazione di una procedura contenziosa dinanzi al Garante o all'autorità giudiziaria.

“Anche ai fini dell'esercizio di tali diritti, deve ritenersi che l'invio anonimo di messaggi pubblicitari senza l'indicazione di un mittente identificabile concreti già

⁷³ Sul quale v. cap. II, par. 5.

⁷⁴ Art. 13, comma 1, lett. e), L. 675/1996; cfr., oggi, art. 7 del Codice della privacy (cap. II, par. 4).

Nel sito Internet del Garante (www.garanteprivacy.it) è riportato un modello-tipo per esercitare tali diritti in maniera agevole, gratuitamente e senza particolari formalità, anche verbalmente o mediante posta elettronica, dimostrando la propria identità. Tale modello, sottolinea il Garante, è utilizzabile in luogo di altri reperibili in reti telematiche che non sono pienamente validi in quanto si riferiscono anche ad aspetti non riconosciuti dalla normativa sulla privacy.

oggi un trattamento illecito di dati personali, a prescindere da quanto dispone il citato d.lg. n. 70/2003 sul commercio elettronico (come si è visto, fuori della materia della protezione dei dati personali) e da quanto, in riferimento ai dati personali, sarà previsto con il recepimento della direttiva n. 2002/58/CE (la quale non consente l'invio di messaggi pubblicitari quando l'identità del mittente viene camuffata o addirittura celata e quando non viene fornito un indirizzo valido che consenta al destinatario di richiedere la cessazione delle comunicazioni: art. 13, par. 4, dir. cit.)”⁷⁵.

Elenchi di possibili destinatari.

L'eventuale elenco predisposto da operatori, contenente i nominativi dei soggetti che non hanno manifestato il consenso o che lo hanno revocato (c.d. *black list*) non può essere utilizzato – secondo il parere espresso in proposito dal Garante – per porre a carico degli interessati, anche indirettamente, un *onere di iscrizione nell'elenco medesimo*.

Come si è illustrato, infatti, il consenso ha un connotato autorizzatorio “positivo” in base al quale *l'eventuale silenzio dell'interessato comporta il diniego del consenso eventualmente richiesto e non rileva come assenso tacito all'invio dei messaggi*.

Consta peraltro, rileva il Garante, che alcuni operatori intendono adottare la diversa prassi di redigere anche tramite siti web *appositi elenchi di persone che hanno manifestato il consenso, distinti in base alle diverse categorie di messaggi commerciali-pubblicitari che gli interessati hanno acconsentito a ricevere*.

Tale prassi, nell'opinione dell'Autorità, se correttamente seguita, può

⁷⁵ Si veda in proposito quanto sopra detto con riferimento al vigente art. 130 del Codice della privacy e quanto si dirà nel capitolo successivo in materia di commercio elettronico.

rappresentare una misura utile, sul piano organizzativo, per garantire un più effettivo rispetto della volontà espressa dai singoli. A tale riguardo, costituirà una pratica utile quella di *garantire agli interessati la possibilità di inserire direttamente il proprio nome nelle diverse liste o di cancellarlo dalle stesse, magari attraverso un'apposita pagina web, ferma restando l'esigenza di identificarli.*

E-mail provenienti dall'estero.

Ad alcuni messaggi, in quanto provenienti dall'estero, *non* è applicabile la legge italiana sulla protezione dei dati personali.

Ciò, d'altra parte, sottolinea il Garante, non comporta l'assoluta mancanza di rimedi o tutela, *potendo l'utente chiedere una verifica da parte della competente autorità nazionale di protezione dei dati personali, ove istituita nel Paese eventualmente individuabile dal messaggio*⁷⁶.

In altri casi, come quelli relativi alle leggi degli *stati federali*, l'invio di messaggi pubblicitari di posta elettronica può essere illecito in base alla legge di alcuni stati, per cui è parimenti possibile, per gli utenti, chiedere alle *competenti autorità pubbliche degli stati di valutare la perseguibilità degli illeciti.*

Va infine tenuto presente che alcune e-mail indesiderate possono essere lo strumento per commettere *reati comuni* (ad esempio di truffa) *che devono considerarsi commessi nel territorio italiano quando, sebbene l'azione è avvenuta*

⁷⁶ Per un elenco delle Autorità nazionali preposte alla protezione dei dati personali si veda http://europa.eu.int/comm/internal_market/privacy/links_en.htm.

Per informazioni sulla disciplina anti-spam vigente nei vari Paesi, v. altresì www.spamlaws.com. Si ricorda che negli Stati Uniti è stato recentemente emanato il *CAN-SPAM Act of 2003* (www.spamlaws.com/federal/108s877.html).

*all'estero, l'evento-reato che ne deriva si è verificato in Italia*⁷⁷.

Sommario

13. Segue: le regole della Netiquette, l'attività della Naming Authority italiana; iniziative e responsabilità dei provider

Com'è noto, la *Netiquette* è costituita dai “principi di buon comportamento” (galateo) e dalle “tradizioni” sviluppatasi spontaneamente nel corso degli anni fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, ed in particolare fra i lettori dei servizi di news Usenet⁷⁸.

Le regole di Netiquette stabiliscono il divieto di inviare tramite posta elettronica *messaggi pubblicitari* o comunque *comunicazioni che non siano state sollecitate* in modo esplicito. A tale norma va attribuito carattere *consuetudinario*⁷⁹.

Deve inoltre essere rilevato che la Registration Authority (RA) italiana, vale a dire il soggetto che presiede all'assegnazione dei nomi a dominio con suffisso “.it”, richiama espressamente la Netiquette nel momento in cui assegna in concessione un nome a dominio, elevando così le regole di Netiquette al rango di *norme contrattuali*⁸⁰.

La Naming Authority italiana (NA), ossia il soggetto che stabilisce le regole in

⁷⁷ Artt. 4 e ss. cod. pen.

⁷⁸ Le regole di Netiquette sono consultabili all'indirizzo www.nic.it/NA/netiquette.txt.

⁷⁹ Cfr. L.M. De Grazia, *Spamming: definizioni ed aspetti legali*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/de_grazia1.html.

⁸⁰ Si veda in proposito De Grazia, *op. cit.* Il sito della RA è raggiungibile all'indirizzo www.nic.it/RA.

base alle quali la RA opera, al fine di assicurare l'applicazione di dette norme, pubblica e cura una *lista* nella quale sono presenti tutte le segnalazioni di presunte violazioni della Netiquette inviate dagli utenti della rete⁸¹.

La *mailing list abuse@na.nic.it* contiene i *servizi controllo abusi dei provider* che intendono efficacemente combattere gli abusi da parte dei propri clienti, ed è quindi il metodo più semplice per raggiungerli, nonché per segnalare chi sta eseguendo la violazione. La pubblicazione della segnalazione nella lista *Abuse* avviene comunque senza attendere eventuali controdeduzioni del presunto *spammer*⁸².

Si ricorda inoltre che è attivo il *newsgroup it.news.net-abuse* nel cui “manifesto” si legge che questo gruppo, “sorto per similitudine ai gruppi mondiali dello stesso nome, serve a riportare notizia di abuso della rete (come gli spam) proveniente da siti *italiani*. È inutile riportare abusi da siti esteri: in questo caso è meglio utilizzare i gruppi *news.admin.net-abuse.** per avere qualche speranza di risposta”⁸³.

Va osservato che alcuni provider hanno preso iniziative al fine di tutelare i loro utenti dalla ricezione di e-mail indesiderate.

⁸¹ La lista è pubblicata all'indirizzo <http://listserv.nic.it/RA/servizi/listserv/abuse.html>. Il sito della NA è raggiungibile all'indirizzo www.nic.it/NA.

⁸² Le violazioni della Netiquette che riguardano *Mail Spamming* o *Unsolicited E-Mail* possono essere segnalate alla Naming Authority ed alla Registration Authority italiane inviando una mail a ABUSE@NA.nic.it. Una copia per conoscenza del messaggio dovrà essere inviata anche all'indirizzo info@nic.it.

Nella segnalazione deve essere incluso il *full header* della mail pervenuta nonché quelle parti del testo del messaggio utili ai fini dell'identificazione del *vero* mittente (indirizzi e-mail, numeri di telefono, fax, indirizzi postali ecc.).

Giova ricordare in proposito che spesso lo spammer usa una tecnica, detta *spoofing*, per mezzo della quale riesce a mascherare la reale provenienza del messaggio, “appoggiandosi” ad un indirizzo e-mail di un terzo o addirittura ad un indirizzo inesistente.

⁸³ Per accedere al newsgroup via Web: <http://groups.google.it/groups?q=it.news.net-abuse>.

La protezione si realizza tramite *filtri anti spamming*, vale a dire appositi *software* che respingono determinati messaggi di posta elettronica precedentemente classificati come indesiderati in base alla loro provenienza da domini “sospetti”. Di solito ciò avviene su segnalazione degli utenti, e dopo aver verificato l’inclusione dello spammer segnalato nella lista tenuta dalla Naming Authority.

Questo meccanismo appare però in contrasto con l’art. 15 della Costituzione italiana, il quale sancisce *l’inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione*. Secondo detta norma, limitazioni possono aversi soltanto per atto motivato dell’autorità giudiziaria, con le garanzie stabilite dalla legge.

Come da alcuni rilevato, l’attivazione del filtro anti spamming avviene infatti spesso all’insaputa degli utenti del provider. Questi possono così perdere messaggi di posta elettronica, magari desiderati, senza rendersene conto, considerato anche che al mittente non viene inviata alcuna comunicazione di mancata trasmissione⁸⁴.

Inoltre, deve considerarsi anche l’art. 616 cod. pen., il quale, nel prevedere il reato di “Violazione, sottrazione e soppressione di corrispondenza”, punisce la condotta di chi distrugge o sopprime corrispondenza anche telematica⁸⁵.

Spesso sono d’altra parte gli stessi contratti di fornitura di accesso alla rete a

⁸⁴ Per questi rilievi si veda F. Iperti e M.P. Berlingieri, *Spamming – Che passione*, in *Newlaw.it*, [www.newLaw.it](http://www.newlaw.it), www.newLaw.it/marketing_privacy_spamming.htm.

⁸⁵ V. A. Lisi, *Tutela della privacy in Internet* cit., pp. 66 e ss. (e autori ivi citati), il quale afferma: “Appare condivisibile, quindi, il ragionamento della dottrina più recente, secondo la quale non ha nessuna rilevanza il grado di sicurezza insito nel tipo di comunicazione che si intende effettuare ai fini della tutela costituzionale, civile e penale della segretezza della comunicazione, ma è essenziale la volontà di inviare un messaggio riservato, e cioè la persuasione e l’affidamento del mittente di utilizzare un sistema di corrispondenza, che nel suo normale svolgimento, assicuri livelli medi di segretezza”.

prevedere un'apposita clausola che stabilisce il divieto di utilizzare le macchine del provider per la diffusione di *spam e-mail*, autorizzando espressamente il provider, in caso di violazione, a cancellare l'accesso alla rete dello spammer.

Interessante questione è infine quella della possibilità di configurare una *responsabilità in capo ai provider* rispetto allo spamming subito dai propri utenti.

La giurisprudenza di merito, con un provvedimento del 2001, anteriore dunque all'entrata in vigore sia del Codice della privacy che del D.L.vo 70/2003 di attuazione della direttiva europea sul commercio elettronico, ebbe occasione di affermare in proposito che, dovendosi riconoscere al contratto tra titolare di indirizzo di posta elettronica e provider natura giuridica di *appalto di servizi*, rientra tra i *doveri collaterali* gravanti sul provider anche quello di *evitare che il proprio utente di posta elettronica sia esposto a spamming effettuato da altri soggetti operanti nella rete*. Oltre a quanto previsto dall'autonomia contrattuale, la suddetta pronuncia vorrebbe dunque far discendere una *responsabilità contrattuale* del provider nei confronti dei propri utenti per violazione dei generali principi di cui agli artt. 1175 e 1375 cod. civ.⁸⁶.

[Sommaro](#)

14. Informazioni ad abbonati e utenti

⁸⁶ Tribunale di Prato, 15 ottobre 2001, *Dir. e prat. soc.* 2002, f. 13, 73, nota (Cassano, Cimino).

Si veda quanto si dirà nel cap. IV, parr. 8 e ss., in relazione alle vigenti regole sulla responsabilità dei provider introdotte dal D.L.vo 70/2003 di attuazione della direttiva europea sul commercio elettronico.

Per qualche consiglio pratico su come difendersi dallo spamming, si veda www.iusreporter.it/Testi/osservaspamming.htm#070103; A. Lisi, *Tutela della privacy in Internet* cit., p. 76 e s.

Proseguendo nell'analisi della normativa di attuazione della direttiva 2002/58/CE, secondo quanto disposto dall'art. 131 (“Informazioni ad abbonati e utenti”) del Codice della privacy⁸⁷, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico è tenuto ad *informare l'abbonato e, ove possibile, l'utente*⁸⁸ *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.*

L'abbonato è tenuto inoltre ad 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.

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

Viene pertanto confermata la disciplina già contenuta in proposito nell'abrogato D.L.vo 171/1998.

Val la pena sottolineare, con riferimento a questa disposizione del testo unico, che, ove si voglia considerare l'e-mail un mezzo che offre inadeguate garanzie di riservatezza – in quanto potenzialmente idonea ad essere letta o finanche modificata nel corso dei passaggi telematici intermedi dal mittente al destinatario – scatterebbero per i soggetti coinvolti nella comunicazione elettronica gli

⁸⁷ Cfr. artt. 4 e 5 direttiva 2002/58/CE; art. 3 D.L.vo 171/1998, già richiamato alla nota n. 10.

⁸⁸ Per le definizioni di “abbonato” e “utente” v. cap. II, par. 2.

obblighi di informazione sopra illustrati⁸⁹.

Sommario

15. Conservazione di dati di traffico per altre finalità

La formulazione originaria dell'art. 132 (“Conservazione di dati di traffico per altre finalità”) del testo unico⁹⁰ stabiliva che, fermo restando quanto previsto dall'art. 123, comma 2⁹¹, *i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante.*

La disposizione ora in esame va a toccare dunque profili delicati, soprattutto se si pensa alle esigenze di bilanciamento tra *sicurezza dello Stato e diritto alla riservatezza dei cittadini*⁹².

Il legislatore italiano ha scelto in proposito di avvalersi della facoltà riconosciutagli dall'art. 15 della direttiva 2002/58/CE di limitare alcuni dei diritti ed obblighi sanciti dalla direttiva stessa qualora tale restrizione costituisca⁹³ “una

⁸⁹ In questo senso, A. Lisi, *Tutela della privacy in Internet* cit., p. 68. Si veda d'altra parte la nota n. 85.

⁹⁰ Cfr. art. 15 direttiva 2002/58/CE.

⁹¹ V. par. 4.

⁹² Per qualche riflessione in argomento si veda M. Cammarata, *Quando è lecito spiare i cittadini*, in *InterLex*, www.interlex.it, www.interlex.it/675/lecito.htm.

⁹³ Ai sensi dell'art. 13, par. 1, direttiva 95/46/CE, il quale prevede che “Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle

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"⁹⁴.

Sul punto la relazione di accompagnamento al Codice afferma che "Il termine, tenendo conto delle osservazioni svolte da entrambe le Commissioni e degli orientamenti e delle evoluzioni in ambito comunitario e internazionale, viene fissato in un periodo non superiore a 30 mesi, che appare congruo rispetto alle esigenze prospettate in sede parlamentare e comunque ampiamente inferiore a quello attuale di cinque anni.

Sul piano formale, tenendo conto della giurisprudenza costituzionale e di legittimità in materia, in particolare sulla natura dei dati in questione e sulle modalità di acquisizione da parte della sola autorità giudiziaria, la finalità della conservazione di tali dati viene più direttamente collegata all'accertamento e alla

disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

- a) della sicurezza dello Stato;
- b) della difesa;
- c) della pubblica sicurezza;
- d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate;
- e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria;
- f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e);
- g) della protezione della persona interessata o dei diritti e delle libertà altrui".

⁹⁴ Tutte le misure statali adottate in base all'art. 15 della direttiva devono conformarsi ai *principi generali del diritto comunitario*, compresi quelli di cui all'art. 6, parr. 1 e 2, del trattato sull'Unione europea.

repressione dei reati, specificando meglio il contesto per il quale l'esigenza cui fa riferimento l'articolo in commento è stata prefigurata, vale a dire in relazione ai dati di traffico telefonico"⁹⁵.

⁹⁵ “Ferma presa di posizione dei Garanti per la privacy europei contro la proposta di introdurre in modo generalizzato, senza tener conto delle garanzie e dei limiti previsti da vari strumenti internazionali e comunitari (da ultimo, la direttiva n. 2002/58/CE pubblicata il 31 luglio 2002), nuovi obblighi di conservazione di dati di traffico relativi alle telefonate, alle e-mail, agli sms, ai collegamenti con Internet, per finalità di polizia e di giustizia.

Le Autorità europee considerano infatti ‘sproporzionata ed inaccettabile’ l'ipotesi avanzata dai governi europei di registrare sistematicamente, anche per finalità diverse da quelle di fatturazione o di pagamento delle interconnessioni, tutte le forme di telecomunicazione e comunicazione elettronica, mettendo a rischio la privacy dei cittadini europei: i Garanti hanno espresso la loro preoccupazione in una dichiarazione approvata in occasione della Conferenza internazionale di Cardiff (9-11 settembre 2002).

Questo il testo integrale della Dichiarazione sulla conservazione sistematica e obbligatoria dei dati di traffico:

Le Autorità europee per la protezione dei dati hanno rilevato con preoccupazione che nell'ambito del Terzo Pilastro dell'UE sono all'esame alcune proposte tali da comportare la conservazione sistematica e obbligatoria dei dati di traffico relativi a tutte le forme di telecomunicazione – durata, localizzazione, numeri utilizzati per chiamate telefoniche, fax, messaggi di posta elettronica, e per altri impieghi di Internet – per un periodo di un anno o più, allo scopo di consentire l'eventuale accesso da parte delle forze dell'ordine e degli organismi preposti alla sicurezza.

Le Autorità europee per la protezione dei dati dubitano fortemente della legittimità e liceità di misure dotate di tale ampiezza.

Desiderano inoltre richiamare l'attenzione sui costi eccessivi che ciò comporterebbe per le imprese operanti nel settore telecomunicazioni ed Internet e sull'assenza di misure analoghe negli USA.

Le Autorità europee per la protezione dei dati hanno più volte sottolineato che una conservazione siffatta costituirebbe un'indebita compressione dei diritti fondamentali garantiti ai singoli dall'articolo 8 della Convenzione europea sui diritti dell'uomo, così come ulteriormente sviluppati nella giurisprudenza della Corte europea dei diritti dell'uomo (v. Parere 4/2001 del Gruppo di lavoro ex Articolo 29, istituito dalla direttiva 95/46/CE, e la Dichiarazione di Stoccolma dell'aprile 2000).

La tutela dei dati di traffico delle telecomunicazioni è prevista attualmente anche dalla Direttiva 2002/58/CE del Parlamento europeo e del Consiglio in materia di privacy e comunicazioni elettroniche (Gazzetta Ufficiale CE L201/37), in base alla quale il trattamento dei dati di traffico è consentito, in linea di principio, ai fini della fatturazione e dei pagamenti di interconnessione.

All'esito di una lunga e franca discussione, la conservazione dei dati di traffico per scopi connessi all'attività delle forze dell'ordine dovrebbe essere conforme alle rigide condizioni previste dall'articolo 15(1) della Direttiva – ossia, caso per caso, solo per un periodo limitato e purché necessaria, opportuna e proporzionata all'interno di una società democratica.

Per la prima volta nell'ordinamento giuridico italiano è stato pertanto introdotto un preciso *obbligo di conservazione dei dati sul traffico telefonico ai fini investigativi*⁹⁶.

Con decreto-legge 24 dicembre 2003, n. 354⁹⁷, ritenuta la straordinaria necessità ed urgenza di *disciplinare le modalità di conservazione dei dati di traffico connesso ai servizi di comunicazione telefonica e via internet, così da prevenirne la perdita nell'ipotesi in cui ne risulti necessaria l'acquisizione ai fini della repressione di reati di particolare gravità*, il Governo è intervenuto sull'art. 132 in esame, sostituendone il testo come segue.

“Art. 132 (Conservazione di dati di traffico per altre finalità) - 1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione dei reati.

Pertanto, qualora sia necessario, in casi specifici, conservare dati di traffico, deve sussistere un'esigenza dimostrabile, il periodo di conservazione deve essere quanto più breve possibile, e le relative modalità devono essere disciplinate con chiarezza attraverso disposizioni di legge, in modo da offrire garanzie sufficienti contro accessi non autorizzati ed ogni altro tipo di abuso.

La conservazione sistematica di dati di traffico delle più svariate tipologie per un periodo di un anno o anche maggiore sarebbe evidentemente sproporzionata e, quindi, in ogni caso inaccettabile.

Le Autorità europee per la protezione dei dati si attendono che il Gruppo di Lavoro ex Articolo 29 sia consultato prima dell'adozione di misure che possano eventualmente scaturire dal dibattito in corso nell'ambito del Terzo Pilastro” (Garante per la protezione dei dati personali, *Newsletter* 9-15 settembre 2002, www.garanteprivacy.it).

⁹⁶ Sul punto si veda G. Costabile, *File di log, testo unico sulla privacy e finalità investigative*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/costabile.html.

⁹⁷ D.L. 24 dicembre 2003, n. 354, *Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia*, GU 29 dicembre 2003, n. 300 (il testo del provvedimento può essere consultato su www.filodiritto.com all'indirizzo www.filodiritto.com/notizieaggiornamenti/30dicembre2003/dl354tribunaliacquedispiustizia.htm)

2. Decorso il termine di cui al comma 1, i dati sono conservati dal fornitore per ulteriori trenta mesi e possono essere richiesti esclusivamente per finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato dell'autorità giudiziaria, d'ufficio o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale.

4. Dopo la scadenza del termine indicato al comma 1, il pubblico ministero richiede al giudice, che decide con decreto motivato, l'autorizzazione ad acquisire i dati. Tale disposizione si applica anche al difensore dell'imputato o della persona sottoposta alle indagini che intenda acquisire direttamente i dati dal fornitore. Il giudice procede all'acquisizione, con decreto motivato, anche d'ufficio.

5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto di particolari misure e di accorgimenti, nel determinare i quali si tiene comunque conto dei seguenti principi:

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato b);

b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;

c) individuare le modalità di accesso ai dati da parte di specifici incaricati del

trattamento in modo tale che, decorso il termine di cui al comma 1, l'accesso sia consentito solo nei casi di cui al comma 4 e all'articolo 7;

d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

6. Le modalità di trattamento dei dati di cui al comma 5 sono individuate con decreto del Ministro della giustizia, di concerto con il Ministro dell'interno, con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, su conforme parere del Garante⁹⁸.

L'intervento del Governo ha provocato accese discussioni tra gli operatori, nonché la pronta reazione del Garante, il quale, con comunicato del 23 dicembre 2003, ha preso atto "con preoccupazione del decreto legge approvato oggi dal

⁹⁸ Il provvedimento è intervenuto altresì sull'art. 181 del Codice della privacy, ivi aggiungendo, in fine, il seguente comma: "6-bis. Fino alla data del 31 dicembre 2005 per la conservazione del traffico si osserva il termine della prescrizione di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171"; nonché sull'art. 183 del Codice sostituendo, al comma 1, la lettera f) con la seguente: "f) il decreto legislativo 13 maggio 1998, n. 171, ad eccezione dell'articolo 4, comma 2, la cui abrogazione decorre dal 1° gennaio 2006".

Si ricorda che l'art. 4, comma 2, D.L.vo 171/1998 prevede quanto segue.

"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;
- 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".

Governo sulla conservazione dei dati del traffico telefonico e su Internet.

In particolare, la nuova disciplina sui dati relativi alle comunicazioni elettroniche e alle utilizzazioni di Internet può anche entrare in conflitto con le norme costituzionali sulla libertà e segretezza delle comunicazioni e sulla libertà di manifestazione del pensiero.

Il Garante confida in un attento esame del decreto da parte del Parlamento”.

Come è stato osservato, il D.L. 354/2003, nel riscrivere l’art. 132 del Codice della privacy, fa riferimento ai “dati relativi al traffico”, prevedendo – tramite richiamo all’art. 123, comma 2, in precedenza analizzato⁹⁹ – l’obbligatorietà della conservazione di quei dati specificamente finalizzati alla *fatturazione*. Dunque verrebbero esclusi “i log dei servizi (come http, ftp, mail, news) che si trovano a un livello più alto dello stack TCP/IP” (A. Monti)¹⁰⁰.

Di contrario avviso è altra parte della dottrina, secondo cui l’art. 132, sia nel testo modificato dal D.L. 354/2003 sia nel testo originale contempla i “dati relativi al traffico” *tout court*, e non solo dunque quelli specificamente finalizzati alla fatturazione. “Dobbiamo quindi ritenere che questi dati siano quelli di cui alla definizione ampia ex art. 4, 2° comma, lett. h, gli stessi cioè regolati dal primo comma dell’art. 123” (F. Veutro)¹⁰¹.

