EMILIO TOSI

PRIME OSSERVAZIONI SULL'APPLICABILITÀ DELLA DISCIPLINA GENERALE DELLA TUTELA DEI DATI PERSONALI A INTERNET E AL COMMERCIO ELETTRONICO

1. Le regole giuridiche del commercio elettronico.

Il progressivo crescente utilizzo di Internet anche per finalità commerciali — e non più solo di scambio di informazioni a titolo di cortesia o nell'esercizio di attività istituzionali *non-profit* — ha richiamato l'attenzione del giurista su una serie di problemi resi ancora più complessi dalla internazionalità del fenomeno.

L'importanza del nuovo mezzo di comunicazione non è sfuggita al recente D.lgs. 31 marzo 1998, n. 114 — recante norme relative al settore del commercio — che all'art. 21 stabilisce — fra l'altro — quanto segue:

« Il ministero dell'industria (...) promuove l'introduzione e l'uso del commercio elettronico con azioni volte a:

a) sostenere una crescita equilibrata del commercio elettronico;

b) tutelare gli interessi dei consumatori; (...)

f) garantire la partecipazione italiana al processo di cooperazione e negoziazione europea ed internazionale per lo sviluppo del commercio elettronico ».

L'oggetto del presente studio sarà limitato all'esame dei profili giuridici connessi alla tutela della privacy « online » ai sensi della L. 31 dicembre 1996, n. 675 e del D.lgs. 31 maggio 1998, n. 171; in particolare si illustreranno il problema del controllo degli utenti di Internet da parte degli *internet provider*; il problema della tutela dei dati personali raccolti *online* in occasione di attività di commercio elettronico; il problema della raccolta invisibile dei dati

personali; il problema della posta elettronica a contenuto pubblicitario[1].

Tuttavia — preliminarmente all'esame dei principi introdotti dalla L. 675/96 applicabili ad Internet e al commercio elettronico — sembra opportuno inquadrare il fenomeno del commercio « online »[2].

Il quadro normativo rilevante in materia di commercio elettronico — oltre che dai già citati profili della tutela della riservatezza — può essere desunto dall'esame dalle seguenti problematiche:

— rilevanza giuridica degli accordi formati « online » per comportamento concludente (c.d. « point and click » agreement) o mediante inizio dell'esecuzione (è il caso dell'invio — con effetto solutorio — dei numeri della carta di credito);

— rilevanza giuridica della firma digitale ai sensi del D.P.R. 10 novembre 1997, n. 513 (attuativo della L. 15 marzo 1997, n. 59 - c.d. « Bassanini Uno »);

— tutela dei consumatori « online » ai sensi degli artt. 1469 *bis* e ss. cod. civ. (clausole abusive), del D.lgs. 15 gennaio 1992, n. 50 (contratti negoziati fuori dei locali commerciali), del D.lgs. 22 maggio 1999, n. 185 (contratti a distanza) e del D.lgs. 25 gennaio 1992, n. 74 (pubblicità ingannevole);

— legge applicabile, giurisdizione e arbitrato.

Particolarmente significativo, ai fini della presente trattazione, può essere la disamina sintetica delle modalità di conclusione del contratto nella prassi negoziale del commercio elettronico.

Il contratto a forma libera, indipendentemente dal mezzo tecnico utilizzato, si conclude quando « chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte » (art. 1326 c.c.). Il contratto, secondo il *principio della ricezione*, s'intende perciò concluso nel momento in cui la dichiarazione giunge all'indirizzo del destinatario.

Anche nel caso del « contratto virtuale » concluso per *e-mail* o attraverso il *world wide web* (www) di Internet — così come per i contratti conclusi secondo i mezzi di comunicazione tradizionali — si ritiene applicabile l'art. 1335 c.c. che consente la presunzione di conoscenza quando proposta ed accettazione « giungono

---

[1] Sulla tutela dei dati personali in generale si vedano FRANCESCHELLI (a cura di), *La tutela della privacy informatica*, Milano, 1998; CUFFARO - RICCIUTO - ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998; ALPA, *La disciplina dei dati personali*, Roma, 1998; BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997.

[2] Sul punto mi permetto rinviare al mio studio, *La conclusione di contratti* « online », in *I problemi giuridici di Internet*, a cura di E. TOSI, Milano, 1999.

all'indirizzo del destinatario, se questi non prova di essere stato senza sua colpa nell'impossibilità di averne notizia ».

L'indirizzo *e-mail*, inserito sulla carta intestata o diffuso *on-line* via Internet e l'indirizzo del sito web (WWW) su Internet, devono essere considerati « indirizzo » — ai sensi e per gli effetti dell'art. 1335 c.c. — cui far pervenire comunicazioni rilevanti ai fini della conclusione del contratto.

Il D.P.R. 513/97 in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici o telematici, *cit.*, all'art. 12, comma 1 (*Trasmissione del documento*) stabilisce, infatti, che: « Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'*indirizzo elettronico* da questi dichiarato ».

Sarà, quindi, onere del soggetto che invii proposte contrattuali a mezzo di *e-mail* — analogamente a quanto si ritiene in relazione al titolare di casella postale reale — controllare periodicamente la posta in arrivo.

