Capitolo XI

di Gianluigi Ciacci

LA TUTELA DEI DATI PERSONALI SU INTERNET

Sommario: 1. Introduzione. – 2. La rete Internet e la lesione della riservatezza dell'individuo. – 2.1. Le possibilità di violazione della posta elettronica. – 2.2. La possibilità di ricostruire il profilo dell'utente: il problema dei « data log ». – 2.3. Le possibilità lesive dei c.d. « cookie » e dei motori di ricerca. – 3. Internet e la disciplina dell'elaborazione informatica di dati personali. – 3.1. Applicabilità della legge n. 675/96 all'attività di trattamento di dati personali connessa ad Internet. – 3.2. La posizione del Garante in materia di offerta di accesso gratuito ad Internet. – 3.3. Applicabilità della legge n. 675/96 alla trasmissione di dati personali attraverso Internet. – 4. Tutela della riservatezza di documenti, corrispondenza, e comunicazioni in transito su Internet. – 4.1. Intercettazioni e sorveglianza elettronica da parte di soggetti pubblici. – 4.2. Intercettazioni e sorveglianza elettronica da parte di soggetti privati. – 4.3. La disciplina introdotta dall'art. 3 del d.lgs. 13 maggio 1998, n. 171. – 4.4. La posizione del Garante in materia di corrispondenza elettronica. – 5. Conclusioni.

1. – Introduzione.

Tre anni dopo l'entrata in vigore della legge italiana sul trattamento dei dati personali, la legge n. 675 del 31 dicembre 1996, la situazione del nostro paese in termini di diffusione delle nuove tecnologie e del loro uso si può considerare profondamente mutata: i gestori della telefonia cellulare riportano più di quindici milioni di abbonati ai loro servizi, usati sempre più anche in maniera alternativa alla semplice telefonia vocale (1), mentre l'avvento

(1) Si pensi al successo dei brevi messaggi di testo, i c.d. *SMS (Short Message System)*, che è possibile inviare attraverso i terminali cellulari, ma anche alle nuove applicazioni *WAP*

della possibilità di connessione gratuita ad Internet ha portato gli utenti della Rete in Italia a quadruplicare il loro numero, ed il mercato del commercio elettronico ad avviare le prime concrete applicazioni. A fronte della indicata nuova prospettiva in cui il nostro Paese si pone oggi rispetto agli altri maggiormente industrializzati, non è purtroppo possibile registrare un'effettiva corrispondente crescita in termini di « maturità informatica », cioè di effettiva consapevolezza delle specifiche peculiarità dei nuovi *media*, e dei servizi da essi resi possibili. E, tra queste peculiarità, si devono ricomprendere anche i possibili rischi legati all'uso di tali tecnologie (2), tra i quali nel presente scritto prenderemo in considerazione quelli legati alla tutela dei dati personali rispetto alle attività di trattamento connesse alla rete Internet (3).

Tale nuova forma di elaborazione a distanza delle informazioni, raro esempio di standardizzazione nel mondo dell'informatica (forse la principale ragione del suo incredibile successo) (4), accresce infatti decisamente il pericolo di lesioni della sfera privata dell'individuo, della sua riservatezza: da un lato, facilitando e rendendo accessibile la comunicazione tra computer lontani migliaia di chilometri (o anche pochi metri), permettendo quindi di moltiplicare gli archivi a disposizione di tutti; e, dall'altro, consentendo a chiunque di pubblicare a larga diffusione le proprie idee, spesso senza alcun

(Wireless Application Protocol), che consentono di collegarsi ad Internet e di utilizzare i servizi senza bisogno di un computer, direttamente con il telefonino.

(2) Occorre comunque precisare che i rilievi circa la pericolosità del mezzo non devono certo costituire un freno all'approccio al fenomeno dell'informatica e di Internet, ed in particolare all'approccio culturale a questo fenomeno: ed anzi devono rappresentare un elemento di stimolo allo studio ed all'approfondimento di tali argomenti, per meglio procedere alla loro disciplina. D'altro canto poi, nella legislazione italiana in mareria di trattamento dei dati personali, gi strumenti tradizionali cartacei vengono equiparati, quanto a pericolosità, ai nuovi mezzi informatici e telematici (così l'art. 5 della legge 31 dicembre 1996 n. 675).