⁹⁹ V. par. 4.

¹⁰⁰ A. Monti, *Dati del traffico: chi-conserva-cosa?*, in *InterLex*, www.interlex.it, www.interlex.it/675/amonti72.htm. Si veda *ibidem* per un tentativo di individuazione analitica dei dati relativi al traffico rilevanti ai fini della disciplina.

¹⁰¹ “In sostanza, l’interpretazione del combinato disposto degli artt. 4, 123 e 132 del codice della privacy, alla luce degli artt. 6 e 15 della direttiva 2002/58/CE, induce a concludere che tutti i dati sottoposti a trattamento dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, sia a fini di trasmissione che di fatturazione, siano i dati o meno ‘strettamente necessari’ per quest’ultima, devono essere conservati per finalità di accertamento e repressione dei reati ai sensi dell’art. 132, come modificato dal decreto legge

Le norme del decreto pongono inoltre problemi – secondo coloro che accolgono la prima delle tesi su esposte – per quanto concerne la loro applicabilità agli ISP, in quanto il legislatore nella formulazione del testo normativo ha adottato come parametro di riferimento i fornitori di servizi di telefonia e i *carrier*.

È stato efficacemente osservato in proposito che “L’aspetto paradossale della situazione creata dal D.L. 354/03 è che, in rapporto ai servizi Internet, l’obbligo di conservazione per gli ISP si configura a seconda della tipologia di commercializzazione dei prodotti. Se housing, hosting, mail e via discorrendo sono fatturati a canone fisso, non c’è obbligo di conservazione. Se gli stessi servizi sono fatturati a tempo o a volume i dati di traffico vanno conservati. È facile immaginare che, se questo decreto legge dovesse essere convertito così com’è, gli ISP dovranno rivedere profondamente la propria offerta commerciale. O addirittura, valutare la possibilità di uscire da questo mercato. Il che, per certi versi, favorirebbe anche l’opera degli investigatori, che avrebbero così a che fare con un numero ridotto di interlocutori. Ma non farebbe certo bene al sistema-paese” (A. Monti)¹⁰².

Il decreto-legge 354/2003 è stato convertito con modificazioni dalla legge 45/2004¹⁰³. Conseguentemente, il testo vigente dell’art. 132 del Codice della privacy risulta pertanto, allo stato, essere il seguente¹⁰⁴.

“Art. 132 (Conservazione di dati di traffico per altre finalità) - 1. Fermo restando

354/03” (F. Vetro, *La conservazione dei dati relativi al traffico: una lettura diversa*, in *InterLex*, www.interlex.it, www.interlex.it/675/veutro1.htm).

¹⁰² A. Monti, *Dati del traffico: chi-conserva-cosa?* cit.

¹⁰³ L. 26 febbraio 2004, n. 45, *Conversione in legge, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l’amministrazione della giustizia*, GU 48 del 27 febbraio 2004.

¹⁰⁴ Le modifiche apportate in sede di conversione sono evidenziate in corsivo.

quanto previsto dall'articolo 123, comma 2, *i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi*, per finalità di accertamento e repressione dei reati.

2. Decorso il termine di cui al comma 1, i dati *relativi al traffico telefonico* sono conservati dal fornitore per ulteriori *ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti* di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato *del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private*. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, *ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante*¹⁰⁵.

4. *Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.*

5. *Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai*

¹⁰⁵ La disposizione del testo unico richiamata prevede che i diritti di cui all'art. 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'art. 145 se i trattamenti di dati personali sono effettuati da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397.

*sensi dell'articolo 17, volti anche a*¹⁰⁶:

- a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato b);
- b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
- c) individuare le modalità *di trattamento dei* dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, *l'utilizzazione dei dati sia consentita* solo nei casi di cui al comma 4 e all'articolo 7;
- d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2¹⁰⁷.

In sede di conversione il legislatore ha specificato dunque che l'obbligo di conservazione concerne i soli dati relativi al traffico *telefonico*. Il periodo di conservazione è stato inoltre ridotto rispetto alla precedente previsione. Il nuovo art. 132 continua comunque a destare perplessità, anche con riguardo all'opinione espressa in materia dai Garanti europei¹⁰⁸.

[Sommaro](#)

¹⁰⁶ L'art. 17 del Codice, come visto nel capitolo II, si occupa dei *dati semisensibili*.

¹⁰⁷ A seguito della conversione del decreto-legge, il comma 6-bis dell'art. 181 del Codice della privacy recita oggi: "*Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171*". La modifica all'art. 183 del Codice è stata soppressa in sede di conversione.

¹⁰⁸ V. nota n. 95.

16. Internet e reti telematiche

In relazione, specificamente, ad *Internet ed alle reti telematiche*, l'art. 133 del Codice della privacy (“Codice di deontologia e di buona condotta”)¹⁰⁹ prevede che il Garante per la protezione dei dati personali promuova, ai sensi dell'art. 12¹¹⁰, la sottoscrizione di un *codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica*.

Detto codice dovrà dettare, in particolare, i criteri per assicurare ed uniformare una più adeguata *informazione e consapevolezza degli utenti delle reti di comunicazione elettronica 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 e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'art. 11¹¹¹*, anche ai fini dell'eventuale rilascio di *certificazioni* attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

Si ricorda che, come previsto dal richiamato art. 12, il rispetto delle disposizioni contenute nel codice adottato *ex art. 133* del testo unico costituirà *condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici*¹¹².

¹⁰⁹ Cfr. art. 20, comma 2, lett. a), D.L.vo 467/2001.

¹¹⁰ Sull'art. 12 si rimanda a quanto detto nel capitolo II, par. 5.

¹¹¹ Sull'art. 11 (“Modalità del trattamento e requisiti dei dati”), v. cap. II, par. 5.

¹¹² In data 19 novembre 2003 AIP, ANFoV, Assoprovider e Federcomin, alla presenza dei ministri Stanca e Gasparri, hanno sottoscritto il *Codice di autoregolamentazione "Internet e minori"*.

Sommario

17. Videosorveglianza

Con disposizione analoga a quella contenuta nell'esaminato art. 133, l'art. 134 del Codice della privacy ("Videosorveglianza")¹¹³, che chiude il titolo X della parte II del testo unico dedicato alle comunicazioni elettroniche, prevede che il Garante promuova, ai sensi dell'art. 12, la sottoscrizione di un codice di deontologia e di buona condotta *per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'art. 11.*

Con il parere 4/2004 il Gruppo di lavoro che riunisce i Garanti europei è intervenuto in materia di videosorveglianza dettando un "decalogo" sulle cautele ed i principi da adottare, tenuto conto delle indicazioni giunte attraverso la consultazione pubblica conclusasi il 31 maggio 2003, alla quale hanno contribuito numerosi soggetti (aziende, studi legali e anche singoli cittadini).

Tra gli obiettivi e finalità del Codice vi è quello di *tutelare il diritto del minore alla riservatezza ed al corretto trattamento dei propri dati personali* nonché quello di agevolare, nel rispetto dell'art. 9 del Decreto legislativo 9 aprile 2003, n. 70 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno – sul quale si veda il capitolo successivo) la tutela del minore nei confronti delle *informazioni commerciali non sollecitate o che sfruttano la debolezza del minore*, ovvero, secondo quanto previsto all'art. 130 del Decreto legislativo 30 giugno 2003, n. 196, nei confronti delle *comunicazioni indesiderate*.

Il testo del Codice è disponibile su www.altalex.com all'indirizzo www.altalex.com/index.php?idnot=72. Per un primo commento si veda M. Dona, *Presentato il Codice "Internet e minori": tanto rumore per nulla?*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_consumatori/dona8.html.

¹¹³ Cfr. art. 20, comma 2, lett. g), D.L.vo 467/2001.

Il documento affronta innanzitutto alcuni aspetti essenziali, quali l'esigenza di armonizzare il quadro normativo sulla base della direttiva europea per la protezione dei dati, ma anche di altri strumenti sovranazionali (Carta dei diritti fondamentali dell'Unione europea; Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione dei dati); la necessità, per chi installa telecamere, di accertare in via preliminare se le immagini rilevate con i sistemi di videosorveglianza comportino il trattamento di dati personali, ossia se si riferiscano a soggetti identificabili (spesso, infatti, le immagini acquisite con le telecamere sono associate ad altri dati come impronte digitali, registrazioni sonore); l'obbligo di far riferimento alle regole elaborate dai Garanti, che si applicano anche ai trattamenti che non sono soggetti espressamente alle disposizioni della direttiva europea (ad esempio trattamenti effettuati per scopi di sicurezza pubblica o per il perseguimento di reati, oppure trattamenti effettuati da una persona fisica per scopi esclusivamente privati o familiari)¹¹⁴.

[Sommaro](#)

¹¹⁴ Si veda in proposito la *Newsletter* n. 203 del 23-29 febbraio 2004 del Garante per la protezione dei dati personali, www.garanteprivacy.it.

CAPITOLO IV

IL D.L.VO 70/2003 DI ATTUAZIONE DELLA DIRETTIVA EUROPEA SUL COMMERCIO ELETTRONICO

SOMMARIO: 1. [Premessa](#) – 2. [Obiettivi e campo di applicazione del D.L.vo 70/2003](#) – 3. [Definizioni](#) – 4. [Mercato interno](#) – 5. [Regime di stabilimento e di informazione](#) – 6. [Comunicazioni commerciali e spamming](#) – 7. [Informazioni dirette alla conclusione del contratto e inoltro dell'ordine](#) – 8. [Responsabilità dei prestatori intermediari \(provider\)](#) – 8.1. [Responsabilità nell'attività di semplice trasporto \(mere conduit\)](#) – 8.2. [Responsabilità nell'attività di memorizzazione temporanea \(caching\)](#) – 8.3. [Responsabilità nell'attività di memorizzazione di informazioni \(hosting\)](#) – 8.4. [Assenza dell'obbligo generale di sorveglianza](#) – 9. [Codici di condotta, composizione delle controversie e cooperazione](#) – 10. [Sanzioni](#)

[INDICE](#)

1. Premessa

Con il [decreto legislativo n. 70 del 9 aprile 2003](#)¹, emanato sulla base della delega

¹ D.L.vo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico*, GU Serie gen. 87 del 14 aprile 2003, Suppl. ord. Il testo del provvedimento può essere consultato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/dlvo70-2003.htm.

contenuta nella legge comunitaria 2001², l'Italia ha dato finalmente attuazione alla

L'entrata in vigore del provvedimento è stata fissata al trentesimo giorno dalla data della sua pubblicazione sulla Gazzetta ufficiale (art. 22).

Nella medesima GU è stato pubblicato anche il D.L.vo 9 aprile 2003, n. 68, *Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione*. Sull'argomento si rimanda all'Osservatorio di www.iusreporter.it dedicato al Diritto d'autore, raggiungibile all'indirizzo www.iusreporter.it/Testi/osservaautore.htm.

² La legge comunitaria 2001 (legge 1 marzo 2002, n. 39, *Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2001*, GU 72 del 26 marzo 2002, Suppl. ord.) aveva infatti delegato il Governo ad emanare un decreto legislativo per dare attuazione alla direttiva europea sul commercio elettronico.

Si riporta il testo dell'art. 31 della legge comunitaria 2001:

“Art. 31 (Attuazione della direttiva 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno)

1. Il Governo è delegato ad emanare, entro il termine e con le modalità di cui all'articolo 1, commi 1 e 2, un decreto legislativo per dare organica attuazione alla 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, nel rispetto dei principi e criteri direttivi generali di cui all'articolo 2, nonché dei seguenti principi e criteri direttivi:

a) definire le informazioni obbligatorie generali che devono essere fornite dal prestatore di un servizio ai destinatari del servizio stesso ed alle competenti autorità da designare ai sensi della normativa vigente nonché le modalità per renderle accessibili, in modo facile, diretto e permanente; in particolare, devono essere indicati in modo chiaro e inequivocabile i prezzi dei servizi, anche riguardo alle imposte e ai costi di consegna e deve essere reso esplicito che l'obbligo di registrazione della testata editoriale telematica si applica esclusivamente alle attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze previste dalla legge 7 marzo 2001, n. 62, o che comunque ne facciano specifica richiesta;

b) definire 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;

c) definire l'impiego di comunicazioni commerciali fornite da soggetti che esercitano una professione regolamentata, nel rispetto delle relative norme applicabili, nonché forme e procedure di consultazione e cooperazione con gli ordini professionali, nel rispetto della loro autonomia, per la predisposizione delle pertinenti norme e per incoraggiare l'elaborazione di codici di condotta a livello comunitario che precisino le informazioni che possono essere fornite a fini di comunicazioni commerciali;

d) disciplinare la responsabilità dei prestatori intermediari con riferimento all'attività di semplice trasporto; in particolare, il prestatore non sarà considerato responsabile delle informazioni trasmesse a condizione che:

- 1) non sia esso stesso a dare origine alla trasmissione;
- 2) non selezioni il destinatario della trasmissione;
- 3) non selezioni né modifichi le informazioni trasmesse;

e) disciplinare la responsabilità dei prestatori con riferimento alla memorizzazione temporanea detta "caching"; il prestatore non sarà considerato responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni, effettuata al solo scopo di rendere più efficace il successivo inoltra ad altri destinatari a loro richiesta, a condizione che egli:

- 1) non modifichi le informazioni;
- 2) si conformi alle condizioni di accesso alle informazioni;
- 3) si conformi alle norme di aggiornamento delle informazioni;
- 4) indichi tali informazioni in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;
- 5) non interferisca con l'uso lecito delle tecnologie ampiamente riconosciute ed utilizzate nel settore per ottenere dati sull'impiego delle stesse informazioni;

6) agisca prontamente per rimuovere le informazioni che ha memorizzato o per disabilitarne l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso;

f) disciplinare la responsabilità dei prestatori con riferimento all'attività cosiddetta di "hosting"; il prestatore non sarà considerato responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che egli:

- 1) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita;
- 2) per quanto attiene alle azioni risarcitorie, non sia al corrente dei fatti o di circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione;
- 3) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso;

g) disciplinare le modalità con le quali i prestatori di servizi delle società dell'informazione sono tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi, con cui hanno accordi di memorizzazione dei dati;

[direttiva 2000/31/CE](#) dell'8 giugno 2000, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*³.

h) favorire l'elaborazione, da parte di associazioni o di organizzazioni imprenditoriali, professionali o di consumatori, di codici di condotta per evitare violazioni dei diritti, garantire la protezione dei minori e salvaguardare la dignità umana;

i) prevedere misure sanzionatorie effettive, proporzionate e dissuasive nei confronti delle violazioni;

l) prevedere che il prestatore di servizi è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha usato la dovuta diligenza;

m) prevedere che, in caso di dissenso fra prestatore e destinatario del servizio della società dell'informazione, la composizione extragiudiziale delle controversie possa adeguatamente avvenire anche per via elettronica”.

Sulle varie fasi del recepimento della direttiva 2000/31/CE, si veda l'*Osservatorio* di www.iusreporter.it dedicato al Commercio elettronico, raggiungibile all'indirizzo www.iusreporter.it/Testi/agg-commel.htm.

³ GUCE L 178 del 17 luglio 2000 (successiva rettifica in GUCE L 285 del 23 ottobre 2002).

Per un commento all'intero provvedimento, si veda AA.VV., *Commento organico alla direttiva 2000/31/CE* (“*Direttiva sul commercio elettronico*”), in *Boll. LUISS Ceradi*, Roma, 2002; G. Briganti, *La direttiva sul commercio elettronico*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/doc-dircommel.htm.

In generale, sul commercio elettronico, si veda A. Sirotti Gaudenzi, *Il commercio elettronico nella Società dell'Informazione*, Napoli, SE, 2003; sull'attuazione della direttiva nell'ordinamento italiano si veda in particolare E.M. Tripodi, *Commercio elettronico e contratti. Tre variazioni sul tema*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6846.

Per gli aspetti *amministrativi* del commercio elettronico, in particolare in ordine all'obbligo di comunicazione di cui all'art. 18 D.L.vo 114/1998, si veda E.M. Tripodi, *Profili amministrativi del commercio elettronico*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., pp. 402 ss.

L'art. 18 del D.L.vo 31 marzo 1998, n. 114, *Riforma della disciplina relativa al settore del commercio, a norma dell'art. 4, comma 4, della legge 15 marzo 1997, n. 59* (GU 24 aprile 1998, n. 95, Suppl. ord.) prevede infatti quanto segue.

“18. *Vendita per corrispondenza, televisione o altri sistemi di comunicazione.* 1. La vendita al dettaglio per corrispondenza o tramite televisione o altri sistemi di comunicazione è soggetta a previa comunicazione al comune nel quale l'esercente ha la residenza, se persona fisica, o la sede legale. L'attività può essere iniziata decorsi trenta giorni dal ricevimento della comunicazione.

2. È vietato inviare prodotti al consumatore se non a seguito di specifica richiesta. È consentito l'invio di campioni di prodotti o di omaggi, senza spese o vincoli per il consumatore.

3. Nella comunicazione di cui al comma 1 deve essere dichiarata la sussistenza del possesso dei requisiti di cui all'art. 5 e il settore merceologico.

4. Nei casi in cui le operazioni di vendita sono effettuate tramite televisione, l'emittente televisiva deve accertare, prima di metterle in onda, che il titolare dell'attività è in possesso dei requisiti prescritti dal presente decreto per l'esercizio della vendita al dettaglio. Durante la trasmissione debbono essere indicati il nome e la denominazione o la ragione sociale e la sede del venditore, il numero di iscrizione al registro delle imprese ed il numero della partita IVA. Agli organi di vigilanza è consentito il libero accesso al locale indicato come sede del venditore.

5. Le operazioni di vendita all'asta realizzate per mezzo della televisione o di altri sistemi di comunicazione sono vietate.

6. Chi effettua le vendite tramite televisione per conto terzi deve essere in possesso della licenza prevista dall'art. 115 del testo unico delle leggi di pubblica sicurezza, approvato con r. d. 18 giugno 1931, n. 773.

7. Alle vendite di cui al presente articolo si applicano altresì le disposizioni di cui al d. l. 15 gennaio 1992, n. 50, in materia di contratti negoziati fuori dei locali commerciali”.

Con riguardo in particolare al D.L.vo 15 gennaio 1992, n. 50, *Attuazione della direttiva n. 85/577/CE in materia di contratti negoziati fuori dei locali commerciali* (GU Serie gen. 27 del 3 febbraio 1992, Suppl. ord.) occorre tener presente che, ai sensi dell'art. 15, comma 2, del già richiamato [D.L.vo 185/1999 sui contratti a distanza conclusi dai consumatori](#), “Fino alla emanazione di un testo unico di coordinamento delle disposizioni di cui al presente decreto legislativo con la disciplina recata dal decreto legislativo 15 gennaio 1992, n. 50, alle forme speciali di vendita previste dall'articolo 9 del decreto legislativo 15 gennaio 1992, n. 50, e dagli articoli 18 e 19 del decreto legislativo 31 marzo 1998, n. 114, si applicano le disposizioni più favorevoli per il consumatore contenute nel presente decreto legislativo [185/1999]”.

Vale la pena inoltre sottolineare che la mancata osservanza dell'obbligo di cui all'art. 18 D.L.vo 114/1998 comporta l'applicazione della sanzione amministrativa di cui all'art. 22 del medesimo provvedimento, consistente nel pagamento di una somma da Euro 2.582 ad Euro 15.494. Si prevede altresì che, in caso di particolare gravità o di recidiva il sindaco possa disporre la sospensione della attività di vendita per un periodo non superiore a venti giorni; in caso di svolgimento abusivo dell'attività il sindaco ordina la chiusura immediata dell'esercizio di vendita.

Per ciò che concerne, infine, le *aste on-line*, si veda la circolare del 17 giugno 2002, n. 3547/C, con cui il Ministero delle attività produttive è intervenuto nella discussa materia fornendo alcune indicazioni sulla disciplina ad esse applicabile (il testo della circolare è disponibile su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/circolareaste.htm). V. inoltre E.M. Tripodi, *Le aste on line: i recenti sviluppi disciplinari tra privato e pubblico (in margine alla Circolare del Ministero delle attività produttive n. 3547/C)*, in *Discipl. Comm. e servizi*, 2002, pp. 491 ss.

Come si legge nella [relazione illustrativa](#)⁴ che accompagna il provvedimento di attuazione, la direttiva europea sul commercio elettronico si fonda sulla *clausola mercato interno* ed è volta ad assicurare la libera prestazione dei servizi on-line nell'insieme della Comunità, creando *regole uniformi per il commercio elettronico*, che è, per sua stessa natura, senza frontiere.

“In particolare, anche in considerazione dell’incertezza esistente in molti Stati membri sulla disciplina da applicare a tale forma di commercio e alle divergenze esistenti tra le varie legislazioni nazionali, la direttiva si propone di fornire una base comune di regole alla prestazione di servizi della società dell’informazione e, dunque, a tutte le transazioni in linea, in cui le negoziazioni e la conclusione degli accordi avvengono senza la presenza fisica dei contraenti.

La direttiva 2000/31 è uno dei punti portanti del piano d'azione della Commissione, che ha lanciato, nel dicembre 1999, l'iniziativa eEurope, con lo scopo di ‘mettere l'Europa in rete’, ed ha presentato un rapporto sullo stato d'avanzamento di questo piano nell'incontro di Lisbona del 23 e 24 marzo 2000.

In questo summit il Consiglio europeo ha fissato un obiettivo ambizioso, divenire l'economia della conoscenza più competitiva e dinamica del mondo, riconoscendo la necessità urgente per l'Europa di sfruttare rapidamente le possibilità offerta dalla *new economy* e, in particolare, da internet”⁵.

Con il provvedimento in esame, il Governo, dunque, “in piena aderenza alla politica europea, attraverso lo strumento di recepimento della direttiva comunitaria, si propone di sviluppare un'economia basata sulla conoscenza, di

⁴ Si farà, più precisamente, riferimento al testo della relazione illustrativa riportato dalla notifica dello schema di decreto legislativo alla Commissione europea, effettuata con nota n. 2003 DAR 0029/I del 24 gennaio 2003.

⁵ Su *eEurope* si veda la seguente pagina web: http://europa.eu.int/information_society/eeurope/.

contribuire allo sviluppo e alla modernizzazione dei mercati facilitando il sorgere di nuove forme di gestione dell'attività imprenditoriale, in particolare di medie o piccole dimensioni, promuovendo nuove tipologie di commercio.

Uno degli obiettivi da perseguire è pervenire, attraverso regole chiare e trasparenti, a costi di produzione minori e ad una migliore scelta e qualità dei prodotti consegnati, accrescendo così la fiducia dei consumatori nei contratti telematici.

Tale fiducia, a monte, deve essere riposta su meccanismi che garantiscano la sicurezza, l'affidabilità delle comunicazioni in rete, la certezza dell'integrità del documento, sistemi rapidi di composizione extragiudiziale delle controversie”.

Il decreto sul commercio elettronico si compone di 22 articoli, che saranno brevemente analizzati nel prosieguo.

Le disposizioni dettate dal provvedimento si vanno ad aggiungere al già complesso quadro normativo italiano in materia ed hanno sollevato accese critiche tra i primi commentatori⁶.

⁶ Si veda M. Cammarata, *Troppe norme, occorre un testo unico*, in *InterLex*, www.interlex.it, www.interlex.it/ecom/troppenorme.htm.

Nello stesso sito, v. M. Cammarata, *Le trappole nei contratti di hosting*, secondo cui “Il testo [del provvedimento] è criptico, confuso, ridondante, con diversi passaggi che fanno rabbrivire i giuristi più attenti”; G. Scorza, *“Testata editoriale telematica”: le sviste del legislatore*, secondo cui “Purtroppo il testo del decreto legislativo 70/03 delude le grandi aspettative che attorno ad esso si erano create e non appare neppure rispondente alle finalità ed agli obiettivi individuati dal legislatore comunitario”.

Secondo E.M. Tripodi, *Commercio elettronico e contratti. Tre variazioni sul tema cit.*, “Le farraginosità del testo della direttiva, frutto dei numerosi compromessi in sede di stesura definitiva, costituiscono un vizio genetico che il nostro decreto ha finito necessariamente per ritrovarsi nel proprio DNA, con, in più, qualche ulteriore motivo di perplessità che forse poteva essere evitato, con riferimento, in particolare, al regime di responsabilità dei *provider* [...] Il recepimento della direttiva 2000/31/CE da parte del nostro legislatore altro non è stato che una ‘ricopiatura’ del testo della direttiva medesima. In sostanza, il D.Lgs. n. 70/2003 più che un atto normativo appare più simile ad un atto amministrativo”.

Sommario

2. Obiettivi e campo di applicazione del D.L.vo 70/2003

Obiettivo fondamentale del decreto sul commercio elettronico è quello di *promuovere la libera circolazione dei servizi della società dell'informazione* (come definiti dall'art. 2), *fra i quali il commercio elettronico* (art. 1, comma 1), garantendo così il buon funzionamento del mercato.