In base al principio di autoresponsabilità e all'interpretazione del contratto secondo buona fede si presuppone che chi intende disciplinare la propria attività contrattuale mediante strumenti elettronici sia d'accordo nell'accettarne i relativi effetti e quindi anche la conclusione del contratto nel momento in cui viene registrata la dichiarazione negoziale nel suo domicilio informatico, indipendentemente dal momento in cui giungerà a conoscenza effettiva dell'interessato: conoscenza che potrà essere conseguente all'utilizzo diligente, per esempio, della funzione di *check-mail*.

Per quanto riguarda, invece, la firma digitale — introdotta dal D.P.R. 513/97 — si ricorrerà necessariamente a tale strumento unicamente per la conclusione « online » di contratti per i quali sia prevista dalla legge la forma scritta *ad substantiam* o *ad probationem*.

Si osservi, infine, che la corrispondenza elettronica — via *e-mail* o via *web* — deve essere assimilata - quanto alla tutela della segretezza — alla corrispondenza in forma scritta: depone in tal senso la previsione di sanzioni penali anche per la violazione della corrispondenza elettronica (artt. 617-*quater*, 617-*quinquies*, 617-*sexies* c.p.) e la recente previsione dell'art. 13 del D.P.R. 513/97.

Prima di procedere alla disamina dei principali problemi connessi all'applicabilità della L. 675/96 a Internet — e al commercio elettronico — corre l'obbligo di far rilevare che — a tutt'oggi — non è stata ancora esercitata la delega al Governo contenuta nella L. 676/96 che individua — all'art. 1, comma, 1 lett. *n*) — le reti telematiche come uno dei casi richiedenti norme *ad hoc* — integrative ed attuative di quelle generali — al fine di « stabilire modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via

telematica, individuando i titolari del trattamento di dati inerenti i servizi accessibili al pubblico e la corrispondenza privata, nonché i compiti dei gestori, anche in rapporto alle connessioni con reti sviluppate su base internazionali ».

La mancanza della predetta normativa di settore non impedisce, però, di applicare a Internet e al commercio elettronico — compatibilmente con la particolare natura tecnica del mezzo di comunicazione considerato — i principi generali della L. 675/96.

In senso favorevole all'applicabilità della Direttiva comunitaria 24 ottobre 1995, n. 46 — relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali — e Direttiva comunitaria 15 dicembre 1997, n. 66 — relativa alla tutela della vita privata nel settore delle telecomunicazioni — si è espresso anche il *Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali* — istituito dall'art. 29 della Direttiva 95/46 — rilevando che: « Sotto il profilo giuridico Internet non opera nel vuoto: il trattamento dei dati personali su Internet deve pertanto rispettare i principi della tutela dei dati così come avviene al di fuori della rete. Ciò non limita assolutamente il ricorso ad Internet, ma al contrario fa parte degli elementi fondamentali volti ad assicurare la fiducia degli utenti nel funzionamento di Internet e dei servizi forniti da esso. La tutela dei dati su Internet è quindi una condizione indispensabile per l'accettazione del commercio elettronico »[3].

2. La tutela dei dati personali su Internet e il controllo degli utenti-navigatori: il problema del « Data Log ».

Esaminiamo, innanzitutto, il problema del controllo degli utenti-navigatori da parte dei fornitori di accesso alla rete Internet. È buona regola che ciascun *Internet provider* anche quando consenta l'utilizzo di pseudonimi o garantisca l'anonimato in rete provveda all'atto della stipula del contratto di accesso all'identificazione dell'utente mediante verifica di valido documento d'identificazione.

Nello stesso senso si esprime l'art. 4a) e 5) della bozza di *Codice di autoregolamentazione per i servizi Internet* adottata dall'AIIP/Telecom Italia[4].

---

[3] Documento di lavoro *Trattamento dei dati personali su Internet* adottato dal *Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali* il 23 febbraio 1999. Si veda anche la dichiarazione ministeriale del Convegno sulle reti globali d'informazione, tenutosi a Bonn nel luglio del 1997, disponibile all'indirizzo: http://www2.echo.lu/bonn/conference.html.

[4] Vedilo in Appendice al volume a cura di E. Tosi, *I problemi giuridici di Internet*, cit., 626 ss.

L'art. 4a) stabilisce come principio generale l'identificabilità di tutti i soggetti di Internet e la possibilità del soggetto identificato di restare anonimo durante l'utilizzo della rete a tutela della propria riservatezza[5].

L'art. 5 stabilisce che i soggetti di Internet devono consentire l'acquisizione dei propri dati personali a chi fornisca loro accesso, *hosting* o entrambi. I fornitori di detti servizi sono tenuti a registrare i dati per renderli disponibili a richiesta dell'autorità giudiziaria. Una volta identificato, l'utente può chiedere al suo fornitore di accesso e *hosting* di avere un identificativo diverso dal suo nome (pseudonimo) con cui operare in Rete (anonimato protetto).

Si prevede, inoltre, che i soggetti firmatari del Codice si obblighino ad estendere ai terzi l'obbligatorietà del Codice stesso attraverso la previsione di un'apposita « clausola di estensione » in tutti i contratti di fornitura di accesso a Internet e di *hosting* che verranno stipulati.