Non rientrano nel campo di applicazione del provvedimento (art. 1, comma 2)⁷:

a) i rapporti fra contribuente e amministrazione finanziaria connessi con l'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi nonché la regolamentazione degli aspetti tributari dei servizi della società dell'informazione ed in particolare del commercio elettronico⁸;

⁷ Con riguardo anche ai considerando 12, 13 e 16 della [direttiva 2000/31/CE](#).

⁸ Con riguardo, in particolare, all'IVA, imposta che colpisce numerosi servizi contemplati dal provvedimento sul commercio elettronico, rilevante è la direttiva 2002/38/CE del 7 maggio 2002, *che modifica temporaneamente la direttiva 77/388/CEE per quanto riguarda il regime di imposta sul valore aggiunto applicabile ai servizi di radiodiffusione e di televisione e a determinati servizi prestati tramite mezzi elettronici*, GUCE L 128 del 15 maggio 2002.

La direttiva 2002/38/CE è stata attuata in Italia con il D.L.vo 1 agosto 2003, n. 273, *Attuazione della direttiva 2002/38/CE, che modifica la direttiva 77/388/CEE, in materia di regime IVA applicabile ai servizi di radiodiffusione e di televisione, nonché a determinati servizi prestati tramite mezzi elettronici*, GU 230 del 3 ottobre 2003. Il provvedimento è entrato in vigore il 4 ottobre 2003 introducendo delle modifiche al DPR 633/1972 (*Istituzione e disciplina dell'imposta sul valore aggiunto*).

A titolo illustrativo, la direttiva (allegato L) elenca i seguenti servizi rientranti nella definizione di "servizi forniti tramite mezzi elettronici" di cui al modificato testo della direttiva 77/388/CE – direttiva 77/388/CEE del Consiglio, del 17 maggio 1977, *in materia di armonizzazione delle legislazioni degli Stati membri relative alle imposte sulla cifra d'affari - sistema comune di imposta sul valore aggiunto: base imponibile uniforme*, GUCE L 145 del 13 giugno 1977 – (art. 9, par. 2, lett. e)):

b) le *questioni relative al diritto alla riservatezza*, con riguardo al *trattamento dei dati personali nel settore delle telecomunicazioni* di cui alla [legge 31 dicembre 1996, n. 675](#) e al [decreto legislativo 13 maggio 1998, n. 171](#)⁹ e successive modificazioni;

-
- fornitura di siti web e web-hosting, gestione a distanza di programmi e attrezzature;
 - fornitura di software e relativo aggiornamento;
 - fornitura di immagini, testi e informazioni e messa a disposizione di basi di dati;
 - fornitura di musica, film, giochi, compresi i giochi di sorte o d'azzardo, programmi o manifestazioni politici, culturali, artistici, sportivi, scientifici o di intrattenimento;
 - fornitura di prestazioni di insegnamento a distanza.

D'altra parte, la direttiva 2002/38/CE specifica che il solo fatto che il fornitore di un servizio e il suo cliente comunichino per *posta elettronica* non implica che il servizio fornito sia un servizio elettronico ai sensi dell'art. 9, par. 2, lett. e), ultimo trattino, della modificata direttiva 77/388/CE.

Il testo della direttiva 2002/38/CE è pubblicato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/direttiva2002-38-ce.htm; il testo del D.L.vo 273/2003 può essere consultato su www.altalex.com all'indirizzo www.altalex.com/index.php?idnot=6648.

In materia si ricorda anche il D.L.vo 20 febbraio 2004, n. 52, *Attuazione della direttiva 2001/115/CE che semplifica e armonizza le modalità di fatturazione in materia di IVA*, GU 49 del 28 febbraio 2004, Suppl. ord. 30.

Si veda inoltre U. Zanini, *La fattura elettronica - La Direttiva 2001/115/CE e il Decreto Legislativo di attuazione*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/zanini.html; W. Maccario, *La tassazione dell'E-Commerce: le imposte dirette*, in *Filodiritto*, www.filodiritto.com, www.filodiritto.com/diritto/pubblico/tributario/tassazioneecommerce/maccario.htm; M. Paracchi e N. Sirtori, *Aspetti tributari e fiscali di internet*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., pp. 1203 ss.; E. Romanelli Grimaldi, *Gli aspetti tributari del commercio elettronico*, in *Il commercio via Internet* cit., pp. 195 ss.

⁹ L'esclusione in parola riguarda *solo* le questioni espressamente indicate. Le norme del D.L.vo 70/2003 e, oggi – stante l'abrogazione del D.L.vo 171/1998 e della L. 675/1996 – del [Codice della privacy](#) dovranno dunque trovare applicazione congiunta nel proprio ambito applicativo. Questo, come si dirà, vale in particolare in materia di *spamming*.

Secondo il considerando 14 della direttiva 2000/31/CE, infatti, "L'applicazione della presente direttiva deve essere pienamente conforme ai principi relativi alla protezione dei dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari".

- c) le intese restrittive della concorrenza;
- d) le prestazioni di servizi della società dell'informazione effettuate da soggetti stabiliti in Paesi non appartenenti allo spazio economico europeo¹⁰;
- e) le attività, dei notai o di altre professioni, nella misura in cui implicano un nesso diretto e specifico con l'esercizio dei pubblici poteri;
- f) la rappresentanza e la difesa processuali;
- g) i giochi d'azzardo, ove ammessi, che implicano una posta pecuniaria, i giochi di fortuna, compresi il lotto, le lotterie, le scommesse i concorsi pronostici e gli altri giochi come definiti dalla normativa vigente, nonché quelli nei quali l'elemento aleatorio è prevalente.

Sono fatte salve dal decreto, inoltre, le disposizioni comunitarie e nazionali sulla tutela della salute pubblica e dei consumatori (come definiti dall'art. 2), sul regime autorizzatorio in ordine alle prestazioni di servizi investigativi o di vigilanza privata, nonché in materia di ordine pubblico e di sicurezza, di prevenzione del riciclaggio del denaro, del traffico illecito di stupefacenti, di commercio, importazione ed esportazione di armi, munizioni ed esplosivi e dei materiali d'armamento di cui alla legge 9 luglio 1990, n. 185 (art. 1, comma 3).

[Sommar](#)

¹⁰ Considerando 58 della direttiva 2000/31/CE: "La presente direttiva non deve applicarsi ai servizi di prestatori stabiliti in un paese terzo. Tuttavia, data la dimensione globale del commercio elettronico, è opportuno garantire la coerenza della normativa comunitaria con quella internazionale. La presente direttiva deve far salvi i risultati delle discussioni sugli aspetti giuridici in corso presso le organizzazioni internazionali (tra le altre, OMC, OCSE, Uncitral)".

3. Definizioni

Ai fini del provvedimento in esame valgono le seguenti *definizioni* (art. 2, comma 1):

A) *servizi della società dell'informazione*: le attività economiche svolte in linea (on-line) nonché i servizi definiti dall'art. 1, comma 1, lett. b), della legge 21 giugno 1986, n. 317, e successive modificazioni¹¹.

Detta norma prevede che 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*¹²;

B) *prestatore*: la persona fisica o giuridica che presta un servizio della società dell'informazione;

¹¹ Si ricorda che, ai sensi della direttiva 2002/58/CE, costituiscono *servizi 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'art. 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica.*

¹² La legge 21 giugno 1986, n. 317 (GU 151 del 2 luglio 1986) reca oggi: *Procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione in attuazione della direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998.*

La disposizione citata nel testo specifica inoltre che per *servizio a distanza* deve intendersi “un servizio fornito senza la presenza simultanea delle parti”; per *servizio per via elettronica* “un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento, compresa la compressione digitale e di memorizzazione di dati e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici”; per *servizio a richiesta individuale di un destinatario di servizi* “un servizio fornito mediante trasmissione di dati su richiesta individuale”.

C) *prestatore stabilito*: il prestatore che esercita effettivamente un'attività economica mediante una stabile organizzazione per un tempo indeterminato.

Viene specificato che “la presenza e l'uso dei mezzi tecnici e delle tecnologie necessarie per prestare un servizio non costituiscono di per sé uno stabilimento del prestatore”¹³.

Come si legge nella relazione illustrativa, infatti, “il concetto di stabilimento non va riferito al luogo in cui si trovano i mezzi tecnici e le tecnologie necessarie ad effettuare la prestazione del servizio: ciò implica che la sede del prestatore dei servizi oggetto della direttiva prescinde dall'ubicazione dei server o dei siti web utilizzati dal medesimo per la prestazione di tali servizi”;

D) *destinatario del servizio*: il soggetto che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili informazioni;

E) *consumatore*: qualsiasi persona fisica che agisca con finalità non riferibili all'attività commerciale, imprenditoriale o professionale eventualmente svolta;

F) *comunicazioni commerciali*: tutte le forme di comunicazione *destinate, in*

¹³ Il testo dello schema di decreto legislativo di attuazione notificato alla Commissione europea, prevedeva, in aggiunta, le parole “quando svolgono funzioni meramente ausiliarie e preparatorie”.

A questo proposito, si ricorda quanto contenuto nel parere (favorevole con osservazioni) espresso dalla X Commissione parlamentare sullo schema di provvedimento:

“a) con riferimento all'articolo 2, comma 1, lettera c), si valuti l'opportunità di mantenere nel testo del decreto legislativo la precisazione che la presenza e l'uso di mezzi tecnici e delle tecnologie necessarie per prestare un servizio non costituiscono di per sé uno stabilimento del prestatore «quando svolgono funzioni meramente ausiliarie e preparatorie», atteso che tale precisazione non trova corrispondenza nella direttiva - la quale stabilisce che il luogo di stabilimento è quello in cui le società esercitano la loro attività economica e che, ai sensi dell'articolo 3, comma 1, dello schema, la disciplina nazionale risulta applicabile ai prestatori stabiliti sul territorio italiano”.

Sul parere si veda l'*Osservatorio* di www.iusreporter.it sul Commercio elettronico, sopra citato.

modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di un soggetto che esercita un'attività agricola, commerciale, industriale, artigianale o una libera professione.

Non sono di per sé comunicazioni commerciali:

1) *le informazioni che consentono un accesso diretto all'attività dell'impresa, del soggetto o dell'organizzazione, come un nome di dominio, o un indirizzo di posta elettronica;*

2) *le comunicazioni relative a beni, servizi o all'immagine di tale impresa, soggetto o organizzazione, elaborate in modo indipendente, in particolare senza alcun corrispettivo;*

G) *professione regolamentata: professione riconosciuta ai sensi dell'art. 2, del decreto legislativo 27 gennaio 1992, n. 115, ovvero ai sensi dell'art. 2 del decreto legislativo 2 maggio 1994, n. 319¹⁴;*

¹⁴ D.L.vo 27 gennaio 1992, n. 115, *Attuazione della direttiva n. 89/48/CEE relativa ad un sistema generale di riconoscimento dei diplomi di istruzione superiore che sanzionano formazioni professionali di una durata minima di tre anni*, GU 40 del 18 febbraio 1992, il cui articolo 2 ("Professioni") prevede:

"1. Ai fini del presente decreto si considerano professioni:

a) le attività per il cui esercizio è richiesta la iscrizione in albi, registri ed elenchi, tenuti da amministrazioni o enti pubblici, se la iscrizione è subordinata al possesso di una formazione professionale rispondente al requisito di cui al comma 3 dell'art. 1;

b) i rapporti di impiego pubblico o privato, se l'accesso ai medesimi è subordinato, da disposizioni legislative o regolamentari, al possesso di una formazione professionale rispondente al requisito di cui al comma 3 dell'art. 1;

c) le attività esercitate con l'impiego di un titolo professionale il cui uso è riservato a chi possiede una formazione professionale rispondente al requisito di cui al comma 3 dell'art. 1;

d) le attività attinenti al settore sanitario nei casi in cui il possesso di una formazione professionale rispondente al requisito di cui al comma 3 dell'art. 1 è condizione determinante ai fini della retribuzione delle relative prestazioni o della ammissione al rimborso".

H) *ambito regolamentato*: le disposizioni applicabili ai prestatori di servizi o ai servizi della società dell'informazione, indipendentemente dal fatto che siano di carattere generale o loro specificamente destinate.

L'ambito regolamentato riguarda le disposizioni che il prestatore deve soddisfare per quanto concerne:

- 1) l'accesso all'attività di servizi della società dell'informazione, quali le disposizioni riguardanti le qualifiche e i regimi di autorizzazione o di notifica;
- 2) l'esercizio dell'attività di un servizio della società dell'informazione, quali, ad esempio, le disposizioni riguardanti il comportamento del prestatore, la qualità o i contenuti del servizio, comprese le disposizioni applicabili alla pubblicità e ai contratti, ovvero alla responsabilità del prestatore.

L'ambito regolamentato comprende unicamente i requisiti riguardanti le attività in

L'art. 2 ("Professioni") del D.L.vo 2 maggio 1994, n. 319 (*Attuazione della direttiva 92/51/CEE relativa ad un secondo sistema generale di riconoscimento della formazione professionale che integra la direttiva 89/48/CEE*, GU 123 del 28 maggio 1994, Suppl. ord.) così recita:

"1. Ai fini del presente decreto si considerano professioni:

- a) le attività per il cui esercizio è richiesta la iscrizione in albi, registri ed elenchi, tenuti da amministrazioni o enti pubblici, se la iscrizione è subordinata al possesso di una formazione professionale rispondente ai requisiti di cui ai commi 3 e 4 dell'art. 1;
- b) i rapporti di impiego pubblico o privato, se l'accesso ai medesimi è subordinato, da disposizioni legislative o regolamentari, al possesso di una formazione professionale rispondente ai requisiti di cui ai commi 3 e 4 dell'art. 1;
- c) le attività esercitate con l'impiego di un titolo professionale il cui uso è riservato a chi possiede una formazione professionale rispondente ai requisiti di cui ai commi 3 e 4 dell'art. 1;
- d) le attività attinenti al settore sanitario nei casi in cui il possesso di una formazione professionale rispondente ai requisiti di cui ai commi 3 e 4 dell'art. 1 è condizione determinante ai fini della retribuzione delle relative prestazioni o della ammissione al rimborso".

linea e non comprende i requisiti legali relativi a (art. 2, comma 2)¹⁵:

a) le merci in quanto tali nonché le merci, i beni e i prodotti per le quali le disposizioni comunitarie o nazionali nelle materie di cui all'art. 1, comma 3, sopra illustrato, prevedono il possesso e l'esibizione di documenti, certificazioni, nulla osta o altri titoli autorizzatori di qualunque specie;

b) la consegna o il trasporto delle merci;

c) i servizi non prestati per via elettronica.

Sono inoltre fatte salve dal decreto sul commercio elettronico, ove non espressamente derogate, le disposizioni in materia bancaria, finanziaria, assicurativa e dei sistemi di pagamento¹⁶ nonché le competenze degli organi amministrativi e degli organi di polizia aventi funzioni di vigilanza e di controllo,

¹⁵ Tenuto conto di quanto enunciato dal considerando 21 della direttiva sul commercio elettronico:

“Il campo d'applicazione dell'ambito regolamentato lascia impregiudicata un'eventuale armonizzazione futura all'interno della Comunità dei servizi della società dell'informazione e la futura legislazione adottata a livello nazionale in conformità della normativa comunitaria.

L'ambito regolamentato comprende unicamente requisiti riguardanti le attività in linea, quali l'informazione in linea, la pubblicità in linea, la vendita in linea, i contratti in linea, e non comprende i requisiti legali degli Stati membri relativi alle merci, quali le norme in materia di sicurezza, gli obblighi di etichettatura e la responsabilità per le merci, o i requisiti degli Stati membri relativi alla consegna o al trasporto delle merci, compresa la distribuzione di prodotti medicinali.

L'ambito regolamentato non comprende l'esercizio dei diritti di prelazione su taluni beni, quali le opere d'arte, da parte delle autorità pubbliche”.

¹⁶ Con riferimento a questa norma, si riporta l'osservazione espressa dalla X Commissione parlamentare nel suo parere sullo schema di decreto legislativo:

“b) con riferimento all'articolo 2, comma 3, che fa salve le specifiche disposizioni relative alla materia bancaria, finanziaria, assicurativa e dei sistemi di pagamento, appare opportuno valutare attentamente - anche alla luce della comunicazione della Commissione europea sul commercio elettronico e i servizi finanziari, del 7 febbraio 2001 - se tale previsione non limiti o escluda di fatto la possibilità di applicare il decreto legislativo al commercio on line di prodotti bancari, finanziari o assicurativi, introducendo un'esclusione non prevista dalla direttiva”.

compreso il controllo sulle reti informatiche di cui alla legge 31 luglio 1997, n. 249¹⁷, e delle autorità indipendenti di settore (art. 2, comma 3).

Sommario

4. Mercato interno

L'art. 3 del decreto sul commercio elettronico introduce il *principio in base al quale il controllo dei servizi della società dell'informazione deve essere effettuato all'origine dell'attività*¹⁸.

Ai sensi dell'art. 3, comma 1, del provvedimento, pertanto, *i servizi della società dell'informazione forniti da un prestatore stabilito* – come definito dall'art. 2 – *sul territorio italiano devono conformarsi alle disposizioni nazionali applicabili nell'ambito regolamentato, oltre che alle norme del decreto in esame.*

¹⁷ L. 31 luglio 1997, n. 249, *Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo*, GU Serie gen. 177 del 31 luglio 1997, Suppl. ord.

¹⁸ Principio esplicitato nei considerando 22 e 24 della direttiva 2000/31/CE.

“Il controllo dei servizi della società dell'informazione deve essere effettuato all'origine dell'attività, al fine di assicurare una protezione efficace degli obiettivi di interesse pubblico, ed è pertanto necessario garantire che l'autorità competente assicuri questa tutela non soltanto per i cittadini del suo paese ma anche per tutti i cittadini della Comunità.

Per migliorare la fiducia reciproca tra gli Stati membri, è indispensabile specificare chiaramente questa responsabilità dello Stato membro in cui i servizi hanno origine.

Inoltre, per garantire efficacemente la libera circolazione dei servizi e la certezza del diritto per i prestatori e i loro destinatari, questi servizi devono in linea di principio essere sottoposti alla normativa dello Stato membro nel quale il prestatore è stabilito” (considerando 22).

“Nel contesto della presente direttiva, nonostante il principio del controllo alla fonte dei servizi della società dell'informazione, è legittimo, alle condizioni stabilite dalla presente direttiva, che gli Stati membri adottino misure per limitare la libera circolazione dei servizi della società dell'informazione” (considerando 24).

Le disposizioni relative all'ambito regolamentato (definito dall'art. 2, comma 1, lett. h), sopra illustrato) *non possono d'altra parte limitare la libera circolazione dei servizi della società dell'informazione provenienti da un prestatore stabilito in un altro Stato membro* (art. 3, comma 2).

Si specifica inoltre che alle *controversie che riguardano il prestatore stabilito si applicano le disposizioni del [regolamento CE n. 44/2001](#) del Consiglio del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale* (art. 3, comma 3)¹⁹.

Le disposizioni dei commi 1 e 2 dell'art. 3, appena esaminate, *non trovano applicazione nei seguenti casi* (art. 4):

¹⁹ Regolamento 44/2001/CE, GUCE L 12 del 16 gennaio 2001; successiva rettifica in GUCE L 307 del 24 novembre 2001.

Il Regolamento, entrato in vigore il primo marzo 2002, ha sostituito la Convenzione di Bruxelles sottoscritta il 27 settembre 1968 (GUCE C 189 del 28 luglio 1990) e la Convenzione di Lugano del 16 settembre 1988.

Il principio fondamentale accolto dal Regolamento in materia di competenza giurisdizionale è quello secondo cui la competenza a conoscere di una data controversia presentante elementi di estraneità spetta al giudice dello *Stato in cui è domiciliato il convenuto*, indipendentemente dalla cittadinanza di quest'ultimo.

A questo proposito, infatti, l'art. 2, par. 1, stabilisce che, *salve le altre disposizioni del Regolamento, le persone domiciliate nel territorio di un determinato Stato membro sono convenute, a prescindere dalla loro nazionalità, davanti ai giudici di tale Stato membro*.

Deve d'altro canto osservarsi che, con specifico riferimento al *commercio elettronico B2C*, il Regolamento 44/2001/CE, nel suo ambito di applicazione, tutela il *consumatore on-line* dando a costui la possibilità di *scegliere* se convenire la controparte avanti il giudice dello *Stato di proprio domicilio*, evitando un giudizio all'estero, o avanti il giudice dello Stato di domicilio dell'altra parte, qualora ritenuto conveniente. Più rigide si presentano invece le regole per chi esercita attività di commercio elettronico in ambito comunitario, il quale sarà costretto a citare il consumatore domiciliato in uno Stato membro solo ed esclusivamente in detto Stato.

Si veda T. Ballarino, *Diritto Internazionale Privato*, Padova, Cedam; A. Sirotti Gaudenzi, *Il commercio elettronico nella Società dell'Informazione* cit., pp. 63 ss.; G. Briganti, *Controversie nel commercio elettronico B2C: competenza giurisdizionale e legge applicabile*, 2004, disponibile nella sezione *Internet* degli e-book di *IusOnDemand*, www.iusondemand.com/ebook.

- a) diritti d'autore, diritti assimilati, diritti di cui alla legge 21 febbraio 1989, n. 70 e al decreto legislativo 6 maggio 1999, n. 169, nonché diritti di proprietà industriale;
- b) emissione di moneta elettronica da parte di istituti per i quali gli Stati membri hanno applicato una delle deroghe di cui all'art. 8, par. 1, della direttiva 2000/46/CE del Parlamento europeo e del Consiglio riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica;
- c) l'art. 44, par. 2, della direttiva 85/611/CEE, in materia di pubblicità degli organismi di investimento collettivo in valori mobiliari;
- d) all'attività assicurativa di cui all'art. 30 e al titolo IV della direttiva 92/49/CEE (terza direttiva sulle assicurazioni sui danni), agli artt. 7 e 8 della direttiva 88/357/CEE (seconda direttiva sulle assicurazioni sui danni); al titolo IV della direttiva 92/96/CEE (terza direttiva sulle assicurazioni sulla vita) e all'art. 4 della direttiva 90/619/CEE (seconda direttiva sulle assicurazioni sulla vita), come modificate dalla direttiva 2002/83/CE;
- e) *facoltà delle parti di scegliere la legge applicabile al loro contratto*²⁰;
- f) *obbligazioni contrattuali riguardanti i contratti conclusi dai consumatori*;
- g) validità dei contratti che istituiscono o trasferiscono diritti relativi a beni immobili nei casi in cui tali contratti devono soddisfare requisiti formali;

²⁰ Sulle questioni relative alla *legge applicabile* nel commercio elettronico, v. A. Sirotti Gaudenzi, *Il commercio elettronico nella Società dell'Informazione* cit., pp. 53 ss.; G. Briganti, *Controversie nel commercio elettronico B2C: competenza giurisdizionale e legge applicabile*, 2004, disponibile nella sezione *Internet* degli e-book di *IusOnDemand*, www.iusondemand.com/ebook.

h) *ammissibilità delle comunicazioni commerciali non sollecitate per posta elettronica.*

Ai sensi dell'art. 5, comma 1, del decreto sul commercio elettronico, la libera circolazione di un determinato servizio della società dell'informazione proveniente da un altro Stato membro può inoltre essere *limitata, con provvedimento dell'autorità giudiziaria o degli organi amministrativi di vigilanza o delle autorità indipendenti di settore, per motivi di:*

a) ordine pubblico, per l'opera di prevenzione, investigazione, individuazione e perseguimento di reati, in particolare la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché contro la violazione della dignità umana;

b) tutela della salute pubblica;

c) pubblica sicurezza, compresa la salvaguardia della sicurezza e della difesa nazionale;

d) tutela dei consumatori, ivi compresi gli investitori.

I provvedimenti di cui sopra possono essere adottati solo se, nel caso concreto, siano (art. 5, comma 2):

a) necessari riguardo ad un determinato servizio della società dell'informazione lesivo degli obiettivi posti a tutela degli interessi pubblici di cui al comma 1 dell'art. 5, ovvero che costituisca un rischio serio e grave di pregiudizio agli stessi obiettivi;

b) proporzionati a tali obiettivi.

Fatti salvi i procedimenti giudiziari e gli atti compiuti nell'ambito di un'indagine penale, l'autorità competente, per il tramite del Ministero delle attività produttive ovvero l'autorità indipendente di settore, deve, *prima di adottare il provvedimento limitativo* (art. 5, comma 3):

a) chiedere allo Stato membro di cui al comma 1 dell'art. 5 di prendere provvedimenti e verificare che essi non sono stati presi o che erano inadeguati;

b) notificare alla Commissione europea e allo Stato membro di cui al comma 1 dell'art. 5, la sua intenzione di adottare tali provvedimenti. Dei provvedimenti adottati dalle autorità indipendenti, è data periodicamente comunicazione al Ministero competente.

In caso di *urgenza*, i soggetti di cui al comma 3 dell'art. 5 possono derogare a dette condizioni. I provvedimenti, in tal caso, sono notificati nel più breve tempo possibile alla Commissione e allo Stato membro, insieme ai motivi dell'urgenza (art. 5, comma 4).

[Sommaro](#)

5. Regime di stabilimento e di informazione

Ai sensi dell'art. 6 del provvedimento in esame, *l'accesso all'attività di un prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente* (principio dell'assenza di autorizzazione preventiva).

Secondo la relazione illustrativa, tale principio “costituisce quasi un postulato del principio di libera circolazione, ribadendo che il prestatore di servizi deve essere libero di accedere all'attività di fornitura di tali servizi in qualsiasi Stato membro,

senza necessità di autorizzazione preventiva nello Stato prescelto, essendo soggetto agli adempimenti amministrativi soltanto nello Stato di origine”.

Sono d'altra parte fatte salve *le disposizioni sui regimi di autorizzazione che non riguardano specificatamente ed esclusivamente i servizi della società dell'informazione o i regimi di autorizzazione nel settore dei servizi delle telecomunicazioni* di cui al decreto del Presidente della Repubblica 19 settembre 1997, n. 318, dalla cui applicazione sono esclusi i servizi della società dell'informazione (art. 6, comma 2)²¹.

La disposizione di cui all'art. 6, comma 1, appena esaminata, già in sede di commento della direttiva 2000/31/CE, ha dato luogo a qualche perplessità. Secondo una opinione, infatti, la presenza in Italia di un regime amministrativo contrasterebbe con quanto sancito dal provvedimento comunitario e, oggi, dal D.L.vo 70/2003²². Secondo altra opinione, “In realtà, la direttiva fa divieto agli Stati membri di introdurre delle autorizzazioni preventive (o altri atti amministrativi di analogo contenuto) relative *esclusivamente* all'impiego di un sito Internet per lo svolgimento di un'attività economica (per es. di commercio) ma ciò non significa che non trovino applicazione (o non possano essere introdotte *ex novo*) discipline concernenti i soggetti o le regole di svolgimento dell'attività. Non pare dubbio, allora, che il rispetto di quanto previsto dall'art. 18 del D.Lgs. n. 114/98 non sia messo in discussione dal D.Lgs. n. 70/2003” (E.M. Tripodi)²³.

²¹ D.P.R. 19 settembre 1997, n. 318, *Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni*, GU Serie gen. 221 del 22 settembre 1997, Suppl. ord.

²² F. Sarzana di Sant'Ippolito, *Approvata la direttiva sul commercio elettronico*, in *Corr. giur.*, 2000.

²³ E.M. Tripodi, *Commercio elettronico e contratti. Tre variazioni sul tema cit.*, il quale così prosegue: “Non si capirebbe infatti per quali motivi la vendita a distanza o su catalogo debba sottostare alla disciplina del commercio e non la stessa attività, quando, in luogo del catalogo cartaceo, si impieghi un sito Internet. Forse qualche riflessione andrebbe compiuta sulla validità del Modello COM 6-bis specificatamente predisposto per il commercio elettronico. Qualora si

Ciò posto, il successivo art. 7 del D.L.vo 70/2003 stabilisce le *informazioni generali obbligatorie* che devono essere fornite dal prestatore di un servizio della società dell'informazione.

La disposizione in parola prevede infatti che il prestatore, in aggiunta agli obblighi informativi previsti per specifici beni e servizi, *debba rendere facilmente accessibili, in modo diretto e permanente, ai destinatari del servizio* – come sopra definiti – *e alle Autorità competenti, le seguenti informazioni*²⁴:

- a) il nome, la denominazione o la ragione sociale;
- b) il domicilio o la sede legale;
- c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;

ritenga che non sia più conforme all'art. 6 del D.lgs. n. 70/2003, questo non significherebbe che il dettagliante *on line* risulterebbe *legibus soluto*, restando comunque tenuto alla presentazione del Modello COM 6, relative alle fattispecie ascritte all'art. 18 del D.Lgs. n. 114/98. I due modelli non essendo molto diversi tra loro lascerebbero immutato il risultato finale”.

Sull'art. 18 del D.L.vo 114/1998 v. nota n. 3.

²⁴ La norma si rivolge dunque ai *destinatari del servizio*, siano essi o meno *consumatori* (v. par. 3).

Deve ricordarsi anche quanto disposto per le società tenute all'iscrizione nel registro delle imprese dall'art. 2250 cod. civ. (“Indicazione negli atti e nella corrispondenza”):

“Negli atti e nella corrispondenza delle società soggette all'obbligo dell'iscrizione nel registro delle imprese devono essere indicati la sede della società e l'ufficio del registro delle imprese presso il quale questa è iscritta e il numero d'iscrizione.

Il capitale delle società per azioni, in accomandita per azioni e a responsabilità limitata deve essere negli atti e nella corrispondenza indicato secondo la somma effettivamente versata e quale risulta esistente dall'ultimo bilancio”.

Le società che operano sul Web sono tenute a rispettare i suddetti obblighi relativamente alle indicazioni da fornire sui propri siti agli utenti.

d) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese;

e) gli elementi di individuazione nonché gli estremi della competente autorità di vigilanza qualora un'attività sia soggetta a concessione, licenza od autorizzazione;

f) per quanto riguarda in particolare le *professioni regolamentate*, come definite dall'art. 2:

1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione;

2) il titolo professionale e lo Stato membro in cui è stato rilasciato;

3) il riferimento alle norme professionali e agli eventuali codici di condotta vigenti nello Stato membro di stabilimento e le modalità di consultazione dei medesimi;

g) il numero della partita IVA o altro numero di identificazione considerato equivalente nello Stato membro, qualora il prestatore eserciti un'attività soggetta ad imposta;

h) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;

i) l'indicazione delle attività consentite al consumatore e al destinatario del servizio e gli estremi del contratto qualora un'attività sia soggetta ad autorizzazione o l'oggetto della prestazione sia fornito sulla base di un contratto di

licenza d'uso.

Si specifica altresì che il prestatore è tenuto a *mantenere aggiornate le informazioni di cui sopra* (art. 7, comma 2)²⁵.

In considerazione delle incertezze sorte in proposito, il decreto dispone infine, espressamente, che la *registrazione della testata editoriale telematica è obbligatoria esclusivamente per le attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze previste dalla legge 7 marzo 2001, n. 62* (art. 7, comma 3)²⁶.

Si segnala sin d'ora che, come si vedrà meglio in seguito, la violazione dell'art. 7 appena illustrato, qualora il fatto non costituisca reato, comporta l'applicazione della sanzione amministrativa pecuniaria di cui all'art. 21 del provvedimento.

[Sommaro](#)

6. Comunicazioni commerciali e spamming

²⁵ Ciò affinché gli obblighi informativi previsti possano trovare corretta attuazione, in considerazione anche di quanto disposto dagli artt. 1337 e 1338 cod. civ.

²⁶ Legge 7 marzo 2001, n. 62, *Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n. 416*, GU Serie gen. 67 del 21 marzo 2001.

Critico sulla disposizione dell'art. 7, comma 3, è G. Scorza, "*Testata editoriale telematica*": *le sviste del legislatore* cit., secondo cui "la disposizione – frutto di un cattivo 'suggerimento' del legislatore delegante prontamente raccolto dall'esecutivo – è infatti caratterizzata da una concentrazione di errori e sviste linguistiche prima ancora che giuridiche". Si veda anche E.M. Tripodi, *Commercio elettronico e contratti. Tre variazioni sul tema* cit., secondo cui: "Non è punto chiaro a quale registro si faccia riferimento tra quello della stampa tenuto presso i tribunali ed il Registro degli operatori della comunicazione (meglio noto come 'ROC') tenuto dall'Autorità per le garanzie nelle comunicazioni".

V. infine F. Abruzzo, *Testate on-line: analisi sulla obbligatorietà della registrazione al tribunale ed al ROC*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=5186.

Gli artt. 8, 9 e 10 del decreto in commento si occupano di comunicazioni commerciali e di spamming.

Come si vedrà meglio, alla violazione delle suddette disposizioni l'art. 21 fa conseguire, anche in questo caso, l'applicazione di una sanzione amministrativa pecuniaria ove il fatto non costituisca reato²⁷.

Comunicazioni commerciali.

Il provvedimento sul commercio elettronico, in aggiunta agli obblighi informativi previsti per specifici beni e servizi ed alle informazioni generali obbligatorie illustrate, pone inoltre, all'art. 8, specifici *obblighi di informazione* con riguardo alle *comunicazioni commerciali*, come sopra definite²⁸.

Le comunicazioni commerciali che costituiscono un servizio della società dell'informazione o che di esso siano parte integrante, devono infatti contenere, sin dal primo invio, in modo chiaro ed inequivocabile, una specifica informativa, diretta ad evidenziare:

- a) che si tratta di comunicazione commerciale;
- b) la persona fisica o giuridica per conto della quale è effettuata la comunicazione commerciale;

²⁷ V. par. 10.

²⁸ Per un approfondimento sulla disciplina riservata dalla direttiva europea sul commercio elettronico alle comunicazioni commerciali, si veda G. Briganti, *Le comunicazioni commerciali nella società dell'informazione*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/comunicazioni2.htm.

La comunicazione promozionale via Internet soggiace naturalmente anche alle norme dell'ordinamento italiano riguardanti la comunicazione pubblicitaria in generale. Si veda A. Stazi, *La comunicazione promozionale via Internet: le sue principali modalità e normative applicabili*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/stazi1.html.

c) che si tratta di un'offerta promozionale come sconti, premi, o omaggi e le relative condizioni di accesso;

d) che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione.

Comunicazioni commerciali non sollecitate.

Viene altresì disciplinata dal decreto in esame quella particolare categoria di comunicazioni commerciali costituita dalle *comunicazioni commerciali non sollecitate (spamming)*.

L'art. 9, comma 1, sancisce infatti che tale genere di comunicazioni, *trasmesse da un prestatore per posta elettronica devono, in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al loro ricevimento per il futuro.*

Sono d'altra parte fatti espressamente salvi gli obblighi previsti in materia dal [D.L.vo 185/1999](#) e dal [D.L.vo 171/1998](#) – oggi art. 130 [Codice privacy](#) – che, come visto nel precedente capitolo, regolano in ambiti diversi la questione del *consenso all'invio* di comunicazioni commerciali²⁹. Le disposizioni relative ai contratti a distanza conclusi dai consumatori e alle comunicazioni indesiderate dovranno dunque essere applicate, nel rispettivo ambito, *congiuntamente* a quelle ora in esame.

Occorre ricordare in proposito che un primo schema del provvedimento in parola prevedeva l'istituzione di un *registro nazionale* presso gli uffici del Garante per la

²⁹ V. cap. III, parr. 11 e ss.

protezione dei dati personali; registro nel quale avrebbero potuto iscriversi i soggetti che non si fossero dichiarati contrari a ricevere e-mail commerciali e che avrebbe dovuto dunque essere consultato dalle società che operano in Internet prima di inviare comunicazioni promozionali.

L'istituzione di un siffatto registro è stata però oggetto di parere sfavorevole del Garante, il quale ha rilevato che essa sarebbe stata innanzitutto "fuori delega".

Infatti, dice il Garante nel suo parere, "sia in base all'espressa disposizione della direttiva europea sul commercio elettronico, sia in base ai riferimenti contenuti nella legge delega [legge comunitaria 2001], il legislatore italiano non ha 'competenza' ad introdurre disposizioni che incidano sul trattamento dei dati personali nell'ambito della disciplina riguardante il commercio elettronico.

L'Italia, come altri Paesi, poi, ha da tempo introdotto la regola secondo cui le comunicazioni on-line commerciali o pubblicitarie richiedono il consenso preventivo del destinatario, piuttosto che la successiva opposizione ad ulteriori invii (opt out).

Tale sistema basato sul cosiddetto 'opt in', già in vigore in cinque Paesi europei, è stato prescelto quest'anno come regola comune a livello comunitario ed è ora 'obbligatorio' per i Paesi membri dell'Unione europea, a seguito della recente adozione della direttiva 2002/58/CE sulle comunicazioni elettroniche"³⁰.

³⁰ Pertanto, solo in sede di recepimento della direttiva 2002/58/CE, prosegue il Garante nel suo parere, "potranno prevedersi disposizioni più articolate, mentre lo schema attuale di decreto legislativo sul commercio elettronico potrebbe, al massimo, rinviare alle disposizioni nazionali sulla privacy.

Il sistema ipotizzato nei primi lavori preparatori sul commercio elettronico imporrebbe, quindi, un inutile obbligo di consultare il registro da parte di chiunque desidera inviare e-mail commerciali ovvero di milioni di persone, non potendo incidere sulle norme vigenti che impongono alle società di raccogliere il preventivo consenso informato del destinatario.

Con il testo definitivo del decreto sul commercio elettronico il legislatore italiano ha dunque rinunciato all'istituzione di un simile registro nazionale³¹.

La formulazione dell'art. 9, comma 1, D.L.vo 70/2003 ha indotto taluno a ritenere che il legislatore abbia inteso prevedere un regime di *opt-out* per le *comunicazioni commerciali* inviate tramite *e-mail*³².

A parere di chi scrive, come già rilevato, occorre tener presente che il D.L.vo 70/2003, in attuazione della corrispondente disposizione della direttiva 2000/31/CE, fa espressamente salva l'applicazione in materia di *consenso all'invio* di comunicazioni commerciali via e-mail sia dell'art. 130 del Codice della privacy sia dell'art. 10 D.L.vo 185/1999. La disciplina del consenso all'invio di simili messaggi di posta elettronica deve pertanto essere ricercata nelle disposizioni da ultimo citate³³, le quali, come ampiamente illustrato nel capitolo

Oltre a queste contraddizioni, il Garante evidenzia anche insuperabili difficoltà di realizzazione del meccanismo proposto.

Difficoltà di aggiornamento, praticamente quotidiano, e di consultazione imporrebbero ingenti oneri finanziari, sia sotto il profilo delle spese da sostenere per la gestione del sistema, sia per le risorse umane da dedicare al suo funzionamento, tali da renderlo da subito del tutto ingestibile”.

Garante per la protezione dei dati personali, *Newsletter* 28 ottobre – 3 novembre 2002, www.garanteprivacy.it.

³¹ In tema di spamming, il legislatore non ha poi accolto l'osservazione formulata dalla X Commissione parlamentare nel parere più volte citato, in cui si legge quanto segue:

“d) in relazione a quanto disposto dall'articolo 9, che disciplina le comunicazioni commerciali non sollecitate, appare opportuno prevedere sistemi di filtraggio delle informazioni da parte delle imprese, in conformità a quanto previsto dall'articolo 31, comma 1, lettera b), della legge di delega”.

³² Cfr. C. Blengino e M.A. Senor, *Lo spamming a fini di profitto non costituisce reato* cit.; A. Lisi, *Tutela della privacy in Internet* cit., pp. 71 ss.; L. Pulito, *Spamming: profili penali e prospettive future* cit.; L. Lecchi, *La disciplina delle comunicazioni commerciali secondo il d.lgs. 70/03*, in *Penale.it*, www.penale.it, www.penale.it/lecchi.pdf.

³³ Si ricorda inoltre che dal campo di applicazione del D.L.vo 70/2003 sono espressamente escluse le questioni “relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel

precedente³⁴, con riferimento a siffatti messaggi prevedono un regime di *opt-in* (salvo quanto previsto dall'art. 130, comma 4).

Ciò posto, l'art. 9, comma 1, D.L.vo 70/2003 dove stabilisce che le e-mail di carattere commerciale devono recare "l'indicazione che il destinatario del messaggio può opporsi al loro ricevimento per il futuro" deve intendersi riferito esclusivamente ai casi in cui l'ordinamento, in deroga ai principi di cui all'art. 130 del Codice della privacy e all'art. 10 D.L.vo 185/1999, ammette ancora oggi l'invio di e-mail pubblicitarie a prescindere dal consenso del destinatario, vale a dire in regime di *opt-out*. L'unico caso allo stato ammesso pare d'altra parte essere quello contemplato dall'art. 130, comma 4, del Codice della privacy, concernente le coordinate di posta elettronica già acquisite dal titolare del trattamento nel contesto della vendita di un prodotto o di un servizio.

Proprio l'art. 130, comma 4, contiene con riferimento alla predetta ipotesi una disposizione del tutto analoga a quella di cui all'art. 9 D.L.vo 70/2003 allorché dice che "L'interessato, al momento della raccolta e in occasione dell'invio di

settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675 e al decreto legislativo 13 maggio 1998, n. 171 e successive modificazioni" (art. 1). Il Codice della privacy è stato d'altra parte emanato successivamente al D.L.vo 70/2003.

Si ricorda altresì il considerando 14 della direttiva 2000/31/CE, secondo cui la *protezione dei singoli relativamente al trattamento dei dati personali* è disciplinata *unicamente* dalla 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 [attuata in Italia con il *Codice della privacy*], e dalla 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 [attuata in Italia con il D.L.vo 171/1998 e oggi sostituita, in forza della direttiva 2002/58/CE, dal *Codice della privacy*], che sono *integralmente applicabili ai servizi della società dell'informazione*.

Dette direttive, prosegue il considerando 14, già istituiscono un quadro giuridico comunitario nel campo della protezione dei dati personali e pertanto non è necessario includere tale aspetto nella direttiva sul commercio elettronico per assicurare il buon funzionamento del mercato interno, in particolare la libera circolazione dei dati personali tra gli Stati membri. L'applicazione della direttiva 2000/31/CE deve dunque essere pienamente conforme ai principi relativi alla protezione dei dati personali, *in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari*.

³⁴ Cap. III, parr. 11 e ss.

ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente”.

Così argomentando, si deve giungere a ritenere che l'intero art. 9, comma 1, D.L.vo 70/2003 può trovare applicazione, allo stato, *solo* in relazione alla ipotesi di *opt-out* di cui all'art. 130, comma 4, del Codice della privacy.

Questa sembra d'altro canto essere la volontà del legislatore comunitario il quale, con l'art. 7 della direttiva 2000/31/CE³⁵, ha inteso disciplinare solamente *i casi in cui gli Stati membri permettono comunicazioni commerciali non sollecitate per posta elettronica*, ovvero sia i casi in cui gli Stati prevedono un regime di *opt-out*, senza voler incidere sul diverso regime di *opt-in* previsto oggi in via generale dalla direttiva 2002/58/CE.

Recita infatti espressamente il considerando 30 della direttiva 2000/31/CE che “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”; il considerando 31 aggiunge che “Gli Stati membri che consentono l'invio per via elettronica, da parte di prestatori stabiliti nel loro territorio, di comunicazioni commerciali non sollecitate senza previo consenso del destinatario devono garantire che i prestatori

³⁵ L'art. 7 (“Comunicazione commerciale non sollecitata”) della direttiva sul commercio elettronico così dispone:

“1. Oltre agli altri obblighi posti dal diritto comunitario, gli Stati membri che permettono comunicazioni commerciali non sollecitate per posta elettronica provvedono affinché tali comunicazioni commerciali trasmesse da un prestatore stabilito nel loro territorio siano identificabili come tali, in modo chiaro e inequivocabile, fin dal momento in cui il destinatario le riceve.

2. Fatte salve la direttiva 97/7/CE e la direttiva 97/66/CE, gli Stati membri adottano i provvedimenti necessari per far sì che i prestatori che inviano per posta elettronica comunicazioni commerciali non sollecitate consultino regolarmente e rispettino i registri negativi in cui possono iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni commerciali”.

consultino periodicamente e rispettino i registri negativi in cui possono iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni commerciali”.

Evidentemente, la direttiva 2000/31/CE presuppone che siano *altre* le fonti che disciplinano la questione del consenso all’invio.

In conclusione, sembra dunque ragionevole ritenere che l’art. 9, comma 1, D.L.vo 70/2003 possa essere applicato solo nei confronti di *e-mail di carattere commerciale legittimamente inviate senza previo consenso informato del destinatario*. Unico caso allo stato previsto, come rilevato, pare essere quello di cui all’art. 130, comma 4, del Codice della privacy.

Le e-mail inviate in conformità del regime di *opt-in* di cui all’art. 130 del Codice della privacy e all’art. 10 D.L.vo 185/1999 non sono pertanto soggette alla disposizione in esame. Per esse, come si è visto, l’art. 130, entro il suo ambito applicativo, prevede comunque il divieto di invio effettuato “camuffando o celando l’identità del mittente o senza fornire un idoneo recapito presso il quale l’interessato possa esercitare i diritti di cui all’articolo 7”.

Un obbligo di rendere *identificabile come tale* la comunicazione commerciale desiderata (o sollecitata) in virtù di previo consenso informato dell’interessato deriva in ogni caso dall’art. 8 D.L.vo 70/2003, applicabile, come sopra visto, ad ogni genere di comunicazione commerciale. D’altra parte, l’interessato sarà messo al corrente della possibilità di *opporsi* al ricevimento di siffatte e-mail per il futuro, ai sensi dell’art. 7 del Codice della privacy, tramite l’informativa che gli dovrà essere resa, prima dell’acquisizione del consenso, *ex art. 13 del testo unico*. Sebbene non espressamente previsto, infine, sarà bene comunque ripetere detta informazione circa il diritto di opposizione ad ogni invio, anche in considerazione dell’art. 11 del Codice.

In tema di spamming, il D.L.vo 70/2003 stabilisce inoltre, in favore del

destinatario dei messaggi, che *la prova del carattere sollecitato delle comunicazioni commerciali è onere del prestatore del servizio* (art. 9, comma 2). Sarà dunque compito del prestatore di un servizio della società dell'informazione quello di dimostrare nel corso di un eventuale procedimento di aver acquisito il previo consenso informato dell'interessato; consenso che, come già rilevato, deve essere documentato per iscritto³⁶.

Comunicazioni commerciali nelle professioni regolamentate.

Viene infine dettata una disposizione specifica circa *l'uso delle comunicazioni commerciali nelle professioni regolamentate*, come sopra definite: *l'impiego di comunicazioni commerciali che costituiscono un servizio della società dell'informazione o che di esso sono parte, fornite da chi esercita una professione regolamentata, deve essere conforme alle regole di deontologia professionale e in particolare, all'indipendenza, alla dignità, all'onore della professione, al segreto professionale e alla lealtà verso clienti e colleghi* (art. 10)³⁷.

Con riguardo in particolare alla *professione forense*, si ricorda che in data 26 ottobre 2002 il Consiglio Nazionale Forense ha introdotto nuove regole in materia di *pubblicità informativa dell'avvocato*, modificando l'art. 17 del vigente Codice deontologico.

³⁶ V. cap. II, par. 7.

³⁷ Con riferimento all'art. 10, nel parere espresso dalla X Commissione parlamentare sullo schema di decreto di attuazione si legge quanto segue:

“e) con riferimento all'articolo 10, relativo all'uso delle comunicazioni commerciali nelle professioni regolamentate, si valuti l'opportunità di prevedere forme e procedure di consultazione con gli ordini professionali, secondo quanto stabilito dall'articolo 31, comma 1, lettera c), della legge di delega”.

Sull'uso delle comunicazioni commerciali nelle professioni regolamentate si veda anche G. Briganti, *Le comunicazioni commerciali nella società dell'informazione* cit., par. 5.

Il nuovo testo della disposizione citata (“Informazioni sull'esercizio professionale”) consente all'avvocato di dare informazioni sulla propria attività professionale, secondo correttezza e verità, nel rispetto della dignità e del decoro della professione e degli obblighi di segretezza e riservatezza.

Quanto ai mezzi di informazione, prosegue l'art. 17, devono ritenersi consentiti, per quel che qui interessa:

- le brochures informative inviate anche a mezzo posta a soggetti determinati;
- gli annuari professionali, le rubriche, le riviste giuridiche, i repertori e i bollettini con informazioni giuridiche;
- i rapporti con la stampa (secondo quanto stabilito dall'art. 18 del Codice deontologico);
- i siti web e le reti telematiche (Internet), purché propri dell'avvocato o di studi legali associati o di società di avvocati, nei limiti della informazione, e previa segnalazione al Consiglio dell'ordine. Con riferimento ai siti già esistenti l'avvocato è tenuto a procedere alla segnalazione al Consiglio dell'ordine di appartenenza entro 120 giorni.

Devono al contrario ritenersi vietati, tra l'altro, i giornali e gli annunci pubblicitari in genere; i mezzi di divulgazione anomali e contrari al decoro; le sponsorizzazioni; le telefonate di presentazione e le visite a domicilio non specificatamente richieste; l'utilizzazione di Internet per offerta di servizi e consulenze gratuite, in proprio o su siti di terzi.