In linea con quanto detto è anche il *Codice di deontologia e di buona condotta per i servizi telematici* adottato dall'Associazione Nazionale Fornitori di Video Audio Informazione (ANFOV) approvato nel novembre 1997 ed entrato in vigore il 1º gennaio 1998 che all'art. 6 stabilisce[6]:

« I fornitori di accesso e di servizi (...) accertano l'identità degli utenti e degli abbonati richiedendo l'esibizione o la produzione di un documento personale (...) mantengono un *log* attraverso il quale sia possibile risalire all'identità degli utenti o degli abbonati (...) ».

L'art. 6 del Codice di deontologia ANFOV pone, quindi, a carico del fornitore di accesso o di servizi l'onere di mantenere un registro elettronico c.d. *Data Log* attraverso cui sia possibile:

— risalire alla identità degli utenti o degli abbonati che hanno fatto accesso o concesso a terzi la facoltà di accedere al sistema o alla rete telematica, in via temporanea o permanente;

— risalire all'identità degli utenti o degli abbonati che hanno utilizzato il servizio o concesso a terzi la facoltà di utilizzarlo per diffondere o distribuire contenuti.

Nel caso di commissione di reati a mezzo Internet può essere, infatti, di fondamentale importanza per il *provider* individuare l'autore dell'illecito al fine di escludere o limitare eventuali proprie responsabilità penali o civili. E a maggior ragione nel caso

[5] Sul problema dell'anonimato in rete si veda anche la Raccomandazione del *Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali* n. 3/97 - *Anonimato su Internet* - del 3 dicembre 1997.

[6] Vedilo in Appendice al volume a cura di E. Tosi, *I problemi giuridici di Internet*, cit., 616 ss.

in cui l'utente abbia commesso l'illecito grazie all'anonimato assicurato dal *provider*.

Sino all'8 maggio 1997, data dell'entrata in vigore della legge sulla « privacy » (L. 675/96), tali controlli venivano effettuati — spesso all'insaputa dell'utente, in assenza di un preciso quadro normativo di riferimento — mediante l'utilizzo di diverse tipologie di registri elettronici contenenti ora la semplice durata dei collegamenti alla rete Internet ora il tracciamento completo dei movimenti virtuali degli utenti.

Solo raramente la modulistica contrattuale richiamava espressamente l'utilizzo di detto registro elettronico; non certo per informare l'utente ma solo per ottenere la specifica adesione al suo utilizzo, in caso di controversia, quale prova, piena ed incontrovertibile, dei fatti e degli atti compiuti dall'abbonato medesimo in relazione all'*Internet provider* fornitore dei servizi.

La prassi della conservazione di detto registro elettronico soddisfa, oltre che finalità tecniche di controllo dell'efficienza del sistema, finalità di tutela contrattuale ed extracontrattuale del *provider*.

Tutela contrattuale, potendo essere utilizzato, in un eventuale giudizio, al fine di dimostrare la durata degli accessi al servizio Internet e la correttezza degli importi addebbitati, anche in relazione alla verificazione del rispetto da parte dell'utente degli eventuali limiti d'uso mensile o annuale e alla conseguente applicazione di tariffe diversificate.

Tutela extracontrattuale, potendo essere utilizzato, a richiesta dell'autorità giudiziaria, per verificare la commissione di eventuali illeciti civili e penali da parte degli utenti del *provider*. Sono, inoltre, evidenti, in tal caso, le finalità dissuasive dalla commmissione di reati derivanti dalla consapevolezza dell'utente — quando informato, correttamente, di tale controllo — che i comportamenti virtuali tenuti su Internet sono registrati dal *provider* e possono essere valutati dall'Autorità Giudiziaria per sanzionare eventuali violazioni di legge.

Anteriormente alla legge sulla « privacy », che ha introdotto limiti e regole generali al trattamento dei dati personali, pur essendo dubbia la legittimità di tale strumento — che può costituire una forma penetrante di violazione dell'altrui « privacy », in difetto di espressa disposizione di legge che attribuisca al *provider* il potere-dovere di provvedere alla conservazione di detto registro — non si poteva andare oltre le affermazioni di principio per impedire eventuali abusi in assenza di un quadro normativo di riferimento.

Successivamente all'entrata in vigore della legge 675/96 sulla tutela della riservatezza l'utilizzo e la conservazione — non richiesta, nemmeno oggi, da alcuna disposizione di legge — da parte del *provider* del registro elettronico in parola, ha subito forti limitazioni a tutela dell'interessato dal trattamento dei dati personali.

È del tutto evidente, infatti, che un registro in cui sia possibile immagazzinare dati relativi alla navigazione dell'utente, consente al *provider* di creare un dettagliato profilo personale del navigatore virtuale, anche con riferimento a dati sensibili quali, per esempio, orientamento politico o sessuale.

Per non parlare del rischio di un utilizzo illecito di tali dati; si pensi a finalità estorsive, da parte del *provider* stesso o da parte di terzi che riescano ad accedere al contenuto di detto registro.

Per poter continuare ad utilizzare detto registro, che può anche contenere, come si è visto, dati sensibili occorre, pertanto, rispettare alcuni principi generali introdotti dalla legge sulla privacy a partire dall'8 maggio 1997.

In primo luogo, il *provider*, oltre alle informazioni che deve dare all'interessato ai sensi dell'art. 10, L. 675/96, deve informare adeguatamente e correttamente, oralmente o per iscritto, l'interessato-utente dell'esistenza di tale registro, della natura dei dati ivi registrati (precisando se ad esempio si tratti della mera registrazione dei tempi d'accesso o dei dati relativi ai siti visitati e/o al loro contenuto), della finalità (finalità di fatturazione, finalità commerciali, finalità di controllo), della durata e delle modalità del trattamento.

L'interessato-utente, ricevuta l'informativa, deve fornire il suo indispensabile consenso al trattamento che deve essere documentato per iscritto (*ad probationem*, quindi) in caso di dati non sensibili e prestato in forma scritta, a pena di invalidità (*ad substantiam*, quindi), solo in caso di dati sensibili.

In difetto del consenso dell'interessato-utente si ritiene che il *provider* non possa utilizzare il registro elettronico in parola salvo che venga contrattualmente previsto per registrare esclusivamente i tempi d'accesso ad Internet: trattandosi di trattamento necessario per l'esecuzione dell'obbligo di pagamento del canone di accesso da parte dell'interessato-utente — finalità di fatturazione — non è, infatti, richiesto il consenso *ex* art. 12.1 lett. *a*) L. 695/96.

Nello stesso senso depone l'art. 4 del D.lgs. 13 maggio 1998, n. 171 — recante norme in materia di tutela della riservatezza nel settore delle telecomunicazioni — secondo cui « 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 finalità di fatturazione — nel qual caso il trattamento è consentito fino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento — e le finalità di commercializzazione di servizi di telecomunicazioni — nel qual caso occorre, però, il consenso dell'interessato.

Nulla dice, invece, il D.lgs. 171/98 in relazione al trattamento dei dati personali per finalità di controllo dell'utente da parte del fornitore del servizio di telecomunicazioni che dovrà, quindi,

essere oggetto di specifica pattuizione contrattuale — con riguardo anche alla durata del trattamento — e di consenso informato in forma scritta a pena di nullità, potendo l'attività di controllo interessare anche il trattamento di dati sensibili.

Le violazioni dell'art. 4 del D.lgs. 171/98 comportano l'applicazione delle sanzioni penali di cui all'art. 35 della L. 675/96 previste per il trattamento illecito dei dati personali (reclusione sino a due anni e in caso di danno sino a 3 anni).

In secondo luogo, il *provider* dovrà notificare al Garante il trattamento automatizzato iniziato a partire dal 1° gennaio 1998 preventivamente all'inizio dello stesso (nel caso di trattamento automatizzato dei dati iniziato prima del 1° gennaio 1998 il termine ultimo per l'adempimento era il 31 marzo 1998) e richiedere l'autorizzazione del Garante per il trattamento dei dati personali sensibili qualora non risultino applicabili le *Autorizzazioni generali* per categorie di trattamento predisposte dal Garante.

In terzo luogo, il *provider* deve sin da ora, anche se la legge 675/96 concede sei mesi di tempo dall'emanazione del regolamento contenente le misure minime di sicurezza da osservare, adottare le misure di sicurezza informatica necessarie per garantire, come già adesso richiede l'art. 15 comma 1 della legge citata, il rispetto della riservatezza e dell'integrità dei dati contenuti nel registro elettronico, anche al fine di evitare che tali dati vengano utilizzati per finalità illecite.

È quindi tenuto ad installare, seguendo le indicazioni di consulenti in sicurezza informatica, protezioni fisiche (allarmi, chiavi hardware, sistemi biometrici) e virtuali (firewall, chiavi software, sistemi crittografici) a tutela del sistema informatico e dei supporti che contengono tali dati.

Si ricorda, in proposito, che l'art. 2.3 del D.lgs. 171/98 pone a carico del fornitore di un servizio di telecomunicazioni accessibile al pubblico, l'obbligo informativo di rendere edotto l'utilizzatore del servizio dell'esistenza di particolari rischi di violazione della sicurezza della rete, indicando i possibili rimedi e i relativi costi.

Si osservi, infine, che l'art. 15 della proposta di Direttiva dell'Unione Europea del 18 novembre 1998, n. 586 sul commercio elettronico esclude — salve espresse richieste formulate dall'autorità giudiziaria per finalità di salvaguardia della sicurezza nazionale, difesa, pubblica sicurezza e per la prevenzione, investigazione, individuazione e sanzione di attività criminali — qualsiasi obbligo generale del *provider* di monitorare l'attività degli utenti.

3. La tutela dei dati personali nel commercio elettronico: il problema dell'informativa e del consenso « online ».

La prassi del commercio elettronico è, senza dubbio, caratterizzata da numerose occasioni di raccolta dei dati personali del navi-

gatore — consumatore « virtuale », ora palesi — mediante la richiesta di compilazione di generici formulari elettronici o di veri e propri ordini di beni o servizi — ora occulte — si pensi al caso emblematico dei « cookie » di cui si dirà successivamente.