Quanto ai contenuti della informazione, il nuovo testo dell'art. 17 del Codice deontologico forense consente l'indicazione dei seguenti dati:

- i dati personali necessari (nomi, indirizzi, anche web, numeri di telefono e fax e indirizzi di posta elettronica, dati di nascita e di formazione del professionista, fotografie, lingue conosciute, articoli e libri pubblicati, attività didattica, onorificenze, e quant'altro relativo alla persona, limitatamente a ciò che attiene all'attività professionale esercitata);
- le informazioni dello studio (composizione, nome dei fondatori anche defunti, attività prevalenti svolte, numero degli addetti, sedi secondarie, orari di apertura);
- l'indicazione di un logo;
- l'indicazione della certificazione di qualità (l'avvocato che intenda fare menzione di una certificazione di qualità deve depositare presso il Consiglio dell'ordine il giustificativo della certificazione in corso di validità e l'indicazione completa del certificatore e del campo di applicazione della certificazione ufficialmente riconosciuta dallo Stato).

In particolare, è *espressamente consentita l'utilizzazione della rete Internet e del sito web per l'offerta di consulenza*, nel rispetto dei seguenti obblighi:

- indicazione dei dati anagrafici, partita Iva e Consiglio dell'ordine di appartenenza;
- impegno espressamente dichiarato al rispetto del Codice deontologico, con la riproduzione del testo, ovvero con la precisazione dei modi o mezzi per consentirne il reperimento o la consultazione;
- indicazione della persona responsabile;
- specificazione degli estremi della eventuale polizza assicurativa, con copertura riferita anche alle prestazioni on-line e indicazione dei massimali;

- indicazione delle vigenti tariffe professionali per la determinazione dei corrispettivi.

È vietata invece l'indicazione di dati che riguardano terze persone; dei nomi dei clienti (il divieto deve ritenersi sussistente anche con il consenso dei clienti); delle specializzazioni (salvo le specifiche ipotesi previste dalla legge); dei prezzi delle singole prestazioni (è vietato pubblicare l'annuncio che la prima consultazione è gratuita); delle percentuali delle cause vinte o l'esaltazione dei meriti; del fatturato individuale o dello studio; di promesse di recupero; di offerte comunque di servizi (in relazione a quanto disposto dall'art. 19 del Codice deontologico forense)³⁸.

L'avvocato, per non incorrere nelle sanzioni previste dal D.L.vo 70/2003 per la violazione del suo art. 10, sopra esaminato, dovrà dunque conformarsi alle regole di cui al novellato art. 17 del Codice deontologico forense³⁹.

Sommario

³⁸ Con delibera del 28/11/2003, l'Ordine degli Avvocati di Pistoia ha fornito le sue precisazioni sul nuovo testo dell'art. 17 del Codice deontologico forense. Con riferimento alla Rete, in particolare, l'Ordine ha puntualizzato che deve ritenersi vietato l'inserimento di pubblicità, anche di terzi, sul sito web dell'avvocato nonché la consulenza prestata tramite siti gestiti da terzi (società di servizi, associazioni ecc.). Il testo della delibera può essere consultato su www.altalex.com all'indirizzo www.altalex.com/index.php?idnot=1038.

Sull'avvocato in Internet si veda C. Giurdanella, *Lo studio legale on line*, Napoli, Ed. Simone, 2003.

In tema di *consulenze professionali on-line* si segnala anche quanto affermato dal Garante per la protezione dei dati personali in occasione della concessione di una autorizzazione, con la quale sono stati definiti limiti e garanzie per il trattamento di dati, anche sensibili, connessi allo svolgimento di attività di consulenza on-line. Si veda la *Newsletter* del Garante, 1-7 dicembre 2003, n. 194, www.garanteprivacy.it.

³⁹ Ciò per evitare, altresì, di incorrere in *sanzioni disciplinari* dovute alla violazione del medesimo art. 17. Anche l'avvocato, inoltre, è soggetto alle prescrizioni relative all'invio di comunicazioni elettroniche indesiderate sin qui esaminate, nonché a tutti gli obblighi informativi posti dal provvedimento in esame.

7. Informazioni dirette alla conclusione del contratto e inoltro dell'ordine

Proseguendo nell'analisi delle norme introdotte nell'ordinamento giuridico italiano dal D.L.vo 70/2003 di attuazione della direttiva europea sul commercio elettronico, occorre prendere ora in esame le disposizioni di cui agli artt. 12 (informazioni dirette alla conclusione del contratto) e 13 (inoltro dell'ordine) del provvedimento.

Con riguardo alla conclusione dei contratti del commercio elettronico⁴⁰, l'art. 12, comma 1, prevede che, oltre agli obblighi informativi previsti per specifici beni e servizi nonché a quelli stabiliti dall'art. 3 del [D.L.vo 185/1999](#)⁴¹, il *prestatore di*

⁴⁰ “Un accordo negoziale si dice ‘contratto *on line*’ quando per la sua conclusione, tutte le parti, o una di esse, abbiano utilizzato una delle modalità legata ai protocolli tecnici di trasmissione telematica di dati (tali sono quelli utilizzati da Internet)”, P. Parigi, *Contratti on line*, in *INTERNET. Nuovi problemi e questioni controverse* cit., p. 103.

“Sulla conclusione del contratto *on line*” – osserva E.M. Tripodi, *Commercio elettronico e contratti. Tre variazioni sul tema* cit. con riferimento alla norma che ci si appresta ad esaminare – “lo spazio di questo contributo non sarebbe sufficiente neppure per articolare una premessa date le complicazioni che, immediatamente, sorgerebbero a causa di una serie di disposizioni che scontano un evidente compromesso tra i principi di *common law* e quelli di *civil law* che governano la dinamica negoziale. A ciò si aggiunga l'impiego di una terminologia sciatta e senza un preciso significato tecnico giuridico. Il riferimento va, ovviamente, al termine ‘ordine’, ovvero all'atto di ‘accusare ricevuta’ che sembra tratta di peso da formule contrattuali consegnate ad un gergo giuridicamente ben poco raffinato”.

⁴¹ Si riporta il testo dell'art. 3 del D.L.vo 185/1999:

“3. (*Informazioni per il consumatore*). 1. In tempo utile, prima della conclusione di qualsiasi contratto a distanza, il consumatore deve ricevere le seguenti informazioni:

- a) identità del fornitore e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del fornitore;
- b) caratteristiche essenziali del bene o del servizio;
- c) prezzo del bene o del servizio, comprese tutte le tasse o le imposte;
- d) spese di consegna;

*un servizio della società dell'informazione, salvo diverso accordo tra parti che non siano consumatori, debba fornire in modo chiaro, comprensibile ed inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario del servizio, le seguenti informazioni*⁴²:

a) le varie fasi tecniche da seguire per la conclusione del contratto;

e) modalità del pagamento, della consegna del bene o della prestazione del servizio e di ogni altra forma di esecuzione del contratto;

f) esistenza del diritto di recesso o di esclusione dello stesso ai sensi dell'articolo 5, comma 3;

g) modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

h) costo dell'utilizzo della tecnica di comunicazione a distanza, quando è calcolato su una base diversa dalla tariffa di base;

i) durata della validità dell'offerta e del prezzo;

j) durata minima del contratto in caso di contratti per la fornitura di prodotti o la prestazione di servizi ad esecuzione continuata o periodica.

2. Le informazioni di cui al comma 1, il cui scopo commerciale deve essere inequivocabile, devono essere fornite in modo chiaro e comprensibile, con ogni mezzo adeguato alla tecnica di comunicazione a distanza impiegata, osservando in particolare i principi di buona fede e di lealtà in materia di transazioni commerciali, valutati alla stregua delle esigenze di protezione delle categorie di consumatori particolarmente vulnerabili.

3. In caso di comunicazioni telefoniche, l'identità del fornitore e lo scopo commerciale della telefonata devono essere dichiarati in modo inequivocabile all'inizio della conversazione con il consumatore, a pena di nullità del contratto.

4. Nel caso di utilizzazione di tecniche che consentono una comunicazione individuale, le informazioni di cui al comma 1 sono fornite, ove il consumatore lo richieda, in lingua italiana. In tal caso, sono fornite nella stessa lingua anche la conferma e le ulteriori informazioni di cui all'articolo 4⁷.

La violazione dell'art. 3 del D.L.vo 185/1999 è punita con una sanzione amministrativa pecuniaria dall'art. 12 del provvedimento.

Giova ricordare inoltre che anche per i contratti on-line concernenti "beni di consumo" trovano applicazione gli artt. 1519*bis* e ss. cod. civ. recentemente introdotti in attuazione della direttiva 1999/44/CE (D.L.vo 2 febbraio 2002, n. 24, *Attuazione della direttiva 1999/44/CE su taluni aspetti della vendita e delle garanzie di consumo*, GU 57 dell'8 marzo 2002, Suppl. ord.).

⁴² Le informazioni di cui all'art. 12 del provvedimento in esame vanno ad aggiungersi a quelle generali obbligatorie che devono essere fornite da un qualunque prestatore di un servizio della società dell'informazione ai sensi dell'art. 7 del medesimo decreto. Si veda in proposito il par. 5.

- b) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;
- c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore;
- d) gli eventuali codici di condotta⁴³ cui aderisce e come accedervi per via telematica;
- e) le lingue a disposizione per concludere il contratto oltre all'italiano;
- f) l'indicazione degli strumenti di composizione delle controversie⁴⁴.

Quanto sopra *non è applicabile ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti* (art. 12, comma 2).

Si prevede altresì che le *clausole e le condizioni generali del contratto proposte al destinatario debbano essere messe a sua disposizione in modo che gli sia consentita la memorizzazione e la riproduzione* (art. 12, comma 3)⁴⁵.

La violazione degli obblighi di cui all'art. 12 appena esaminato comporta l'applicazione della sanzione amministrativa pecuniaria di cui all'art. 21 del

⁴³ Sui *codici di condotta* nel commercio elettronico si veda *infra*, par. 9.

⁴⁴ Sulla *composizione delle controversie* nel commercio elettronico si veda *infra*, par. 9.

⁴⁵ V. M.C. Raiola, *Considerazioni sull'efficacia delle clausole vessatorie nell'e-commerce*, in *Il Commercio via Internet* cit., pp. 96 ss.

Si veda anche quanto segue nel testo a proposito dell'art. 13, comma 1, del provvedimento.

provvedimento⁴⁶.

Ai sensi dell'art. 13, comma 1, del D.L.vo 70/2003, *le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica.*

La disposizione, limitandosi ad un generico rinvio alle “norme sulla conclusione dei contratti”, non risolve i rilevanti problemi legati alla *formazione dell'accordo telematico*⁴⁷.

Vale la pena dunque richiamare a questo proposito quanto imposto agli Stati membri dall'art. 9, par. 1, della direttiva 2000/31/CE, secondo cui “Gli Stati membri provvedono affinché il loro ordinamento giuridico renda possibili i contratti per via elettronica. Essi, in particolare, assicurano a che la normativa relativa alla formazione del contratto non osti all'uso effettivo dei contratti elettronici e non li privi di efficacia e validità in quanto stipulati per via elettronica”.

Il considerando 34 della direttiva recita inoltre che “Gli Stati membri dovrebbero adeguare le parti della propria legislazione relative soprattutto ai requisiti di forma che potrebbero ostacolare il ricorso ai contratti per via elettronica. L'esame delle legislazioni che richiedono tale adeguamento dovrebbe essere sistematico e

⁴⁶ V. par. 10.

⁴⁷ In argomento si veda M. Rosciano, *La conclusione del contratto telematico: tutela attuale e prospettive future. Verso una nuova dimensione della contrattazione*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit. pp. 559 ss.; P. Parigi, *Contratti on line* cit.; M. Morelli, *Contratti telematici e crisi dell'accordo: i contratti “point and click”*, in *Informatica Giuridica*, a c. di G. Rognetta, Napoli, Ed. Simone, 2001, pp. 189 ss.; E. Ruggiero, *Il contratto telematico*, Napoli, Ed. Simone, 2003; F. Sarzana di Sant'Ippolito, *I contratti di Internet e del commercio elettronico*, Milano, Giuffrè, 2001; A.R. Sirotti Gaudenzi, *L'imprenditore in Rete e i contratti telematici*, in *Notiziario Giuridico Telematico*, www.notiziariogiuridico.it, www.notiziariogiuridico.it/sirotti_gaudenzi_commercioel.html.

comprendere tutte le fasi e gli atti necessari alla formazione del contratto, compresa l'archiviazione del medesimo. Il risultato di tale adeguamento dovrebbe rendere possibili i contratti per via elettronica. L'effetto giuridico delle firme elettroniche è disciplinato dalla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa a regole comunitarie sulle firme elettroniche⁴⁸.

Ai sensi dell'art. 13, comma 2, del provvedimento in esame, *salvo differente accordo tra parti diverse dai consumatori, il prestatore deve altresì, senza ingiustificato ritardo e per via telematica, accusare ricevuta dell'ordine del destinatario.*

Detta ricevuta deve contenere un riepilogo delle condizioni generali e particolari applicabili al contratto, le informazioni relative alle caratteristiche essenziali del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili.

L'ordine e la ricevuta si considerano pervenuti quando le parti alle quali sono

⁴⁸ La direttiva europea sulle firme elettroniche è stata recepita in Italia con il [D.L.vo 23 gennaio 2002, n. 10](#), *Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche* (GU del 15 febbraio 2002, n. 39).

In argomento si veda G. Briganti, *Le firme elettroniche* cit.; A. Lisi e A.R. Sirotti Gaudenzi, *Il documento informatico nel commercio elettronico nazionale e internazionale*, in *Internet Law Digest*, www.internet-law-digest.org, www.internet-law-digest.org/show_document.php?document_id=000000004&PHPSESSID=7af7c049aed261f32c7f7a8037fb3989.

Con riferimento alla materia delle firme elettroniche, si ricorda in particolare l'avvenuta pubblicazione del "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10" (DPR 7 aprile 2003, n. 137, GU 138 del 17 giugno 2003), il quale ha sollevato delicate questioni. Il testo del provvedimento può essere consultato su www.iusreporter.it all'indirizzo www.iusreporter.it/Testi/dpr137-2003.htm.

Si veda anche l'*Osservatorio* di www.iusreporter.it dedicato all'argomento all'indirizzo www.iusreporter.it/Testi/firmeelettroniche.htm.

indirizzati hanno la possibilità di accedervi (art. 13, comma 3)⁴⁹.

Le disposizioni di cui ai commi 2 e 3 dell'art. 13, appena illustrate, *non si applicano ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti* (art. 13, comma 4).

Deve rilevarsi inoltre come la violazione dell'art. 13 *non* comporti l'applicazione della sanzione amministrativa pecuniaria di cui all'art. 21 del provvedimento.

Occorre infine ricordare che, ai sensi dell'art. 11, il decreto sul commercio elettronico *non si applica* a:

- a) contratti che istituiscono o trasferiscono diritti relativi a beni immobili, diversi da quelli in materia di locazione;
- b) contratti che richiedono per legge l'intervento di organi giurisdizionali, pubblici poteri o professioni che implicano l'esercizio di pubblici poteri;
- c) contratti di fideiussione o di garanzie prestate da persone che agiscono a fini che esulano dalle loro attività commerciali, imprenditoriali o professionali;
- d) contratti disciplinati dal diritto di famiglia o di successione.

L'art. 9 della direttiva europea sul commercio elettronico prevedeva la semplice *facoltà* per gli Stati membri di stabilire dette esclusioni.

⁴⁹ Non si richiede cioè che l'ordine e la ricevuta siano visualizzati per via elettronica rispettivamente dal prestatore e dal destinatario del servizio, sarà infatti sufficiente che l'e-mail raggiunga il gestore del servizio della parte a cui è indirizzato il messaggio e che, quindi, il destinatario del messaggio sia in grado di accedervi tramite la propria casella di posta elettronica (in analogia a quanto previsto dall'art. 1335 cod. civ.).

Sommario

8. Responsabilità dei prestatori intermediari (provider)

Il *prestatore intermediario (provider)*, come può leggersi nella relazione illustrativa che accompagna il decreto legislativo in esame, è “il soggetto che esercita un’attività imprenditoriale di prestatore di servizi della società dell’informazione offrendo servizi di connessione, trasmissione ed immagazzinamento dei dati, ovvero ospitando un sito sulle proprie apparecchiature”.

Il codice di deontologia e di buona condotta adottato dall’Associazione Nazionale Fornitori di Videoaudioinformazione (ANFOV)⁵⁰ distingue tre tipologie di provider:

- *fornitore di accesso (access provider)*: il soggetto che offre al pubblico l’accesso ad una rete;
- *fornitore di servizi (service provider)*: il soggetto che offre al pubblico servizi di comunicazione e/o di trattamento delle informazioni destinati al pubblico, oppure ad utenti e abbonati;
- *fornitore di contenuti (content provider)*: il soggetto che offre al pubblico informazioni che transitano sulla rete telematica e destinate al pubblico, oppure ad utenti e abbonati⁵¹.

⁵⁰ Consultabile su www.anfov.it all’indirizzo http://www.anfov.it/associazione/codice_tit1.html.

⁵¹ Gli *usi degli Internet Providers* sono stati raccolti dalla Camera di Commercio di Milano con deliberazione del 23/07/2001, n. 258.

“Con la generica qualifica di *provider* si fa generalmente riferimento ad una pluralità di soggetti che rientrano nella categoria degli operatori che la direttiva 2000/31/Ce definisce ‘prestatori di servizi della società dell’informazione’. Ai fini della presente riflessione, le diverse tipologie di *provider* devono essere tenute ben distinte. E ciò in quanto, mentre l’*access provider* fornisce agli utenti la connessione alla rete, il *service provider* fornisce servizi ulteriori (caselle *e-mail*, *chatroom*, *forum* telematici, *newsgoup*, motori di ricerca, gestione di banche dati, e bacheche elettroniche in cui gli utenti possono pubblicare i propri materiali e quant’altro), ed il *content provider* veicola in rete, tramite il suo sito, propri contenuti (notizie di cronaca, ricette di cucina, fotografie d’autore, sentenza della Suprema Corte di Cassazione, racconti, barzellette, etc.). L’*Host provider*, infine, è un *service provider* che mette a disposizione uno spazio del disco rigido del proprio *server* per ‘ospitare’ i siti creati da utenti che desiderano svolgere il ruolo di *service* o *content provider* pur non avendo a disposizione le necessarie tecnologie. È bene chiarire che a queste figure di intermediari si deve aggiungere quella del c.d. *maintener*, il quale non è un vero e proprio *provider*, in quanto non è un intermediario di Internet, bensì un operatore che interagisce burocraticamente e tecnicamente, per conto di un *provider* che intende ‘aprire’ un sito web, con gli enti preposti alla registrazione dei nomi di dominio” (F. Di Ciommo)⁵².

La direttiva 2000/31/CE disciplina la *responsabilità* di detti prestatori intermediari mediante una serie di disposizioni, oggi recepite dal D.L.vo 70/2003 (artt. 14-16)⁵³. Si ricorda preliminarmente quanto enunciato dal legislatore europeo nel

⁵² F. Di Ciommo, *Responsabilità civili in Internet: i soggetti, i comportamenti illeciti, le tutele*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=6878.

⁵³ F. Di Ciommo, *Responsabilità civili in Internet: i soggetti, i comportamenti illeciti, le tutele* cit. rileva come la direttiva 2000/31/CE rappresenti l’unico riferimento normativo europeo in materia di responsabilità civile dei *provider*.

“Infatti, anche nei settori specifici in cui esistono regole comuni che disciplinano determinati aspetti della realtà digitale, mancano disposizioni che riguardano l’imputazione della responsabilità ed in particolare mancano riferimenti alla eventuale responsabilità dei prestatori che offrono servizi sfruttando la tecnologia digitale e le tecnologie di rete. È il caso, ad esempio, della

considerando 40 della direttiva:

“Le attuali o emergenti divergenze tra le normative e le giurisprudenze nazionali, nel campo della responsabilità dei prestatori di servizi che agiscono come intermediari, impediscono il buon funzionamento del mercato interno, soprattutto ostacolando lo sviluppo dei servizi transnazionali e introducendo distorsioni della concorrenza. In taluni casi, i prestatori di servizi hanno il dovere di agire per evitare o per porre fine alle attività illegali. La presente direttiva dovrebbe costituire la base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime. Tali sistemi potrebbero essere concordati tra tutte le parti interessate e andrebbero incoraggiati dagli Stati membri. È nell'interesse di tutte le parti attive nella prestazione di servizi della società dell'informazione istituire e applicare tali sistemi. Le disposizioni della presente direttiva sulla responsabilità non dovrebbero impedire ai vari interessati di sviluppare e usare effettivamente sistemi tecnici di protezione e di identificazione, nonché strumenti tecnici di sorveglianza resi possibili dalla tecnologia digitale, entro i limiti fissati dalle direttive 95/46/CE e 97/66/CE”⁵⁴.

direttiva 2001/29/CE del 22 maggio 2001, relativa all'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; la quale volutamente – malgrado la diversa soluzione praticata dal legislatore americano con il DMCA – ha evitato di stabilire regole specifiche circa la responsabilità dei *provider* per la violazione on-line di diritti d'autore compiuta dagli utenti di Internet.

Ciò si giustifica in ragione del fatto che, in Europa, la questione relativa alla responsabilità dei prestatori di servizi della società dell'informazione viene avvertita come problema di carattere generale da risolvere in modo unitario, per cui si è preferito demandare il compito di disciplinare la responsabilità dei *provider*, per ogni fattispecie illecita compiuta on-line dagli utenti, interamente alla direttiva 2000/31/CE”.

Sulla responsabilità dei provider, v. anche A. Pierucci, *La responsabilità extracontrattuale dei fornitori di servizi telematici*, in *Il diritto della nuova economia* cit., pp. 495 ss.; A.R. Sirotti Gaudenzi, *L'imprenditore in Rete e i contratti telematici* cit.; G. Cassano e I.P. Cimino, *La responsabilità extracontrattuale dei provider*, in *InterLex*, www.interlex.it, www.interlex.it/regole/cass_cim1.htm.

⁵⁴ Come più volte ricordato, la direttiva 97/66/CE è stata recepita in Italia con l'abrogato D.L.vo 171/1998; la direttiva 95/46/CE con l'abrogata L. 675/1996. Oggi il riferimento va dunque alle disposizioni del Codice della privacy esaminate nei precedenti capitoli.

Gli articoli da 14 a 16 del D.L.vo 70/2003, nel disciplinare la responsabilità dei prestatori intermediari, distinguono tra:

- *attività di semplice trasporto (mere conduit)*: è ad esempio il caso, spiega la relazione illustrativa, del fornitore dei servizi di posta elettronica e del fornitore dei servizi di connessione a Internet;
- *attività di memorizzazione intermedia e temporanea di informazioni effettuata allo scopo di rendere più efficace il successivo inoltramento ad altri destinatari che ne hanno fatto richiesta (caching)*;
- *attività di memorizzazione di informazioni fornite dal destinatario del servizio, come la messa a disposizione di uno spazio server per siti o pagine web (hosting)*.

Come si vedrà, l'art. 17 del provvedimento in parola stabilisce infine, in favore dei provider, l'assenza dell'obbligo generale di sorveglianza⁵⁵.

Il provvedimento sul commercio elettronico non introduce una specifica forma di responsabilità per i provider, bensì afferma che, ferma restando l'applicazione delle altre regole di diritto comune, per andare incontro a responsabilità extracontrattuale in ordine al fatto illecito commesso on-line dagli utenti, nei confronti del provider dovranno difettare le condizioni espressamente previste dal D.L.vo 70/2003. Viene insomma introdotta una sorta di "immunità condizionata"

⁵⁵ Si ricorda anche quanto disposto in tema di *diritto d'autore* dall'art. 68bis L. 633/1941, così come introdotto dal [D.L.vo 68/2003](#) di attuazione della direttiva 2001/29/CE:

"1. Salvo quanto disposto in ordine alla responsabilità dei prestatori intermediari dalla normativa in materia di commercio elettronico, sono esentati dal diritto di riproduzione gli atti di riproduzione temporanea privi di rilievo economico proprio che sono transitori o accessori e parte integrante ed essenziale di un procedimento tecnologico, eseguiti all'unico scopo di consentire la trasmissione in rete tra terzi con l'intervento di un intermediario, o un utilizzo legittimo di un'opera o di altri materiali".

dell'intermediario⁵⁶.

“In sostanza, dice il testo, i fornitori di servizi non hanno alcuna responsabilità per i contenuti, a condizione che non intervengano in alcun modo sui contenuti stessi, il che è già ampiamente previsto dal nostro ordinamento (e da qualsiasi ordinamento di un paese democratico). Tuttavia la formulazione delle norme è tale da ingenerare non poche perplessità in relazione alla natura degli interventi dei fornitori di servizi, perché è noto che le attività di trasmissione e instradamento delle informazioni comportano sempre qualche forma di ‘intervento’ che potrebbe rientrare tra le cause di non esenzione della responsabilità” (M. Cammarata)⁵⁷.

La responsabilità del prestatore viene dunque definita in negativo: se sussistono le condizioni di cui al D.L.vo 70/2003 allora il prestatore non potrà essere chiamato a rispondere degli illeciti commessi on-line dagli utenti. Se, viceversa, il provider pone in essere un comportamento contrario a quanto sancito dal provvedimento,

⁵⁶ Così F. Di Ciommo, *Responsabilità civili in Internet: i soggetti, i comportamenti illeciti, le tutele* cit.