Anche la raccolta e il trattamento dei dati personali via Internet devono essere improntati al rispetto dei principi generali indicati dalla L. 675/96.

In particolare sembra opportuno richiamare i seguenti principi generali:

— il *principio di liceità e trasparenza* del trattamento dei dati personali posto dall'art. 9;

— il *principio dell'informativa* all'interessato posto dall'art. 10;

— il *principio del consenso* dell'interessato posto dall'art. 11;

— il *principio della notificazione* al Garante del trattamento di dati personali da parte del titolare posto dall'art. 7;

— il *principio di sicurezza* del trattamento posto dall'art. 15.

Le norme richiamate — come già si è detto in relazione al problema del controllo degli utenti — costituiscono un importante parametro di valutazione della liceità del trattamento dei dati personali su Internet e nel commercio elettronico.

L'art. 9 della L. 675/96 è di fondamentale importanza perchè fornisce all'interprete i criteri generali di valutazione della liceità del trattamento, utili anche ai fini dell'azione risarcitoria di cui all'art. 18 per il caso di danni derivanti da trattamento illecito. In particolare detto articolo stabilisce che i dati personali oggetto di trattamento devono essere:

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 non incompatibili con tali scopi;

c) esatti e se necessario aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per cui sono raccolti o successivamente trattati;

d) conservati come dati personali per un periodo non superiore a quello necessario per le finalità per cui sono stati raccolti o successivamente trattati.

L'art. 10 della L. 675/96 prevede l'obbligo del titolare del trattamento[7] di informare — oralmente o per iscritto — l'interessato

[7] Nel corso della presente relazione si è spesso parlato di titolare del trattamento: ma in relazione a quali dati trasmessi via Internet si può parlare di titolarità? La Direttiva comunitaria 95/46 sulla tutela dei dati personali chiarisce nel 47° considerando che relativamente ai messaggi di posta elettronica e per quelli immessi in aree liberamente consultabili da tutti gli utenti deve considerarsi titolare del trattamento colui che è autore del messaggio anziché la persona che effettua il servizio di trasmissione;

— o la persona presso la quale sono raccolti i dati personali — preliminarmente al trattamento circa:

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

— la natura obbligatoria o facoltativa del conferimento dei dati;

— le conseguenze di un eventuale rifiuto di rispondere;

— i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

— i diritti di cui all'art. 13;

— il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile.

Non vi è dubbio che l'informativa di cui all'art. 10 possa e debba essere resa anche in forma elettronica — via Internet — ogni qualvolta si proceda alla raccolta di dati del navigatore — consumatore « virtuale ».

In tal senso depone anche l'art. 10 del *Codice di deontologia e di buona condotta per i servizi telematici* adottato dall'Associazione Nazionale Fornitori di Video Audio Informazione (ANFOV) il quale stabilisce che:

« 1. L'informativa, a norma della L. 675/96 e sue successive modificazioni deve contenere:

a) le finalità e modalità delle operazioni di comunicazione e conservazione dei dati personali (anche di quelli raccolti automaticamente come i *log* o le intestazioni delle *e-mail*);

b) le comunicazioni e operazioni registrate ed il tempo di conservazione di tali registrazioni.

2. Le informative chiariscono anche quali dati siano accessibili agli altri utenti e abbonati. Prima dello svolgimento di un'operazione, l'utente e l'abbonato devono avere una chiara contezza della circostanza che l'operazione può essere oggetto di monitoraggio.

3. Le formule adottate per l'informativa sono collocate in modo chiaramente visibile e sono di facile comprensione.

4. L'informativa deve essere posizionata in ogni luogo, sito o pagina da cui vengono raccolte informazioni personali ».

Ma veniamo all'ipotesi — tipica del commercio elettronico — di raccolta dei dati necessari per la conclusione del « contratto » « virtuale ».

Normalmente si tratterà di dati anagrafici e fiscali necessari per la stipula e l'esecuzione del contratto e come tali rientranti nell'esclusione del consenso dell'interessato di cui all'art. 12.1 lett. *b*).

---

quest'ultima sarà, invece, da considerarsi *titolare* con riferimento ai dati personali necessari per il funzionamento del servizio di accesso alla rete (si pensi al c.d. *data log*).

Per trattare tali dati in senso conforme alle disposizioni della L. 675/96 sarà, quindi, sufficiente che il soggetto che effettua la raccolta dei dati « online » in occasione e per la stipula di un contratto via Internet, informi con la massima trasparenza l'interessato degli scopi della raccolta e degli altri elementi previsti dall'art. 10 della L. cit., non essendo necessario anche il consenso dell'interessato.

Il problema del consenso si porrà, invece, nel caso in cui il *provider* — o il fornitore di beni o servizi *online* — utilizzi i dati personali raccolti per la conclusione del contratto per finalità diverse dalla stipula ed esecuzione dello stesso, oppure provveda a raccogliere dati dell'interessato non strettamente necessari alla stipula e alla esecuzione del contratto.

Trattasi di dati personali che pur essendo necessari alla stipula e alla esecuzione del contratto non vengono utilizzati solo per tali finalità ma anche per altre — si pensi ad esempio per attività di *web-marketing* — oppure di dati personali che per loro natura — siano essi dati comuni o a maggior ragione dati sensibili — non sono necessari alla stipula del contratto.

Referente normativo in materia di consenso è l'art. 11 il quale stabilisce che:

« 1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 10 ».

Questa la regola per i dati comuni.

Per i dati sensibili — ossia quelli 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 idonei a rivelare lo stato di salute e la vita sessuale — l'art. 22 della L. 675/96 prevede che il trattamento possa essere effettuato solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, ove non siano applicabili le autorizzazioni generali.

In buona sostanza — al di fuori dei casi di esclusione del consenso di cui all'art. 12 — per trattare *dati comuni* non necessari per la stipula e l'esecuzione del contratto oppure necessari alla stipula e all'esecuzione del contratto ma utilizzati per finalità diverse, sarà sufficiente che il titolare del trattamento documenti per iscritto — quindi *ad probationem* — il consenso dell'interessato; mentre per trattare *dati sensibili* occorrerà che il titolare del trattamento ottenga il consenso scritto — quindi *ad substantiam* — dell'interessato a pena di nullità e la relativa autorizzazione

del Garante al trattamento dei dati sensibili qualora non siano applicabili le *autorizzazioni generali* per determinate categorie di trattamento rilasciate in via preventiva dal Garante.

Si tratta a questo punto di chiarire la validità del consenso dell'interessato prestato *online*.

Esaminiamo innanzitutto il caso del consenso per il trattamento dei dati sensibili eventualmente raccolti via Internet. *Nulla quaestio* sulla inidoneità del consenso per via telematica atipica[8] a produrre gli effetti del consenso per iscritto. L'unica modalità ammissibile al fine di ottenere un consenso scritto, validamente prestato per via telematica è quello di ricorrere alle modalità e garanzie tecniche tipizzate dal D.P.R. 513/97 recante norme in materia di firma digitale e del relativo regolamento tecnico esecutivo[9]. L'interessato dovrà quindi utilizzare la firma digitale per prestare validamente via Internet il consenso al trattamento dei dati personali sensibili.

Il quadro giuridico relativo al consenso *ad probationem* prestato per il trattamento dei dati comuni non necessari alla stipula ed esecuzione del contratto o utilizzati per finalità diverse non pone alcun problema in caso di utilizzo della forma telematica tipica introdotta dalla firma digitale di cui al D.P.R. 513/97.

Ma *quid iuris* in caso di consenso per dati comuni manifestato utilizzando la forma telematica atipica di Internet senza utilizzare, quindi, le specifiche modalità tecniche introdotte dal D.P.R. 513/97?

È conclusione, ormai dominante in dottrina, la qualificazione del documento elettronico quale documento in senso giuridico[10].

Sembrerebbe, quindi, ragionevole ritenere ammissibile e valido il consenso prestato attraverso *e-mail* o via *web* al fine di soddisfare il requisito della documentazione scritta richiesta dall'art. 11.3 L. 675/96 per il trattamento dei dati comuni.

Non si dimentichi, infatti, che la L. 675/96 sembra accontentarsi — al fine di soddisfare il requisito della documentazione per

---

[8] Relativamente alla distinzione tra forma telematica tipica e atipica mi permetto rinviare al mio studio, *La forma del contratto di subfornitura*, in *Subfornitura*, a cura di V. FRANCESCHELLI, Milano, 1999, 98 ss.

[9] D.P.C.M. 8 febbraio 1999 (in *G.U.* 15 aprile 1999, n. 87).

[10] Il documento elettronico è ormai pacificamente qualificato come documento in senso giuridico sia attraverso la dimostrazione che anche nella forma elettronica sono riscontrabili le caratteristiche essenziali della forma scritta (FRANCHESCHELLI, *Computer, documento elettronico e prova civile*, in *Giur. it.*, 1988, IV, 314 ss. BORRUSO, *Computer e diritto*, Milano, I, 1988, 219; PARISI, *Il contratto concluso mediante computer*, Padova, 1987 70; STALLONE, *La forma dell'atto giuridico elettronico*, in *Contratto e Impresa*, 1990, 770-771), sia attraverso la configurabilità di una autonoma « forma elettronica » dotata di garanzie analoghe a quelle richieste dal legislatore alla forma scritta (CLARIZIA, *Informatica e conclusione del contratto*, Milano, 1985, 86).

iscritto del consenso *ex* art. 11.3 L. cit. — anche della comunicazione del consenso in forma orale[11] ed è quindi più permissiva della normativa di diritto comune che richiede pur sempre — anche per la forma scritta *ad probationem* — la manifestazione del consenso mediante documento dotato di sottoscrizione[12] al quale — evidentemente — il documento elettronico — privo della firma digitale — non può essere equiparato[13].

4. La raccolta invisibile dei dati personali: il problema dei « cookie ».

Esaminiamo ora uno strumento — ricorrente nella prassi del commercio elettronico — utilizzato per memorizzare determinati comportamenti del navigatore-consumatore, normalmente a sua insaputa: trattasi del c.d. *cookie*.