⁵⁷ M. Cammarata, *Sotto torchio gli operatori della Rete*, in *InterLex*, www.interlex.it, www.interlex.it/regole/torchio.htm, il quale così prosegue: “E’ ovvio che, ai fini dell’attribuzione di una responsabilità, il giudice indagherà su quello che i giuristi chiamano ‘l’elemento soggettivo dell’illecito’, dovrà cioè stabilire se l’intervento del provider sui contenuti sia una mera operazione tecnica o se vi sia l’intenzione di influire in qualche modo sui contenuti stessi: solo in questo caso si potrà parlare di responsabilità del fornitore. Tuttavia l’esperienza insegna che disposizioni così generiche costituiscono un pericolo non trascurabile: non è comunque positivo che un’assenza di responsabilità sia sancita da un giudice al termine di un’istruttoria o addirittura di un processo, laddove una norma più chiara eviterebbe all’origine l’intervento dell’autorità giudiziaria”.

Con riguardo alle questioni concernenti la *responsabilità penale del provider*, si rimanda a D. Minotti, *Responsabilità penale: il provider è tenuto ad “attivarsi”?*, in *InterLex*, www.interlex.it, www.interlex.it/regole/minotti8.htm, il quale osserva che “il decreto, agli artt. 14, 15 e 16, solleva i prestatori da ogni responsabilità (diverse da quelle amministrative fissate nel decreto) a condizione che essi non intervengano sulle informazioni (i.e. i dati) da loro memorizzate o veicolate. Previsione di mero valore riproduttivo, atteso che, anche senza il decreto, l’intervento (‘causale’) sulle informazioni (consapevolmente illecite) poteva già condurre, per i principi generali di diritto penale, ad ipotesi di concorso commissivo”.

Si veda anche M. Cammarata, *Le trappole nei contratti di hosting*, in *InterLex*, www.interlex.it, www.interlex.it/regole/trappole.htm.

allora scatterà l'obbligo di risarcire il danno prodotto. Si tratterà evidentemente di una responsabilità solidale con l'autore dell'illecito *ex art. 2055 cod. civ.*⁵⁸.

8.1. Responsabilità nell'attività di semplice trasporto (mere conduit)

Ai sensi dell'art. 14, comma 1, del decreto sul commercio elettronico, nella prestazione di un servizio della società dell'informazione consistente nel:

- trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio,
- o nel fornire un accesso alla rete di comunicazione,

il prestatore non è responsabile delle informazioni trasmesse a condizione che:

- a) non dia origine alla trasmissione;
- b) non selezioni il destinatario della trasmissione;
- c) non selezioni né modifichi le informazioni trasmesse.

In pratica, dice la relazione illustrativa, “si stabilisce che il *carrier*, l'operatore

⁵⁸ “Proseguendo l'analisi della direttiva 2000/31/Ce, pare interessante notare come la normativa in parola non lasci l'accertamento della colpa del *provider* alla discrezionalità del giudice. Quest'ultimo, infatti, non è genericamente chiamato, come sarebbe in forza dell'art. 2043, a valutare la correttezza della condotta e dell'atteggiamento psichico dell'intermediario, bensì è tenuto ad applicare i principi della direttiva – che il d. lgs. 70/2003 ha riprodotto fedelmente –, e dunque esclusivamente ad accertare, quando il danneggiato agisca contro l'intermediario cercando di provare la sua colpa specifica, che quest'ultimo non abbia posto in essere nessuna delle condizioni che fanno scattare la sua responsabilità.

Siamo, a ben vedere, alle prese con un sistema di imputazione della responsabilità basato esclusivamente sulla colpa specifica dell'intermediario, e cioè sulla colpa per violazione di legge; mentre al giudice è precluso, in quanto inutile al fine dell'imputazione della responsabilità, ogni accertamento ulteriore relativo all'atteggiamento psichico del convenuto” (F. Di Ciommo, *Responsabilità civili in Internet: i soggetti, i comportamenti illeciti, le tutele cit.*).

telefonico, non è responsabile di ciò che passa sulla sua rete”⁵⁹.

Le predette attività di trasmissione e di fornitura di accesso *includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse*, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo (art. 14, comma 2).

L'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2 dell'art. 14, appena illustrate, *impedisca o ponga fine alle violazioni commesse*.

8.2. Responsabilità nell'attività di memorizzazione temporanea (caching)

Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, *il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltramento ad altri destinatari a loro richiesta, a condizione che* (art. 15, comma 1):

- a) non modifichi le informazioni;
- b) si conformi alle condizioni di accesso alle informazioni;
- c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;

⁵⁹ Sulla dibattuta questione dei *dialer*, si veda M. Cammarata, *Occorre una querela per fermare i truffatori*, in *InterLex*, www.interlex.it, www.interlex.it/regole/709truffa.htm.

d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;

e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

Anche in questo caso, l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1 dell'art. 15, appena illustrato, impedisca o ponga fine alle violazioni commesse (art. 15, comma 2).

8.3. Responsabilità nell'attività di memorizzazione di informazioni (hosting)

Ai sensi dell'art. 16, comma 1, del provvedimento sul commercio elettronico, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, *il prestatore non è responsabile delle informazioni memorizzate a richiesta del destinatario, a condizione che detto prestatore:*

a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;

b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per

disabilitarne l'accesso⁶⁰.

Le disposizioni di cui sopra *non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore* (art. 16, comma 2).

L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle predette attività, impedisca o ponga fine alle violazioni commesse (art. 16, comma 3).

8.4. Assenza dell'obbligo generale di sorveglianza

Nella prestazione dei servizi di *mere conduit, caching e hosting*, di cui sopra, *il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite* (art. 17, comma 1).

D'altra parte, fatte salve le disposizioni di cui agli artt. 14, 15 e 16 del provvedimento, già illustrate, *il prestatore è comunque tenuto* (art. 17, comma 2):

a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni

⁶⁰ Si ricorda a questo proposito quanto contenuto nel già richiamato parere espresso dalla X Commissione parlamentare sullo schema di decreto legislativo:

“f) in relazione a quanto previsto dall'articolo 16 - secondo cui il prestatore di un servizio non è responsabile qualora, non appena a conoscenza dell'illiceità di un'attività o di un'informazione, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso -, al fine di evitare che sia vanificata qualsiasi azione efficace ed immediata tesa alla rimozione dalla rete di materiale illecito appare opportuno precisare che la comunicazione delle autorità non costituisce condizione necessaria per la rimozione delle informazioni o per la disabilitazione dell'accesso; conseguentemente, all'articolo 16, comma 1, lettera b), le parole: «su comunicazione» potrebbero essere sostituite dalle seguenti: «anche a seguito di comunicazione»”.

illecite riguardanti un suo destinatario del servizio della società dell'informazione;

b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Conseguentemente, il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non abbia agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non abbia provveduto ad informarne l'autorità competente (art. 17, comma 3)⁶¹.

“Anche qui saremmo di fronte a un'ipotesi pacifica di responsabilità extracontrattuale, per la prima parte della disposizione, dunque a una norma superflua. Ma la seconda parte è talmente vaga da consentire qualsiasi interpretazione, estensiva o restrittiva: che significa ‘avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo’? Basta una e-mail di segnalazione, o una lettura casuale, o occorre una diffida o un qualche altro atto

⁶¹ Un cenno merita l'applicazione delle disposizioni appena illustrate in materia di *spamming*. Ci si chiede se sia possibile configurare una qualche forma di responsabilità extracontrattuale in capo ai provider in relazione allo *spamming effettuato o subito dai propri abbonati* (fatte salve dunque eventuali clausole contrattuali).

Alla luce degli artt. 14-17 del D.L.vo 70/2003 può risponderci in senso negativo, ove risultino soddisfatte in capo al provider tutte le condizioni richieste dal suddetto provvedimento.

D'altra parte, si ricorda che il Garante per la protezione dei dati personali, ex art. 130 del Codice della privacy (cap. III, par. 11.4), in caso di reiterate violazioni della predetta disposizione, può *prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono state inviate le comunicazioni indesiderate*.

formale?” (M. Cammarata)⁶².

Va sottolineato che la direttiva 2000/31/CE, nel prevedere all’art. 15 l’ “assenza dell’obbligo generale di sorveglianza”, prevedeva la *facoltà*, e non l’obbligo, per gli Stati membri di stabilire a carico del prestatore quanto oggi sancito dalle lettere a) e b) dell’art. 17, comma 2, del decreto legislativo in parola.

E’ stato inoltre osservato che il combinato disposto degli artt. 16 e 17 del D.L.vo 70/2003 pone delicate questioni in relazione ai *contratti di hosting*, nel caso – frequente – in cui questi prevedano la facoltà del provider di verificare i dati immessi dall’utente e rimuovere quelli che appaiono illeciti o comunque non aderenti alla *netiquette* o alla *policy* dell’azienda⁶³.

[Sommaro](#)

9. Codici di condotta, composizione delle controversie e cooperazione

Codici di condotta.

L’art. 18 del decreto legislativo 70/2003 attribuisce alle *associazioni o*

⁶² M. Cammarata, *Sotto torchio gli operatori della Rete* cit.

Sulla *notification* si veda, in particolare, G. Cassano e I.P. Cimino, *La responsabilità extracontrattuale dei provider* cit., secondo cui “Da una parte, dunque, il provider ha l’obbligo di *attivarsi* al fine di impedire il perpetrarsi di violazioni commesse on line dai propri clienti mediante la porzione di server loro concessa. D’altra (come già detto), è tenuto a valutare attentamente l’attendibilità delle *notification* che gli perverranno, se non vorrà rendersi contrattualmente inadempiente nei riguardi del proprio cliente per l’ipotesi in cui il contenuto rimosso dalla Rete si riveli affatto illecito o illegittimamente utilizzato”.

⁶³ M. Cammarata, *Le trappole nei contratti di hosting* cit., secondo il quale “dal momento in cui il provider dichiara di sorvegliare i contenuti immessi dai clienti si può presumere che egli possa essere effettivamente a conoscenza dell’eventuale illiceità di tali contenuti. E quindi si addossa le relative responsabilità!”.

organizzazioni imprenditoriali, professionali o di consumatori il compito di promuovere l'adozione di codici di condotta, da trasmettersi al Ministero delle attività produttive e alla Commissione europea con ogni utile informazione sulla loro applicazione e sul loro impatto nelle pratiche e consuetudini relative al commercio elettronico.

La medesima disposizione stabilisce inoltre che il codice di condotta, se adottato, deve essere reso accessibile per via telematica e deve essere redatto, oltre che in lingua italiana e inglese, almeno in un'altra lingua comunitaria.

Viene altresì specificato che nella redazione dei codici di condotta deve essere garantita la protezione dei minori e salvaguardata la dignità umana.

L'art. 16, ult. par., della direttiva 2000/31/CE, aggiunge che “Gli Stati membri e la Commissione favoriscono la partecipazione delle associazioni che rappresentano i consumatori al processo di elaborazione e di applicazione dei codici di condotta di cui al paragrafo 1, lettera a), che riguardano i loro interessi. Per tener conto delle loro esigenze specifiche, dovrebbero essere consultate, ove opportuno, le associazioni che rappresentano i non vedenti, gli ipovedenti e i disabili”.

In base al considerando 49 della direttiva 2000/31/CE, rimangono in ogni caso *impregiudicati il carattere volontario di siffatti codici di condotta e la possibilità per le parti interessate di decidere liberamente se aderirvi*⁶⁴.

È stato osservato che “L'ultima normativa sul commercio elettronico, adottata dal legislatore in attuazione della Direttiva Comunitaria n. 2000/31/CE, sembra essere nata sotto il segno della deregulation reale e non apparente. Che non si tratti di una mera operazione di delegificazione ma di una sostanziale promozione della

⁶⁴ Sul *Codice di autoregolamentazione Internet e minori*, v. cap. III, nota n. 112.

normazione interpretistica risulta ictu oculi proprio dall'art. 18 del D.Lgs n. 70/2003, il quale rimanda appunto alle associazioni ed organizzazioni imprenditoriali il compito di promuovere l'adozione di codici di condotta” (R. Spelta)⁶⁵.

Composizione delle controversie.

Con riguardo alla *composizione delle controversie nel commercio elettronico*, l'art. 19 del provvedimento in parola stabilisce innanzitutto che, in caso di lite, al prestatore e al destinatario del servizio della società dell'informazione è riconosciuta la possibilità di adire anche *organi di composizione extragiudiziale, operanti anche per via telematica*⁶⁶.

Tali organi, ove operino in conformità ai principi previsti dall'ordinamento comunitario e da quello nazionale, sono notificati, su loro richiesta, alla Commissione dell'Unione europea per l'inserimento nella *Rete europea di composizione extragiudiziale delle controversie* (EEJ-Net).

Come può leggersi nel relativo sito, “EEJ-Net è una rete di meccanismi per la risoluzione extragiudiziale delle controversie attiva negli Stati membri dell'UE e del SEE. Si tratta di una struttura di informazione e sostegno a disposizione di tutti i consumatori dei paesi dell'UE e del SEE, a cui si può ricorrere per comporre

⁶⁵ R. Spelta, *Codici di condotta ex art. 18 del D.Lgs n. 70/2003*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/spelta.html.

⁶⁶ Sulla *composizione extragiudiziale delle controversie nel commercio elettronico*, si veda A. Lisi, *Passaggio dall'ADR internazionale all'ADR on line nel commercio elettronico*, in *La Pratica Forense*, www.comuni.it/servizi/praticaforense, <http://www.comuni.it/servizi/praticaforense/articolo.php?idart=113>; M. Pievani e E. Ruggiero, *L'Adr on line*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., pp. 506 ss.; M.F. Tari, *Ruolo delle Alternative Dispute Resolution on line nel commercio elettronico*, in *Altalex*, www.altalex.com, www.altalex.com/index.php?idnot=5784; M. Tinti, *Commento all'Art. 19 del D.LGS. N. 70/2003*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_tecnologie/tinti.html.

le vertenze commerciali con le imprese residenti in un altro Stato membro. La finalità di EEJ-Net è di facilitare l'accesso alla giustizia ai consumatori dell'UE/SEE, in particolare per quanto concerne le controversie transfrontaliere connesse alle transazioni elettroniche. Per far ciò, EEJ-Net mette in collegamento i diversi organismi di risoluzione extragiudiziale delle vertenze in materia di consumo operanti negli Stati membri dell'UE e del SEE”⁶⁷.

Gli organi di composizione extragiudiziale delle controversie devono comunicare alla Commissione europea nonché al Ministero delle attività produttive, che provvede a darne comunicazione alle Amministrazioni competenti per materia, le decisioni significative che adottano sui servizi della società dell'informazione, nonché ogni altra informazione su pratiche, consuetudini od usi relativi al commercio elettronico.

La direttiva 2000/31/CE si occupa espressamente anche dei *ricorsi giurisdizionali*. L'art. 18, par. 1, stabilisce infatti che “Gli Stati membri provvedono affinché i ricorsi giurisdizionali previsti dal diritto nazionale per quanto concerne le attività dei servizi della società dell'informazione consentano di prendere rapidamente provvedimenti, anche provvisori, atti a porre fine alle violazioni e a impedire ulteriori danni agli interessi in causa”⁶⁸.

⁶⁷ Sulla *Rete europea di composizione extragiudiziale delle controversie transfrontaliere* (EEJ-Net) si veda il sito www.eejnet.org.

Si ricorda anche quanto espresso nel suo parere dalla X Commissione parlamentare a proposito dell'art. 19 del provvedimento:

“g) si valuti l'opportunità, in relazione all'articolo 19, relativo alla composizione delle controversie, di richiamare espressamente gli organismi di conciliazione delle camere di commercio, industria, artigianato ed agricoltura, in considerazione dell'esperienza che le stesse hanno acquisito sul fronte della giustizia alternativa in base a varie disposizioni di legge”.

⁶⁸ Con riguardo ai provider, si veda il par. 8.

L'art. 18, par. 2, della direttiva sul commercio elettronico introduce altresì una modifica all'allegato della direttiva 98/27/CE, inserendo la direttiva 2000/31/CE stessa tra quelle contemplate dal suddetto allegato.

In base al considerando 52 della direttiva, inoltre, “L’esercizio effettivo delle libertà del mercato interno rende necessario garantire alle vittime un accesso efficace alla soluzione delle controversie. I danni che possono verificarsi nell’ambito dei servizi della società dell’informazione sono caratterizzati sia dalla loro rapidità che dalla loro estensione geografica. Stante questa peculiarità, oltre che la necessità di vigilare affinché le autorità nazionali non rimettano in questione la fiducia che esse dovrebbero reciprocamente avere, la presente direttiva dispone che gli Stati membri garantiscano la possibilità di azioni giudiziarie appropriate. Gli Stati membri dovrebbero esaminare la necessità di dare accesso ai procedimenti giudiziari mediante appropriati strumenti

La direttiva 98/27/CE è stata recepita nell’ordinamento italiano con il D.L.vo 224/2001 (*Attuazione della direttiva 98/27/CE relativa a provvedimenti inibitori a tutela degli interessi dei consumatori*, GU 137 del 15 giugno 2001), il quale a sua volta è andato ad incidere sulla legge 30 luglio 1998, n. 281 (*Disciplina dei diritti dei consumatori e degli utenti*, GU Serie gen. 189 del 14 agosto 1998).

A seguito delle modifiche introdotte con il D.L.vo 224/2001, all’art. 1 della legge 30 luglio 1998, n. 281, risulta aggiunto il seguente comma:

“2-bis. Oltre a quanto disposto ai commi 1 e 2, la presente legge si applica nelle ipotesi di violazione degli interessi collettivi dei consumatori contemplati nelle direttive europee di cui all’allegato I alla presente legge. Il Ministro dell’industria, del commercio e dell’artigianato, di concerto con il Ministro della giustizia, aggiorna l’elenco delle direttive comunitarie di cui a tale allegato con decreto, in attuazione degli obblighi derivanti da norme comunitarie”.

L’allegato I della L. 281/1998, riprodotto l’allegato della direttiva 98/27/CE, dovrà essere pertanto modificato in modo da ricomprendervi oggi anche la direttiva 2000/31/CE, *con la conseguenza che in ipotesi di violazione degli interessi dei consumatori contemplati dal provvedimento europeo sul commercio elettronico si applicherà anche la suddetta L. 281/1998*.

Con riguardo alla reale portata della disposizione, si veda però G. De Marzo, *Tutela inibitoria degli interessi collettivi e diritto comunitario*, in *Sarannomagistrati.it*, www.sarannomagistrati.it, www.sarannomagistrati.it/articoli/13.htm, secondo il quale:

“[...] l’avvenuta trasposizione delle restanti direttive di cui all’elenco allegato alla direttiva 98/27 rende, in linea di massima, superflua la ricerca di ulteriore copertura normativa per le posizioni di interesse collettivo.

[...] A non voler seguire il percorso argomentativo appena tratteggiato, uno spazio operativo alla disposizione in esame può comunque essere individuato in relazione a situazioni previste dalle direttive di riferimento e non recepite, o per l’inadeguato sforzo del legislatore interno o perché contemplate da modifiche delle direttive stesse apportate successivamente al provvedimento nazionale di adeguamento”.

elettronici”⁶⁹.

Cooperazione.

Presso il *Ministero delle attività produttive*, senza maggiori oneri a carico del bilancio dello Stato, l’art. 20 del decreto in esame prevede l’istituzione di un *punto di contatto nazionale*, destinato a fornire *assistenza e collaborazione agli Stati membri e alla Commissione europea*. Il punto di contatto dovrà essere accessibile anche per via telematica⁷⁰.

Il Ministero delle attività produttive deve altresì provvedere affinché sul proprio sito⁷¹ siano rese tempestivamente disponibili per le Amministrazioni pubbliche, i destinatari e i fornitori di servizi:

⁶⁹ Con riguardo alla “necessità di dare accesso ai procedimenti giudiziari mediante appropriati strumenti elettronici”, si ricorda che con il D.P.R. 123/2001 (*Regolamento recante disciplina sull’uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo innanzi alle sezioni giurisdizionali della Corte dei Conti*, GU 89 del 17 aprile 2001) sono state gettate in Italia le basi per il c.d. *processo telematico*.

In argomento si veda G. Briganti, *Il c.d. processo telematico*, in *Iusreporter*, www.iusreporter.it, www.iusreporter.it/Testi/doc-teleprocesso.htm e successivi aggiornamenti.

⁷⁰ In tema di cooperazione, si ricorda la *Rete giudiziaria europea in materia civile e commerciale*.

Come può leggersi nel relativo sito (http://europa.eu.int/comm/justice_home/ejn/index_it.htm):

“La rete è formata dai rappresentanti delle autorità giudiziarie e amministrative degli Stati membri che si riuniscono più volte all’anno per scambiare informazioni ed esperienze e per rafforzare la cooperazione tra gli Stati membri nel settore del diritto civile e commerciale.

Il principale obiettivo della rete è di facilitare la vita dei cittadini che devono far fronte a qualsiasi tipo di controversia di natura ‘transfrontaliera’, cioè che coinvolge più di uno Stato membro.

Infatti, l’Unione europea è caratterizzata attualmente da una grande varietà di sistemi giudiziari nazionali e tale diversità pone spesso dei problemi quando le controversie oltrepassano le frontiere. Pertanto, può rivelarsi utile per i privati e per le imprese e, a maggior ragione, per gli operatori del diritto conoscere i diversi sistemi giuridici nazionali in materia civile e commerciale nonché gli strumenti legislativi dell’Unione europea e di altre organizzazioni internazionali come le Nazioni Unite, la conferenza dell’Aja e il Consiglio d’Europa”.

⁷¹ Il sito del Ministero delle attività produttive è raggiungibile all’indirizzo www.minindustria.it.

a) le *informazioni generali* sui diritti ed obblighi contrattuali e sui meccanismi di reclamo e ricorso disponibili in caso di controversie, nonché sui codici di condotta elaborati con le associazioni di consumatori iscritte nell'elenco di cui all'art. 5 della legge 30 luglio 1998, n. 281⁷²;

⁷² Si riporta il testo dell'art. 5 della già richiamata L. 281/1998:

“Art. 5. (*Elenco delle associazioni dei consumatori e degli utenti rappresentative a livello nazionale*). - 1. Presso il Ministero dell'industria, del commercio e dell'artigianato e' istituito l'elenco delle associazioni dei consumatori e degli utenti rappresentative a livello nazionale.

2. L'iscrizione nell'elenco e' subordinata al possesso, da comprovare con la presentazione di documentazione conforme alle prescrizioni e alle procedure stabilite con decreto del Ministro dell'industria, del commercio e dell'artigianato, da emanare entro sessanta giorni dalla data di entrata in vigore della presente legge, dei seguenti requisiti:

a) avvenuta costituzione, per atto pubblico o per scrittura privata autenticata, da almeno tre anni e possesso di uno statuto che sancisca un ordinamento a base democratica e preveda come scopo esclusivo la tutela dei consumatori e degli utenti, senza fine di lucro;

b) tenuta di un elenco degli iscritti, aggiornato, annualmente con l'indicazione delle quote versate direttamente all'associazione per gli scopi statutari;

c) numero di iscritti non inferiore allo 0,5 per mille della popolazione nazionale e presenza sul territorio di almeno cinque regioni o province autonome, con un numero di iscritti non inferiore allo 0,2 per mille degli abitanti di ciascuna di esse, da certificare con dichiarazione sostitutiva dell'atto di notorietà resa dal legale rappresentante dell'associazione con le modalita' di cui all'articolo 4 della legge 4 gennaio 1968, n. 15.

d) elaborazione di un bilancio annuale delle entrate e delle uscite con indicazione delle quote versate dagli associati e tenuta dei libri contabili, conformemente alle norme vigenti in materia di contabilita' delle associazioni non riconosciute;

e) svolgimento di un'attivita' continuativa nei tre anni precedenti;

f) non avere i suoi rappresentanti legali subito alcuna condanna, passata in giudicato, in relazione all'attivita' dell'associazione medesima, e non rivestire i medesimi rappresentanti la qualifica di imprenditori o di amministratori di imprese di produzione e servizi in qualsiasi forma costituite, per gli stessi settori in cui opera l'associazione.

3. Alle associazioni dei consumatori e degli utenti e' preclusa ogni attivita' di promozione o pubblicita' commerciale avente per oggetto beni o servizi prodotti da terzi ed ogni connessione di interessi con imprese di produzione o di distribuzione.

4. Il Ministro dell'industria, del commercio e dell'artigianato provvede annualmente all'aggiornamento dell'elenco.

b) *gli estremi delle autorità, organizzazioni o associazioni presso le quali possono ottenere ulteriori informazioni o assistenza;*

c) *gli estremi e la sintesi delle decisioni significative riguardo a controversie sui servizi della società dell'informazione, comprese quelle adottate dagli organi di composizione extragiudiziale nonché informazioni su pratiche, consuetudini od usi relativi al commercio elettronico.*

[Sommar](#)

10. Sanzioni

L'art. 20 della direttiva europea sul commercio elettronico stabilisce che “Gli Stati membri comminano sanzioni per la violazione delle norme nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni devono essere effettive, proporzionate e dissuasive”.