Il *cookie* non è altro che un contenitore di informazioni — normalmente di carattere commerciale — che viene inviato — attraverso il *browser* — dal sito *web* che si sta visitando alla memoria interna del computer utilizzato per la navigazione.

L'utilità di tale strumento va rinvenuta nella possibilità di personalizzare determinati aspetti della navigazione in funzione dei consumi e degli interessi manifestati dall'utente nel corso della stessa.

Si pensi, fra l'altro, alla possibilità del sito di riconoscere l'utente e di calibrare il contenuto dei *banner* pubblicitari in funzione del profilo ricostruito dal *cookie* in relazione ai dati raccolti nel corso di navigazioni precedenti.

Ma tale raccolta « invisibile » di dati è compatibile o meno con la tutela della privacy?

Secondo Manganelli — componente dell'Autorità Garante per la Protezione dei Dati Personali — il *cookie* non sarebbe stru-

[11] Buttarelli, *cit.*, 282.

[12] Si osservi che in ogni caso il consenso prestato attraverso *e-mail* o via *web* potrebbe essere interpretato — in senso conforme alla prassi instauratasi nel settore bancario — come comportamento concludente atto a manifestare — quantomeno provvisoriamente — il consenso dell'interessato al trattamento di dati comuni. Sul problema del consenso si vedano Vignali, *Il consenso delll'interessato al trattamento dei dati*, in Franceschelli (a cura di), *La tutela della privacy informatica*, cit. 143; Cuffaro, *A proposito del ruolo del consenso*, 117 e Oppo, *Sul consenso dell'interessato*, 123 ss., entrambi in Cuffaro - Ricciuto - Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, cit.

[13] Si vedano in tal senso Zagami, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, cit., 158; Giannantonio, *Manuale di diritto dell'informatica*, Padova, 1997, 354 il quale ritiene che pur essendo considerato un documento in senso giuridico, il documento elettronico non è equiparabile alla scrittura privata in senso tecnico poiché non vi è apponibile la sottoscrizione.

mento illecito di raccolta dei dati solo nei limiti in cui non sia possibile attraverso i dati da esso registrati identificare il navigatore, e quindi associare il profilo tracciato ad un soggetto individuato[14].

A diverse conclusioni — nel senso della illiceità ai sensi della L. 675/96 — si deve evidentemente pervenire qualora il c.d. *cookie* registri — senza il consenso dell'interessato — un profilo del consumatore non in forma anonima ma riferibile immediatamente ad un utente individuato oppure non si limiti alla registrazione di dati di natura commerciale ma trasferisca informazioni relative al contenuto della memoria di massa del computer di navigazione.

In entrambi i casi sembra, però, ragionevole ritenere — tenuto conto delle problematiche relative alla legge applicabile e alla eterogeneità dei livelli di protezione — che lo strumento migliore di tuela del navigatore dalla raccolta occulta di informazioni che lo riguardano, sia in definitiva l'*autotutela* e quindi — in questo caso — l'utilizzo avanzato dei *browser* di navigazione che allo stato della tecnologia sono in grado di segnalare all'utente quando un *cookie* sta per essere registrato sul proprio computer, così consentendogli di impedirne — se del caso — la registrazione.

Sul punto si è espresso anche il *Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali* — di cui si è già detto *supra* — esprimendosi a favore dell'applicabilità al trattamento dei dati invisibili via Internet delle Direttive comunitarie 95/46 e 97/66 ed invitando i progettisiti di software e hardware a tenere conto e rispettare i principi posti da queste al fine di rafforzare la « privacy » degli utenti Internet[15].

5. Limiti di liceità dell'invio di posta elettronica pubblicitaria alla luce della L. 675/96 e del D.lgs. 171/98.

Come si è rilevato all'inizio di questa relazione, Internet è nata come strumento di comunicazione *non-profit* e solo successivamente — con l'affermarsi del commercio elettronico — è divenuta

[14] Manganelli, *Il Sole 24 Ore* , 24 ottobre 1997, inserto Informatica, II.

[15] Raccomandazione n. 1/99 — *Sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware* — del 23 febbraio 1999. Sulla tutela della privacy in Internet si vedano anche Buttarelli, *cit.*, 577 ss. e Poullet, *Riservatezza e sicurezza delle reti*, in *Internet e Privacy: quali regole?*, Suppl. n. 1 al Boll. n. 5/1998, *Garante per la protezione dei dati personali*, 22 ss.

strumento usuale di trasmissione di proposte contrattuali e messaggi pubblicitari[16].

Le regole autodisciplinari di buon comportamento — *Netiquette* — che ogni nuovo utente si impegna a rispettare con la stipula del contratto di accesso ai servizi della rete, stabiliscono, infatti, il divieto di utilizzare la posta elettronica per inviare messaggi di natura pubblicitaria non richiesti esplicitamente dal destinatario.

Sono, invece, ammessi i c.d. *banner* che non sono altro che spazi pubblicitari virtuali inseriti nei siti di natura commerciale.

Ciò nonostante il fenomeno dello *spamming* (noto anche come *junk- mail*), ossia il frequente invio di messaggi non desiderati dal destinatario, spesso a contenuto pubblicitario, è destinato a progressiva diffusione.