Il considerando 54 precisa che “Le sanzioni previste nella presente direttiva

5. All'elenco di cui al presente articolo possono iscriversi anche le associazioni dei consumatori e degli utenti operanti esclusivamente nei territori ove risiedono minoranze linguistiche costituzionalmente riconosciute, in possesso dei requisiti di cui al comma 2, lettere a), b), d), e) e f), nonché con un numero di iscritti non inferiore allo 0,5 per mille degli abitanti della regione o provincia autonoma di riferimento, da certificare con dichiarazione sostitutiva dell'atto di notorietà resa dal legale rappresentante dell'associazione con le modalità di cui all'articolo 4 della legge 4 gennaio 1968, n. 15.

5-bis. Il Ministero dell'industria, del commercio e dell'artigianato comunica alla Commissione europea l'elenco di cui al presente articolo e le successive variazioni, al fine dell'iscrizione nell'elenco degli enti legittimati a proporre azioni inibitorie a tutela degli interessi collettivi dei consumatori”.

Si veda anche il D.M. 19 gennaio 1999, n. 20, *Regolamento recante norme per l'iscrizione nell'elenco delle associazioni dei consumatori e degli utenti rappresentative a livello nazionale*, GU Serie gen. 29 del 5 febbraio 1999.

lasciano impregiudicati le altre sanzioni o mezzi di tutela previsti dal diritto nazionale. Gli Stati membri non sono tenuti a prevedere sanzioni di tipo penale per la violazione delle disposizioni nazionali adottate in attuazione della presente direttiva”.

In attuazione del provvedimento comunitario, l’art. 21 del D.L.vo 70/2003 detta pertanto le sanzioni per la violazione di alcuni degli obblighi posti a carico dei prestatori dei servizi della società dell’informazione dalle disposizioni sin qui brevemente analizzate.

Più esattamente, le sanzioni sono riferite alla violazione degli obblighi di cui:

- all’art. 7: informazioni generali obbligatorie;
- all’art. 8: obblighi di informazione per la comunicazione commerciale;
- all’art. 9: comunicazione commerciale non sollecitata;
- all’art. 10: uso delle comunicazioni commerciali nelle professioni regolamentate;
- all’art. 12: informazioni dirette alla conclusione del contratto⁷³.

Si prevede dunque che, *salvo che il fatto costituisca reato*⁷⁴, le violazioni di cui agli artt. 7, 8, 9, 10 e 12 del decreto siano punite con *il pagamento di una sanzione amministrativa pecuniaria da 103 euro a 10.000 euro*. Nei casi di particolare gravità o di recidiva i limiti minimo e massimo della sanzione sono raddoppiati.

Le sanzioni previste sono applicate ai sensi della legge 24 novembre 1981, n. 689⁷⁵.

⁷³ Si vedano rispettivamente i parr. 5, 6 e 7 del presente capitolo.

⁷⁴ Nel qual caso potranno ovviamente trovare applicazione le relative sanzioni penali previste dall’ordinamento italiano.

⁷⁵ Legge 24 novembre 1981, n. 689, *Modifiche al sistema penale*, GU 329 del 30 novembre 1981, Suppl. ord.

Fermo restando quanto previsto in ordine ai poteri di accertamento degli ufficiali e degli agenti di polizia giudiziaria dall'art. 13 della predetta legge⁷⁶, all'accertamento delle violazioni provvedono, d'ufficio o su denuncia, gli organi di polizia amministrativa.

Il rapporto di accertamento delle violazioni di cui sopra è presentato al *Ministero delle attività produttive*, fatta salva l'ipotesi di cui all'art. 24 della legge 24 novembre 1981, n. 689 (“Connessione obiettiva con un reato”)⁷⁷.

⁷⁶ L'art. 13 L. 689/1981 così dispone:

“13. (*Atti di accertamento*). Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica.

Possono altresì procedere al sequestro cautelare delle cose che possono formare oggetto di confisca amministrativa, nei modi e con i limiti con cui il codice di procedura penale consente il sequestro alla polizia giudiziaria.

È sempre disposto il sequestro del veicolo a motore o del natante posto in circolazione senza essere coperto dall'assicurazione obbligatoria e del veicolo posto in circolazione senza che per lo stesso sia stato rilasciato il documento di circolazione.

All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria, i quali, oltre che esercitare i poteri indicati nei precedenti commi, possono procedere, quando non sia possibile acquisire altrimenti gli elementi di prova, a perquisizioni in luoghi diversi dalla privata dimora, previa autorizzazione motivata del pretore del luogo ove le perquisizioni stesse dovranno essere effettuate. Si applicano le disposizioni del primo comma dell'art. 333 e del primo e secondo comma dell'art. 334 del codice di procedura penale.

È fatto salvo l'esercizio degli specifici poteri di accertamento previsti dalle leggi vigenti”.

⁷⁷ L'art. 24 L. 689/1981 così dispone:

“24. (*Connessione obiettiva con un reato*). Qualora l'esistenza di un reato dipenda dall'accertamento di una violazione non costituente reato, e per questa non sia stato effettuato il pagamento in misura ridotta, il giudice penale competente a conoscere del reato è pure competente a decidere sulla predetta violazione e ad applicare con la sentenza di condanna la sanzione stabilita dalla legge per la violazione stessa.

Se ricorre l'ipotesi prevista dal precedente comma, il rapporto di cui all'art. 17 è trasmesso, anche senza che si sia proceduto alla notificazione prevista dal secondo comma dell'art. 14, all'autorità

Sommario

giudiziaria competente per il reato, la quale, quando invia la comunicazione giudiziaria, dispone la notifica degli estremi della violazione amministrativa agli obbligati per i quali essa non è avvenuta. Dalla notifica decorre il termine per il pagamento in misura ridotta.

Se l'autorità giudiziaria non procede ad istruzione, il pagamento in misura ridotta può essere effettuato prima dell'apertura del dibattimento.

La persona obbligata in solido con l'autore della violazione deve essere citata nell'istruzione o nel giudizio penale su richiesta del pubblico ministero. Il pretore ne dispone d'ufficio la citazione. Alla predetta persona, per la difesa dei propri interessi, spettano i diritti e le garanzie riconosciuti all'imputato, esclusa la nomina del difensore d'ufficio.

Il pretore, quando provvede con decreto penale, con lo stesso decreto applica, nei confronti dei responsabili, la sanzione stabilita dalla legge per la violazione.

La competenza del giudice penale in ordine alla violazione non costituente reato cessa se il procedimento penale si chiude per estinzione del reato o per difetto di una condizione di procedibilità".

CAPITOLO V

TUTELA DELL'INTERESSATO E SANZIONI

SOMMARIO: 1. [Premessa](#) – 2. [Tutela dell'interessato](#) – 2.1. [Forme di tutela dinanzi al Garante](#) – 2.2. [Tutela giurisdizionale](#) – 3. [Sanzioni](#) – 3.1. [Violazioni amministrative](#) – 3.2. [Illeciti penali](#) – 4. [È sanzionabile la spedizione di una prima e-mail di richiesta di consenso per il successivo invio di comunicazioni commerciali?](#)

[INDICE](#)

1. Premessa

A conclusione dell'esame della normativa di attuazione della direttiva 2002/58/CE contenuta nel Codice della privacy, occorre ora soffermarsi brevemente sulle *forme di tutela* che il testo unico offre all'interessato nonché sull'*apparato sanzionatorio* ivi previsto.

Dovrà pertanto essere brevemente analizzata la parte III del Codice della privacy, specificamente il titolo I ("Tutela amministrativa e giurisdizionale", artt. 141-152) e il titolo III ("Sanzioni", artt. 161-172).

[Sommar](#)io

2. Tutela dell'interessato

Il Codice della privacy prevede che l'*interessato*¹, al fine di tutelare i propri diritti, possa rivolgersi al *Garante per la protezione dei dati personali* o, in alternativa, al *giudice ordinario*².

2.1. Forme di tutela dinanzi al Garante

L'art. 141 del testo unico, nell'enunciare le *forme di tutela* disponibili dinanzi al *Garante*³ prevede che l'interessato possa rivolgersi all'Autorità:

a) mediante *reclamo circostanziato* (nei modi previsti dall'art. 142), per *rappresentare una violazione della disciplina rilevante*⁴ in materia di trattamento di dati personali;

¹ Sulle definizioni adottate dal testo unico v. cap. II, par. 2.

² Cfr. art. 22 direttiva 95/46/CE.

In argomento, si veda E. Olimpia Policella, *Le azioni a tutela dei dati personali nel Codice privacy*, in *Diritto&Diritti*, www.diritto.it, www.diritto.it/articoli/dir_privacy/policella2.html.

³ Sull'Autorità v. il titolo II della parte III del Codice (artt. 153-160).

⁴ “Da segnalare il riferimento alla ‘disciplina rilevante’ in materia di protezione dei dati, con il quale il codice, da un lato, reca un ulteriore riconoscimento delle nuove fonti normative rappresentate dai codici di deontologia, che si aggiungono, quale ulteriore parametro di liceità del trattamento, alle disposizioni di legge o di regolamento, e, dall'altro, opportunamente rinvia a disposizioni anche di altri settori dell'ordinamento che comunque rilevino ai fini dell'applicazione dei principi in materia di protezione dei dati personali” (così la relazione di accompagnamento al Codice).

“La precisazione normativa in ordine all'indicazione della portata delle azioni di reclamo e segnalazione ha determinato [...] un notevole ampliamento dei poteri dell'Authority innanzi alla quale, dal 1 gennaio del 2004, potranno essere fatte valere tutte le violazioni della normativa a tutela dei dati personali e non solo quelle inerenti il mancato esercizio dei diritti di accesso, di cancellazione, rettifica, integrazione, ecc. di cui all'art. 13 della Legge 675/1996 (art. 7 del Codice privacy)” (E. Olimpia Policella, *Le azioni a tutela dei dati personali nel Codice privacy* cit.).

b) mediante *segnalazione*, se non è possibile presentare il reclamo circostanziato di cui sopra, *al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima*;

c) mediante *ricorso*, se intende far valere gli specifici diritti di cui all'art. 7⁵ secondo le modalità e per conseguire gli effetti previsti dagli artt. 145-151⁶.

Il reclamo deve contenere un'indicazione per quanto possibile dettagliata *dei fatti e delle circostanze* su cui si fonda, *delle disposizioni che si presumono violate e delle misure richieste*, nonché *gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante* (art. 142).

Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'art. 9, comma 2, ed è presentato al Garante *senza particolari formalità*. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono⁷.

⁵ Sull'art. 7 v. cap. II, par. 4.

⁶ Sui quali v. *infra*.

⁷ Si prevede inoltre che il Garante possa predisporre un *modello per il reclamo* da pubblicare nel *Bollettino*, di cui favorisce altresì la disponibilità con strumenti elettronici.

Con riguardo al procedimento da seguire in ordine ai reclami, l'art. 143 (cfr. artt. 21 e 31 L. 675/1996) prevede quanto segue.

“1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:

a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;

b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

Secondo quanto disposto dall'art. 145 del Codice, *i diritti di cui all'art. 7 del testo unico*, esaminati nel capitolo II, possono essere fatti valere dinanzi all'autorità giudiziaria o con *ricorso al Garante*⁸.

Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria. *La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto*⁹.

L'art. 146 ("Interpello preventivo") prescrive che, salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto *solo dopo che è stata avanzata richiesta sul*

c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività.

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti".

Il successivo art. 144, in ordine alle *segnalazioni*, prevede che "I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni di cui all'articolo 141, comma 1, lettera b), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento".

Su reclami e segnalazioni v. anche E. Olimpia Policella, *Le azioni a difesa dei dati personali nel Codice privacy* cit.

⁸ L'alternatività concerne dunque esclusivamente le controversie aventi ad oggetto i diritti attribuiti all'interessato dall'art. 7 del Codice. Una eventuale *azione di risarcimento dei danni* sofferti dovrà essere pertanto necessariamente proposta al giudice ordinario. È comunque possibile rivolgersi prima con ricorso al Garante per far valere in quella sede i diritti di cui all'art. 7 e poi al giudice ordinario per richiedere il risarcimento dei danni patrimoniali e non patrimoniali.

⁹ Cfr. art. 29 L. 675/1996.

medesimo oggetto al titolare o al responsabile ai sensi dell'art. 8, comma 1¹⁰, e sono decorsi i termini previsti dall'articolo ora in esame, di cui appresso, ovvero è stato opposto alla richiesta un diniego anche parziale¹¹.

In base al secondo comma della disposizione, il riscontro alla richiesta da parte del titolare o del responsabile deve essere fornito *entro quindici giorni dal suo ricevimento*. Entro detto termine, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile devono darne comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Il ricorso è proposto *nei confronti del titolare del trattamento* e deve indicare (art. 147)¹²:

a) *gli estremi identificativi del ricorrente*, dell'eventuale procuratore speciale, del *titolare* e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7;

b) *la data della richiesta presentata al titolare* o al responsabile ai sensi dell'art. 8, comma 1, oppure il *pregiudizio imminente ed irreparabile* che permette di prescindere dalla richiesta medesima;

c) *gli elementi posti a fondamento della domanda*;

d) *il provvedimento richiesto al Garante*;

¹⁰ Sull'art. 8 ("Esercizio dei diritti") v. cap. II, par. 4.

¹¹ Cfr. art. 29 L. 675/1996.

¹² Cfr. art. 18 DPR 501/1998.

e) il *domicilio eletto* ai fini del procedimento.

Il ricorso è *sottoscritto dal ricorrente o dal procuratore speciale e reca in allegato:*

a) la copia della richiesta rivolta al titolare o al responsabile ai sensi dell'art. 8, comma 1;

b) l'eventuale procura;

c) la prova del versamento dei diritti di segreteria.

Al ricorso è unita, altresì, la *documentazione utile* ai fini della sua valutazione e l'indicazione di un *recapito per l'invio di comunicazioni* al ricorrente o al procuratore speciale mediante *posta elettronica, telefax o telefono*.

Il ricorso è *rivolto al Garante* e la relativa *sottoscrizione è autenticata*. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un *procuratore speciale iscritto all'albo degli avvocati* al quale la procura è conferita ai sensi dell'art. 83 del codice di procedura civile, ovvero con *firma digitale in conformità alla normativa vigente*.

Il ricorso è validamente proposto solo se è trasmesso con *plico raccomandato*, oppure *per via telematica* osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento prescritte ai sensi dell'art. 38, comma 2¹³, ovvero *presentato direttamente presso l'Ufficio del Garante*.

¹³ V. cap. II, par. 12.

Relativamente al *procedimento relativo al ricorso*, l'art. 149 del Codice prescrive quanto segue¹⁴.

Fuori dei casi in cui è dichiarato inammissibile¹⁵ o manifestamente infondato, il ricorso è *comunicato al titolare del trattamento entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea*¹⁶.

In caso di *adesione spontanea*, è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, inoltre, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

Nel procedimento dinanzi al Garante il titolare, il responsabile e l'interessato hanno *diritto di essere sentiti*, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare *memorie o documenti*. A tal fine l'invito di cui sopra è trasmesso anche al ricorrente e reca l'indicazione del *termine entro il quale il*

¹⁴ Cfr. art. 29 L. 675/1996; art. 20 DPR 501/1998.

¹⁵ L'art. 148 del Codice prevede quanto segue in ordine ai casi di *inammissibilità* del ricorso.

“1. Il ricorso è inammissibile:

a) se proviene da un soggetto non legittimato;

b) in caso di inosservanza delle disposizioni di cui agli articoli 145 e 146;

c) se difetta di taluno degli elementi indicati nell'articolo 147, commi 1 e 2, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante ai sensi del comma 2, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.

2. Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso”.

¹⁶ L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, ove indicato nel ricorso.

titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva.

Nel procedimento il ricorrente può *precisare la domanda* nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare.

Il Garante può disporre, anche d'ufficio, l'espletamento di una o più *perizie*. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.

Nel procedimento, il titolare e il responsabile possono essere *assistiti da un procuratore o da altra persona di fiducia*¹⁷.

In base al successivo art. 150¹⁸, se la particolarità del caso lo richiede, il Garante *può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento* (art. 150, comma 1)¹⁹.

¹⁷ Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni di cui all'art. 150, comma 2, può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni. Il decorso dei termini previsti dall'art. 150, comma 2 e dall'art. 151 è sospeso di diritto dal 1° agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste il pregiudizio di cui all'art. 146, comma 1, e non preclude l'adozione dei provvedimenti di cui all'art. 150, comma 1.

¹⁸ Cfr. art. 29 L. 675/1996; art. 20 DPR 501/1998.

¹⁹ Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'art. 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2 dell'art. 150. Il medesimo provvedimento è impugnabile unitamente a tale decisione.

Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, *ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto* (art. 150, comma 2).

Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.

Il provvedimento espresso, anche provvisorio, adottato dal Garante è *comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax*²⁰.

Secondo quanto disposto dall'art. 151²¹, avverso il provvedimento espresso o il rigetto tacito di cui all'art. 150, comma 2, appena esaminato, *il titolare o l'interessato possono proporre opposizione dinanzi al tribunale con ricorso ai sensi del successivo art. 152. L'opposizione non sospende l'esecuzione del*

²⁰ Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento di cui ai commi 1 e 2 dell'art. 150, il Garante, sentite le parti ove richiesto, dispone le *modalità di attuazione* avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, o di suo rigetto, *il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli artt. 474 e 475 del codice di procedura civile.*

²¹ Cfr. art. 29 L. 675/1996.

provvedimento. Sull'opposizione, il tribunale provvede nei modi di cui all'art. 152²².

La *mancata osservanza dei provvedimenti pronunciati dal Garante* ai sensi dei commi 1 e 2 dell'esaminato art. 150, come si vedrà, comporta l'applicazione delle *sanzioni penali* di cui all'art. 170 del Codice.

2.2. Tutela giurisdizionale

L'art. 152 disciplina il *procedimento innanzi all'autorità giudiziaria ordinaria*, sostituendo la precedente previsione di un procedimento in camera di consiglio con un *nuovo procedimento* instaurabile con ricorso innanzi al tribunale in composizione monocratica.

Come si legge nella relazione di accompagnamento al Codice, l'art. 152 introduce un procedimento molto snello, che tuttavia assicura pienamente alle parti le dovute garanzie, strutturato in modo da assicurare in tempi brevi la decisione.

²² “Gli articoli 147, 148 e 149 regolano le formalità di presentazione del ricorso, i casi di inammissibilità dello stesso e il relativo procedimento, in maniera pressoché pedissequa alla previgente normativa, salvo alcune precisazioni apparse necessarie al fine di assicurare una maggiore snellezza ed efficacia alla procedura.

In tal senso, fra l'altro, a seguito di qualche incertezza applicativa verificatasi, si è chiarito che il ricorso è proposto nei confronti del titolare ed è rivolto al Garante (art. 147, commi 1 e 4). In relazione all'evoluzione tecnologica, è previsto che il ricorso è validamente proposto anche se è trasmesso per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento dell'istanza.

Qualche intervento di razionalizzazione si registra nell'ambito del procedimento dove alcuni termini sono stati adeguati all'esperienza applicativa di questi anni, ivi compreso quello entro il quale il Garante deve adottare la propria decisione sul ricorso (sessanta giorni) (art. 149).

Da ultimo, si segnala un importante intervento in materia di spese del procedimento, in base al quale in caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese, o di suo rigetto, il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile (art. 150, comma 6)” (così la relazione di accompagnamento).

Secondo quanto disposto dall'art. 152 del testo unico²³, dunque, *tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del Codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.*

Per tutte le controversie di cui sopra l'azione si propone con *ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento*. Il tribunale decide in ogni caso in composizione monocratica.

Se è presentato avverso un provvedimento del Garante, il ricorso è proposto *entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito*. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

La proposizione del ricorso *non sospende l'esecuzione del provvedimento del Garante*. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.

Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.

Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al

²³ Cfr. art. 29 L. 675/1996.

Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.

Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.

Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.

Con la sentenza il giudice, anche in deroga al divieto di cui all'art. 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, *prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.*

La sentenza *non è appellabile*, ma è ammesso il ricorso per cassazione.

Sommario

3. Sanzioni

Il titolo III della parte III del Codice della privacy si occupa delle *sanzioni* distinguendo tra *violazioni amministrative* (capo I)²⁴ ed *illeciti penali* (capo II).

Alla luce della disciplina interessante le *comunicazioni elettroniche*, verranno dunque brevemente esaminate le disposizioni più rilevanti e pertinenti.

3.1. Violazioni amministrative

L'art. 161 del testo unico²⁵ punisce l'*omessa o inidonea informativa all'interessato* prevedendo che la violazione delle disposizioni di cui all'art. 13 del Codice²⁶ è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di

²⁴ “Il capo I riguarda le fattispecie per la cui violazione è prevista l'applicazione di una sanzione amministrativa.

In tutti i casi l'importo delle sanzioni è stato adeguato alla nuova moneta dell'euro e opportunamente calibrato, come già analogamente effettuato in occasione di precedenti decreti, rispetto alla gravità delle violazioni e all'effettività della sanzione. Nell'applicazione della legge n. 675/1996, si è registrata, infatti, in vari casi, la particolare esiguità delle sanzioni, anche in rapporto al livello di altre sanzioni amministrative pecuniarie introdotte in altri settori dell'ordinamento, tale da non costituire un efficace deterrente anche in ragione delle particolari condizioni economiche dei titolari cui, spesso, sono irrogate le sanzioni medesime.

Si registra un unico intervento integrativo della normativa, in base al quale può essere applicata, in ogni caso, a titolo di sanzione accessoria, la pubblicazione dell'ordinanza-ingiunzione del Garante. La previsione non riguarda, ovviamente, la fattispecie dell'omessa o incompleta notificazione ove la sanzione accessoria è già prevista come obbligatoria (art. 165)” (così la relazione di accompagnamento).

²⁵ Cfr. art. 39 L. 675/1996.

²⁶ Sull'art. 13 (“Informativa”) v. cap. II, par. 5.

trattamenti che presentano rischi specifici ai sensi dell'art. 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

Il successivo art. 162²⁷ prevede inoltre che la *cessione dei dati* in violazione di quanto previsto dall'art. 16, comma 1, lett. b)²⁸, o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

In ordine alla *notifica del trattamento*, l'art. 163²⁹ sancisce che chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli artt. 37 e 38³⁰, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della *pubblicazione dell'ordinanza-ingiunzione*, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica³¹.

²⁷ Cfr. art. 16 L. 675/1996.

²⁸ Sull'art. 16 ("Cessazione del trattamento") v. cap. II, par. 5.

²⁹ Cfr. art. 34 L. 675/1996.

³⁰ Sugli artt. 37 e 38 v. cap. II, par. 12.

³¹ In base all'art. 164, inoltre, chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli artt. 150, comma 2 (sul quale v. par. 2.1.), e 157 è punito con la sanzione amministrativa del pagamento di una somma da lire quattromila euro a lire ventiquattromila euro.

Ai sensi del successivo art. 165, nei casi di cui agli artt. 161, 162 e 164, appena esaminati, può essere applicata la sanzione amministrativa accessoria della *pubblicazione dell'ordinanza-ingiunzione*, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Con riguardo al *procedimento di applicazione* delle sanzioni sopra illustrate, l'art. 166 prevede che l'organo competente a ricevere il rapporto e ad irrogare le sanzioni è *il Garante*. Si osservano, in quanto applicabili, le disposizioni della già richiamata legge 24 novembre 1981, n. 689, e successive modificazioni.

In materia di *spamming*, occorre infine ricordare che l'art. 179 del Codice va a modificare l'art. 12 del D.L.vo 185/1999, dedicato alla disciplina dei contratti a distanza conclusi dai consumatori.

Come accennato nel capitolo II, l'art. 12 del D.L.vo 185/1999 detta le sanzioni per la violazione dell'art. 10 del medesimo provvedimento, relativo ai "Limiti all'impiego di talune tecniche di comunicazione a distanza"³². Il comma 1 della disposizione in parola prevede dunque che, fatta salva l'applicazione della legge penale qualora il fatto costituisca reato, il fornitore che contravviene alle norme di cui all'art. 10 è punito con la sanzione amministrativa pecuniaria da 516 euro a 5.160 euro.

Le sanzioni sono applicate ai sensi della L. 689/1981. Fermo restando quanto previsto in ordine ai poteri di accertamento degli ufficiali e degli agenti di polizia giudiziaria dall'art. 13 della predetta L. 689/1981³³, all'accertamento delle violazioni provvedono, d'ufficio o su denuncia, gli organi di polizia amministrativa.

In base alla modifica apportata dal Codice della privacy al comma 3 dell'art. 12 D.L.vo 185/1999, il rapporto previsto dall'art. 17 L. 689/1981³⁴, nel caso di

³² V. cap. III, par. 11.6.