Il disagio derivante da tale pratica illecita sotto più profili — disciplinare, civile e penale — consiste, essenzialmente, nel rallentamento delle funzioni del sistema informatico utilizzato dal destinatario di tali messaggi indesiderati con conseguente indebito aggravio dei costi di accesso. L'utente — pur essendo sempre in grado di scegliere il materiale da visionare o meno — si trova, però, inerme di fronte al meccanismo automatizzato di scaricamento della posta elettronica, che riversa sul sistema tutto il materiale pervenuto all'indirizzo *e-mail*.

Attualmente sono, comunque, disponibili sul mercato programmi di filtraggio della *e-mail* che consentono un buon livello di protezione dalla corrispondenza elettronica indesiderata.

L'invio reiterato di posta elettronica pubblicitaria non richiesta né gradita viene sanzionato dagli utenti della rete con il c.d. *flaming*, ossia l'invio alla casella di posta elettronica del mittente di numerosi messaggi di protesta che — se compiuto da un numero elevato di utenti — può, persino, avere per effetto quello di paralizzare l'utilizzo ordinario della casella del soggetto mittente.

La discutibile prassi commerciale dello *spamming* sembra, tuttavia, ricadere nella previsione di cui all'art. 10 del recente D.lgs. 13 maggio 1998, n. 171 in base al quale « 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 comu-

[16] Sull'argomento si vedano ZENO ZENCOVICH, *La pubblicità telematica nei servizi di telecomunicazione*, AIDA, 5/1996, 251 ss.; GAMBINO, *La pubblicità telematica*, in *Concorrenza e Mercato*, 5/1997, 403 ss.; IMPERIALI R. - IMPERIALI R., *La tutela della privacy in azienda*, Milano, 1998, 161; e da ultimo VALERIANI, *La direttiva 97/7/CE in materia di vendita a distanza e la pubblicità via Internet*, in questa *Rivista*, 1999, 208 ss.

nicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato ».

La violazione dell'art. 10 del D.lgs. 171/98 comporta l'applicazione delle sanzioni penali di cui all'art. 35 della L. 675/96 previste per il trattamento illecito dei dati personali (reclusione sino a due anni e in caso di danno sino a 3 anni).

Si osservi, inoltre, che il nuovo regolamento del servizio telefonico Telecom (D.M. 8 maggio 1997, n. 197) all'art. 26 prevede quanto segue:

« 1. L'abbonato non può servirsi del proprio impianto per effettuare comunicazioni che arrechino molestia o che violino le leggi vigenti.

2. L'abbonato non può utilizzare il servizio in modo da creare turbativa ad altri abbonati.

3. L'abbonato si impegna a non consentire ad altri di utilizzare il suo telefono per telefonate moleste.

4. Il gestore ha la facoltà di sospendere immediatamente il servizio senza preavviso qualora l'abbonato ne faccia l'uso improprio indicato nei casi precedenti dandone, se del caso, idonea comunicazione alle autorità competenti ».

Da quanto sopra si evince chiaramente che — anche anteriormente all'entrata in vigore del D.lgs. 171/98 — nel concetto di « turbativa » telefonica poteva rientrare — stante la contrarietà alle norme di autodisciplina della *Netiquette* — l'invio di posta elettronica pubblicitaria non richiesta.

Il soggetto disturbato dall'attività di *web marketing* poteva, quindi avvalersi — anche anteriormente alla tutela introdotta dal D.lgs. 171/98 — della tutela assicurata dal gestore della rete telefonica consistente nella facoltà di questo di sospendere il servizio dell'abbonato che ne faccia uso improprio e di segnalare il fatto alle autorità competenti.

Corre l'obbligo, infine, di far cenno al testo della già citata proposta di direttiva dell'Unione Europea del 18 novembre 1998 avente ad oggetto la regolamentazione del commercio elettronico.

Le comunicazioni commerciali sono disciplinate dagli artt. 6 (Informazioni da fornire) e 7 (Comunicazioni commerciali non richieste).

All'art. 6 si stabilisce che:

« Gli Stati membri prevedono nelle loro legislazioni che la comunicazione commerciale soddisfi i seguenti requisiti:

a) la comunicazione pubblicitaria deve essere chiaramente identificabile come tale;

b) deve essere chiaramente identificabile la persona fisica o giuridica per conto della quale è fatta la comunicazione pubblicitaria;

c) offerte promozionali, sconti, premi e omaggi, ove autorizzati, devono essere chiaramente identificabili come tali e le condizioni

necessarie per beneficiarne devono essere facilmente accessibili e presentate in modo preciso e non equivocabile;

d) concorsi promozionali o giochi, ove autorizzati, devono essere chiaramente identificabili come tali e le condizioni per la partecipazione devono essere facilmente accessibili e presentate in modo preciso e non equivocabile ».

L'art. 7 — della proposta di Direttiva 586/98 citata — prevede, infine, che:

« Gli Stati membri prevedono nelle loro legislazioni che la comunicazione commerciale non sollecitata per posta elettronica sia chiaramente e inequivocabilmente identificabile come tale non appena ricevuta dal destinatario ».