³³ V. cap. IV, nota n. 76.

³⁴ L'art. 17 L. 689/1981 dispone quanto segue.

violazione dell'art. 10 D.L.vo 185/1999 in materia di spamming, deve oggi essere presentato al *Garante per la protezione dei dati personali*³⁵.

3.2. Illeciti penali

L'art. 167 del Codice della privacy³⁶ punisce il *trattamento illecito di dati* stabilendo che, salvo che il fatto costituisca più grave reato, chiunque, *al fine di*

“Obbligo del rapporto. Qualora non sia stato effettuato il pagamento in misura ridotta, il funzionario o l'agente che ha accertato la violazione, salvo che ricorra l'ipotesi prevista nell'art. 24, deve presentare rapporto, con la prova delle eseguite contestazioni o notificazioni all'ufficio periferico cui sono demandati attribuzioni e compiti del Ministero nella cui competenza rientra la materia alla quale si riferisce la violazione o, in mancanza, al prefetto.

Deve essere presentato al prefetto il rapporto relativo alle violazioni previste dal testo unico delle norme sulla circolazione stradale, approvato con d. p. r. 15 giugno 1959, n. 393, dal testo unico per la tutela delle strade, approvato con r. d. 8 dicembre 1933, n. 1740 e dalla l. 20 giugno 1935, n. 1349, sui servizi di trasporto merci.

Nelle materie di competenza delle regioni e negli altri casi, per le funzioni amministrative ad esse delegate, il rapporto è presentato all'ufficio regionale competente.

Per le violazioni dei regolamenti provinciali e comunali il rapporto è presentato, rispettivamente, al presidente della giunta provinciale o al sindaco.

L'ufficio territorialmente competente è quello del luogo in cui è stata commessa la violazione.

Il funzionario o l'agente che ha proceduto al sequestro previsto dall'art. 13 deve immediatamente informare l'autorità amministrativa competente a norma dei precedenti commi, inviandole il processo verbale di sequestro.

Con decreto del Presidente della Repubblica, su proposta del Presidente del Consiglio dei Ministri, da emanare entro centottanta giorni dalla pubblicazione della presente legge, in sostituzione del d. p. r. 13 maggio 1976, n. 407, saranno indicati gli uffici periferici dei singoli Ministeri, previsti nel primo comma, anche per i casi in cui leggi precedenti abbiano regolato diversamente la competenza.

Con il decreto indicato nel comma precedente saranno stabilite le modalità relative alla esecuzione del sequestro previsto dall'art. 13, al trasporto ed alla consegna delle cose sequestrate, alla custodia ed alla eventuale alienazione o distruzione delle stesse; sarà altresì stabilita la destinazione delle cose confiscate. Le regioni, per le materie di loro competenza, provvederanno con legge nel termine previsto dal comma precedente”.

³⁵ Prima della modifica, il rapporto andava presentato all'ufficio provinciale dell'industria, del commercio e dell'artigianato della provincia di residenza o sede legale dell'operatore commerciale.

trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 18, 19, 23³⁷ e, in particolare, con riguardo alle comunicazioni elettroniche, 123, 126 e 130, ovvero in applicazione dell'art. 129, è punito, se dal fatto deriva *nocumento*, con la *reclusione da sei a diciotto mesi* o, se il fatto consiste nella *comunicazione o diffusione*, con la *reclusione da sei a ventiquattro mesi*.

Con specifico riferimento alla materia che qui interessa, con pene piuttosto severe, la norma va a colpire dunque la violazione delle disposizioni del Codice sui *dati relativi al traffico*, sui *dati relativi all'ubicazione*, sulle *comunicazioni indesiderate* (spamming) e sugli *elenchi di abbonati*, in precedenza esaminate³⁸.

Il reato configurato dall'art. 167, ovviamente *doloso*, richiede altresì la presenza di *dolo specifico* in capo al soggetto agente (*fine di profitto o di danno*) e, quale *condizione obiettiva di punibilità*³⁹, il verificarsi di un *nocumento*.

³⁶ Cfr. art. 35 L. 675/1996; art. 11 D.L.vo 171/1998.

“L'art. 167 riproduce pressoché pedissequamente l'art. 35 della legge 675/1996, con un unico intervento di razionalizzazione in base al quale si rendono punibili le condotte ivi richiamate solo se dal fatto derivi *nocumento*, mentre in precedenza il *nocumento* costituiva solo un'aggravante.

Le condotte punibili riproducono, oltre a quelle già contenute nel citato art. 35 della legge 675/1996, anche quelle punite ai sensi del medesimo articolo 35 dall'art. 11 del d. lg. 171/1998.

[...] Le pene edittali sono state pienamente adeguate a quanto richiesto dalla Commissione giustizia del Senato” (così la relazione di accompagnamento).

L'art. 11 dell'abrogato D.L.vo 171/1998 disponeva quanto segue.

“1. Per la violazione delle disposizioni di cui agli articoli 4, 9 e 10, restano ferme le sanzioni di cui all'articolo 35 della legge [675/1996]”.

³⁷ Sugli artt. 18 (“Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici”), 19 (“Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari”) e 23 (“Consenso”), v. cap. II, parr. 6 e 7.

³⁸ V. cap. III, parr. 4, 7, 10 e 11.

³⁹ Art. 44 cod. pen.

Deve rilevarsi che *nessuna sanzione*, né amministrativa né penale, è invece prevista per la violazione dell'art. 122 del Codice, relativo alle *informazioni raccolte nei riguardi dell'abbonato o dell'utente* che mira a disciplinare, tra l'altro, l'aspetto alquanto delicato dell'uso di *cookies* e *spyware*⁴⁰. Ciò non comporta, naturalmente, l'irrelevanza dal punto di vista civilistico della condotta, con riguardo ai danni, anche non patrimoniali, che questa cagioni⁴¹.

Ai sensi del comma 2 della disposizione in esame, inoltre, salvo che il fatto costituisca più grave reato, chiunque, *al fine di trarne per sé o per altri profitto o di recare ad altri un danno*, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45 del testo unico⁴², è punito, *se dal fatto deriva nocumento*, con la reclusione da uno a tre anni⁴³.

Con riferimento alle *misure di sicurezza*, l'art. 169 del testo unico⁴⁴ sancisce che chiunque, essendovi tenuto, omette di adottare le *misure minime* previste dall'art. 33⁴⁵ è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

⁴⁰ V. cap. III, par. 3. Sul punto, si veda M. Cammarata, "Spyware", *qualcosa non va nel codice della privacy*, in *InterLex*, www.interlex.it, www.interlex.it/675/spyware.htm; A. Monti, *Codici deontologici: se chi ruba i dati può scrivere le regole* cit.

⁴¹ V. cap. II, par. 5.

⁴² Si veda in proposito quanto detto nel capitolo II.

⁴³ Si ricorda anche l'art. 168 ("Falsità nelle dichiarazioni e notificazioni al Garante"; cfr. art. 37bis L. 675/1996) secondo cui chiunque, nella notificazione di cui all'art. 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

⁴⁴ Cfr. art. 36 L. 675/1996.

⁴⁵ La norma si riferisce alle sole *misure minime*, sulle quali v. cap. II, parr. 11 e ss.

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un *termine per la regolarizzazione* non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a *sei mesi*. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare *una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione*. L'adempimento e il pagamento estinguono il reato⁴⁶.

Ai sensi dell'art. 170 ("Inosservanza di provvedimenti del Garante"), chiunque, essendovi tenuto, non osserva il *provvedimento* adottato dal Garante ai sensi degli artt. 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lett. c), è punito con la reclusione da tre mesi a due anni⁴⁷.

Si ricorda infine che la condanna per uno dei *delitti* previsti dal Codice importa la *pubblicazione della sentenza* (art. 172).

Sommario

4. È sanzionabile la spedizione di una prima e-mail di richiesta di consenso per il successivo invio di comunicazioni commerciali?

⁴⁶ L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli artt. 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758 (*Modificazioni alla disciplina sanzionatoria in materia di lavoro*), e successive modificazioni, in quanto applicabili.

⁴⁷ Sugli artt. 150 ("Provvedimenti a seguito di ricorso") e 143 ("Procedimento per i reclami"), v. par. 2.1.

La *comunicazione commerciale*, di natura promozionale o imprenditoriale, è garantita costituzionalmente dalla libertà d'impresa. Essa è infatti direttamente connessa al principio di cui all'art. 41 della Costituzione italiana⁴⁸.

Il vigente Codice della privacy – così come la direttiva 2002/58/CE sulle comunicazioni elettroniche da esso recepita – non contiene una definizione di *comunicazione commerciale*, contrariamente al D.L.vo 70/2003 di attuazione della direttiva 2000/31/CE sul commercio elettronico.

L'art. 130 del testo unico sulla privacy, come in precedenza illustrato, dispone che le *comunicazioni elettroniche* effettuate mediante *posta elettronica*⁴⁹ a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale sono consentite solo con il *consenso dell'interessato*, salva l'eccezione di cui al comma 4 della medesima disposizione⁵⁰.

Secondo l'art. 4 del Codice della privacy, per *comunicazione elettronica* deve intendersi “ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico”, come ivi definito⁵¹.

⁴⁸ V. Spataro, *Comunicazione, Internet e diritto*, in *Trattato breve di diritto della Rete* cit., p. 47. Si veda anche V. Spataro, *La pubblicità on line*, in *INTERNET. Nuovi problemi e questioni controverse* cit., pp. 191 ss.; M. Quaranta, *Pubblicità on line*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., pp. 482 ss.; A. Della Monica, *La pubblicità on line. Caratteristiche generali*, in *Il commercio via Internet* cit., pp. 151 ss.

⁴⁹ Quanto si dirà nel testo con riferimento alla posta elettronica può essere esteso anche agli altri mezzi (sistemi automatizzati di chiamata, telefax, messaggi MMS, SMS o di altro tipo) contemplati dall'art. 130, commi 1 e 2, del Codice della privacy, salva la necessità di verificare per ognuno la configurabilità di una delle cause di esclusione del consenso di cui all'art. 24 del testo unico.

⁵⁰ Cap. III, par. 11.4.

⁵¹ Cap. II, par.2.

Il Codice di autodisciplina pubblicitaria⁵² afferma che per *pubblicità* deve intendersi *ogni comunicazione diretta a promuovere la vendita di beni o servizi quali che siano i mezzi utilizzati*. La raccolta di usi pubblicitari della Camera di Commercio di Milano definisce la *pubblicità* come *qualsiasi forma di comunicazione che sia diffusa nell'esercizio di una attività commerciale, industriale, artigianale o professionale, allo scopo di promuovere la domanda di beni e servizi*.

L'art. 2 del D.L.vo 74/1992⁵³, recante l'attuazione della direttiva 84/450/CEE come modificata dalla direttiva 97/55/CE in materia di pubblicità ingannevole e comparativa, definisce, ai fini del provvedimento, la *pubblicità* come *qualsiasi forma di messaggio che sia diffuso, in qualsiasi modo, nell'esercizio di un'attività commerciale, industriale, artigianale o professionale allo scopo di promuovere la vendita di beni mobili o immobili, la costituzione o il trasferimento di diritti ed obblighi su di essi oppure la prestazione di opere o di servizi*.

“Nel dare applicazione alla disposizione, l'Autorità garante della concorrenza e del mercato adotta, in genere, il criterio in base al quale la natura pubblicitaria di una comunicazione d'impresa è rinvenibile ogniqualvolta la promozione di beni o servizi si presenti come lo scopo 'primario e diretto' della comunicazione stessa.

Tale accertamento, concernente lo scopo diretto o mediato, primario o secondario, della promozione, viene preliminarmente eseguito sul contenuto della comunicazione, tenendo conto sia delle caratteristiche espressive della comunicazione sia del contesto primario in cui la diffusione risulta essere avvenuta.

⁵² Consultabile su www.iap.it all'indirizzo www.iap.it/it/codice.htm.

⁵³ D.L.vo 25 gennaio 1992, n. 74, *Attuazione della direttiva 84/450/CEE, come modificata dalla direttiva 97/55/CE in materia di pubblicità ingannevole e comparativa*, GU Serie gen. 36 del 13 febbraio 1992, e successive modifiche.

Nessun rilievo determinante assume, invece, la qualificazione data alla comunicazione da parte dell'operatore pubblicitario.

La giurisprudenza individua la corretta nozione di 'pubblicità commerciale' sulla base dei connotati essenziali dell'oggetto (la comunicazione sociale) e dello scopo (un incremento dei profitti attraverso la sollecitazione della domanda e dei consumi) in relazione ad un determinato prodotto o servizio dell'industria o del commercio" (E. Caruso)⁵⁴.

Il trattamento di dati personali⁵⁵ consistente nell'invio di una e-mail senza previo consenso del destinatario, bensì al solo fine di ottenere da costui il consenso per la successiva spedizione di comunicazioni commerciali via posta elettronica, risulta sanzionabile alla luce della disciplina di cui al vigente testo unico (art. 167)⁵⁶?

Occorre innanzitutto stabilire se un siffatto messaggio possa essere fatto rientrare nel campo di applicazione del regime di *opt-in* configurato, quale regola generale

⁵⁴ E. Caruso, *Pubblicità e comunicazioni mobili*, in *Diritto delle nuove tecnologie informatiche e dell'INTERNET* cit., p. 90.

⁵⁵ Si ricorda che per *trattamento*, ai fini del Codice della privacy (art. 4), deve intendersi qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati.

⁵⁶ Fatto salvo quanto previsto, *entro il suo ambito applicativo*, dal D.L.vo 185/1999 sui contratti a distanza conclusi dai consumatori (cap. III, par. 11.6).

Come visto nel paragrafo precedente, si ricorda che l'art. 167 del Codice della privacy punisce con una *sanzione penale* chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto, per quel che qui interessa, dagli artt. 23 e 130 del testo unico, salvo che il fatto costituisca più grave reato e sempreché dal fatto derivi nocumento.

Trattandosi di norma penale, giova altresì sottolineare che dovranno trovare applicazione i relativi criteri ermeneutici.

per le comunicazioni commerciali, dal sopra citato art. 130 del Codice della privacy, collocato nel titolo X della parte II del testo unico, recante la disciplina delle comunicazioni elettroniche⁵⁷.

A parere di chi scrive, non possono ritenersi – *di per sé* – comunicazioni commerciali *le informazioni che consentono un accesso diretto all'attività dell'impresa, del soggetto o dell'organizzazione, come un nome di dominio o un indirizzo di posta elettronica*. In ordine, in particolare, all'indirizzo di posta elettronica l'aspetto *identificativo* deve infatti considerarsi prevalente su quello distintivo. Ciò in linea con la definizione di “comunicazioni commerciali” accolta – sebbene ai soli fini del provvedimento – dal D.L.vo 70/2003 di attuazione della direttiva europea sul commercio elettronico⁵⁸.

Secondo il provvedimento da ultimo citato, infatti, 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 un soggetto che esercita un'attività agricola, commerciale, industriale, artigianale o una libera professione.

Non sono di per sé comunicazioni commerciali:

1) le informazioni che consentono un accesso diretto all'attività dell'impresa, del soggetto o dell'organizzazione, come un nome di dominio, o un indirizzo di posta elettronica;

⁵⁷ Sull'ambito di applicazione del titolo X della parte II del Codice (art. 121), v. cap. III, par. 1.

⁵⁸ Sul quale si rimanda al cap. IV.

2) le comunicazioni relative a beni, servizi o all'immagine di tale impresa, soggetto o organizzazione, elaborate in modo indipendente, in particolare senza alcun corrispettivo”.

Una e-mail con la quale l'operatore si limiti a richiedere il consenso per il successivo inoltro di comunicazioni commerciali, indicando, a tal fine, *esclusivamente* i propri dati *identificativi* – e, ragionevolmente, entro limiti rigorosi, anche il proprio settore di attività – non pare dunque possa essere fatta rientrare nella previsione di cui all'art. 130, commi 1 e 2, del Codice della privacy, il quale, come sopra visto, si riferisce esclusivamente all'uso dell'e-mail:

- per l'invio di *materiale pubblicitario* o
- di *vendita diretta* o
- per il *compimento di ricerche di mercato* o
- di *comunicazione commerciale*.

Il genere di messaggio in discorso si pone infatti in una fase antecedente a quella della promozione propriamente intesa, che avrà invece eventualmente inizio solo con l'invio della prima comunicazione commerciale autorizzata dal destinatario.

Conseguentemente, per stabilire la liceità dell'invio di dette comunicazioni a prescindere dal previo consenso informato dell'interessato occorrerà rifarsi alle norme generali di cui agli odierni artt. 23 e 24 del testo unico sulla privacy⁵⁹.

⁵⁹ Come visto nel capitolo II, in base all'art. 6 del Codice della privacy le *disposizioni generali* della parte I del provvedimento sono infatti destinate a trovare applicazione rispetto a tutti i trattamenti di dati personali, fatte salve le disposizioni integrative o modificative della parte II relative a determinati trattamenti.

Tra le ipotesi di *esclusione del consenso* contemplate dall'art. 24, vi è, come già rilevato, anche quella, riformulata dal testo unico, dei *dati relativi allo svolgimento di attività economiche* (art. 24, lett. d))⁶⁰.

La corrispondente disposizione dell'abrogata L. 675/1996 (art. 12, lett. f)) contemplava espressamente i dati relativi allo svolgimento di attività economiche raccolti anche a fini di informazioni commerciali o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva⁶¹.

Nonostante tale ultimo inciso sia stato eliminato dal vigente art. 24 del Codice della privacy, deve comunque ritenersi che la nozione di “dati relativi allo svolgimento di attività economiche” ivi contenuta sia in grado di ricomprendere oggi anche l'ipotesi dell'indirizzo di posta elettronica – *ad uso non esclusivamente privato*⁶² – trattato ai soli fini dell'invio di una richiesta di consenso per la spedizione di future comunicazioni commerciali.

Come sopra visto, infatti, tale genere di messaggi neppure può definirsi, in sé, “comunicazione commerciale”, mentre i dati personali trattati ai fini della comunicazione certamente attengono “allo svolgimento di attività economiche”.

Ove ne ricorrano i presupposti, potrà inoltre trovare applicazione anche l'ipotesi di esclusione del consenso di cui all'odierno art. 24 lett. c), concernente i *dati*

⁶⁰ V. cap. II, par. 7.

⁶¹ Su questa ipotesi di esclusione del consenso, v. S. Melchionna, *Il significato delle ipotesi di esclusione del consenso*, in *Privacy.it*, www.privacy.it, www.privacy.it/melchionna01.html.

⁶² V. cap. II, nota n. 62.

*provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque*⁶³.

Naturalmente, l'interessato, al quale deve comunque essere fornita un'adeguata *informativa ex art. 13 del Codice della privacy*, potrà – e dovrà essere messo in *condizioni di* – esercitare nei confronti del suddetto trattamento del suo indirizzo di posta elettronica tutti i diritti che gli sono riconosciuti dall'art. 7 del testo unico; in particolare, il diritto di opposizione *per motivi legittimi* di cui all'art. 7, comma 4, lett. a)⁶⁴.

Alla luce di quanto sopra, almeno con riferimento al *B2B*⁶⁵, la tipologia di messaggio in discorso dovrebbe dunque intendersi soggetta ad un regime di *opt-out*, con le dovute conseguenze sia sul piano della responsabilità penale sia sul piano della responsabilità civile⁶⁶.

⁶³ Su questa ipotesi di esclusione del consenso, con particolare riferimento agli indirizzi e-mail reperiti sul Web, si rimanda a quanto detto nel cap. III, par. 12; v. inoltre T. Minella, *La Privacy. Guida all'applicazione della legge 675/1996* cit., pp. 60 ss.

⁶⁴ E non il diritto di opposizione di cui all'art. 7, comma 4, lett. b) in quanto, secondo l'interpretazione accolta nel testo, l'e-mail di richiesta di consenso non può essere fatta rientrare nell'ipotesi ivi prevista (v. cap. II, par. 4). Per la stessa ragione, l'e-mail in parola non sarà soggetta agli obblighi previsti per le comunicazioni commerciali dal D.L.vo 70/2003 (cap. IV, par. 6); né dovrebbe rientrare nell'ambito contemplato dall'art. 140 del Codice della privacy, relativo ai codici di deontologia e di buona condotta nel marketing diretto (cap. III, par. 11.5).

Sul contenuto dell'informativa da rendere all'interessato, v. cap. II, par. 5.

⁶⁵ Si ricorda, tra l'altro, che, come già rilevato, l'art. 13, par. 5, della direttiva 2002/58/CE, in ordine alle comunicazioni commerciali indesiderate, *non richiedeva* la necessaria adozione di un regime di opt-in anche per gli "abbonati che non siano persone fisiche" (cap. III, par. 11.3 e 11.4).

L'applicazione delle esaminate ipotesi di esclusione del consenso si presenta invece più problematica nell'ambito del *B2C (Business to Consumer)*, per tutte le ragioni a suo luogo esposte. Come si ricorderà, l'art. 12 del D.L.vo 185/1999, nel prevedere le sanzioni per la violazione dell'art. 10 del predetto provvedimento, fa *salva l'applicazione della legge penale qualora il fatto costituisca reato*.

⁶⁶ Sulla responsabilità civile, v. cap. II, par. 5.

I principi di cui all'art. 11 del Codice della privacy⁶⁷ suggeriscono d'altra parte di adottare ulteriori cautele a tutela del destinatario, quali ad esempio:

- limitare il più possibile il “peso” del messaggio per ridurre i tempi di *download* ed i relativi costi;
- effettuare un trattamento *istantaneo* dell'indirizzo e-mail, senza procedere dunque alla sua archiviazione in banche dati;
- effettuare un invio *una tantum* o comunque entro un lasso di tempo ragionevolmente ampio;
- inviare l'e-mail di richiesta di consenso solo a coloro che hanno diffuso il proprio indirizzo di posta in Rete per ragioni il più possibile pertinenti all'oggetto delle future comunicazioni commerciali;
- dare all'e-mail un *oggetto chiaro* che la renda precisamente ed immediatamente identificabile;
- prevedere, infine, *modalità che rendano il più agevole ed efficace possibile l'esercizio del diritto di opposizione per motivi legittimi da parte del destinatario del messaggio.*

Nei confronti del trattamento in esame, saranno del resto applicabili, ove ne ricorrano i presupposti, tutte le pertinenti norme del Codice della privacy analizzate nei capitoli precedenti, in particolare quelle relative alle misure di sicurezza.

⁶⁷ Cap. II, par. 5.

La ricostruzione proposta consente di evitare eccessive restrizioni per gli operatori commerciali, a fronte di un sacrificio ridotto per i destinatari dei messaggi, i quali potranno opporsi in ogni momento alla ricezione di ulteriori comunicazioni analoghe⁶⁸.

D'altra parte, lo stesso Garante per la protezione dei dati personali, nel suo recente provvedimento generale sullo spamming⁶⁹, ha rilevato che l'invio di una prima e-mail di richiesta di consenso costituisce elusione della normativa sulla privacy solo nel caso il messaggio *abbia comunque un contenuto promozionale oppure pubblicitario*, o se riconosca solo un diritto di tipo opt-out al fine di non ricevere più messaggi *dello stesso tenore*.

Finalità promozionali oppure pubblicitarie che, come sopra illustrato, paiono non sussistere nel caso di messaggi di posta elettronica i quali si limitino a richiedere la manifestazione di un consenso in ordine al ricevimento di *futuri* messaggi a contenuto promozionale o pubblicitario.

[Sommar](#)

⁶⁸ Cfr. M. Cammarata, *Il principio di finalità e la finalità del principio*, in *InterLex*, www.interlex.it, www.interlex.it/675/principio.htm, secondo cui “i messaggi inviati da operatori commerciali possono non essere considerati inutilmente invasivi da parte di altri operatori [...] Dunque è necessario non fare di ogni erba un fascio e dettare norme più aperte per quello che possiamo definire come *spamming businnes to businnes*. La quasi completa assimilazione delle persone fisiche con enti e persone giuridiche compiuta dalla legge italiana non è condivisa a livello comunitario e la nuova direttiva [2002/58/CE] lascia aperta la regolamentazione dell'invio di messaggi commerciali a destinatari che non siano persone fisiche [...] Si deve considerare un altro punto: per ottenere il consenso preventivo può essere indispensabile inviare una richiesta. Altrimenti come fa il destinatario a esprimere il consenso stesso? Questo è un aspetto che deve essere risolto, perché vietare una prima comunicazione che contenga solo la richiesta di consenso al trattamento può costituire un ostacolo allo svolgimento di legittime attività economiche”.

Con riferimento all'abrogato D.L.vo 171/1998, v. M. Maglio, *Il trattamento dei dati personali e la tutela della vita privata nel settore delle telecomunicazioni: il decreto legislativo del 13 maggio 1998 n. 171. Stampa e privacy: molto rumore per nulla?*, in *Privacy.it*, www.privacy.it, www.privacy.it/maglio10.html.

⁶⁹ In proposito si rimanda al cap. III, par. 12.