(3) Relativamente alle caratteristiche proprie di Internet e dei servizi da essa resi possibili, si può fare riferimento ai vari manuali pubblicati sull'argomento, tra cui si veda ATTIVISSIMO P., *Internet per tutti*, Apogeo 2000, pp. 1-320, CRUMLISH C., *Internet No Problem*, Mc Graw-Hill, 1996, pp. 4-263. In tale sede basti evidenziare la sua natura di mezzo di telecomunicazione, e avvertire che si utilizzerà quale suo sinonimo la parola « Rete ».

(4) La particolare duttilità, economicità ed efficienza delle tecnologie connesse ad Internet, ha fatto sì che il metodo in cui avviene la gestione delle informazioni e la loro diffusione, il protocollo *TCP/IP (Transmission Control Protocol/Internet Protocol)*, fosse poi adottato da tutte le altre reti di telecomunicazione esistenti nel mondo, portando ad una standardizzazione « di fatto » nel settore della telematica.

tipo di controllo, e soprattutto senza alcuna capacità reattiva in genere degli ordinamenti in caso di violazioni di norme imperative (5). E in tale contesto sembra acuire la pericolosità del mezzo il nuovo mercato del commercio elettronico (6), sia perché ha portato ad un aumento dei soggetti che in concreto utilizzano la Rete, sia perché la maggior parte delle applicazioni ad esso attinenti implicano il trattamento di dati personali (si pensi anche semplicemente alla compilazione *on-line* del modulo d'ordine di un determinato bene o servizio ed al suo conseguente invio a destinatari spesso sconosciuti e non facilmente individuabili).

La predisposizione di archivi contenenti dati informatici strettamente personali, pur con le dovute precisazioni che verranno svolte nel presente scritto, è infatti molto semplice attraverso la Rete: le informazioni relative ai propri clienti, i contratti occasionali o anche solo le coordinate del proprio indirizzo I.P. (7), oltre alle informazioni che spontaneamente gli utenti

(5) Pur dovendo prestare attenzione nel non considerare il mondo virtuale di Internet uno spazio senza regole (dovendo in ogni caso applicarsi il diritto positivo, pur con i dovuti adattamenti: in tal senso si veda ALPA G., Cyberlaw, *Problemi giuridici connessi allo sviluppo di Internet*, in *Nuova Giurisprudenza Civile Commentata*, 1998, 6, p. 387, e LANCE R., *Netlaw*, McGraw-Hill, 1995, p. 120) possono essere riportati, quali esempi delle difficoltà che si incontrano nel tentativo di dare effettività alle statuizioni giuridiche nel *cyberspazio*, quello del libro *Le Grand Sécret* in Francia (su cui si veda SEDALLIAN V. e LAMGLOIS P., *Le grand secret ... le plus portagé du monde*, in *Planéte Internet*, marzo 1996, pp. 28-29, e BALLARINO T., *Internet nel mondo della legge*, CEDAM, 1998, p. 203), e quello negli U.S.A. del « *Communication Decency Act* », la sezione del più generale *Telecomunication Act del 1996*, dedicata a vietare la diffusione di materiale illecito su Internet (sulla vicenda del C.D.A. si vedano i siti web *http://www.aclu.org/court/renovacludec.html* consultato l'8 febbraio 2000 e *http://www.ciec.org/SC-appeal/decision.shtml* consultato il 24 gennaio 2000, e *Dir. Inf.*, 1996, p. 640, con nota di ZENO ZENCOVICH V.).

(6) La Commissione europea, nella comunicazione « Un'iniziativa europea in materia di commercio elettronico » [Com (97) 157] lo definisce come « lo svolgimento di attività commerciali e di transazioni per via elettronica che comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica; la distribuzione *on-line* di contenuti digitali; l'effettuazione per via elettronica di operazioni finanziarie e di borsa; gli appalti pubblici per via elettronica ed altre procednre di tipo transattivo delle Pubbliche Amministrazioni ». Per consultare la Comunicazione si può vedere il sito *web* all'indirizzo *http://www.cordis.lu/esprit/src/ecomcom.htm* visitato l' 8 febbraio 2000.

(7) L'*I.P. (Internet Protocol) address* è il numero che identifica in modo esatto la locazione di un « nodo » Internet, cioè di un computer che permette ai singoli utenti di accedere alla Rete (corrisponde quindi all'elaboratore del *provider*): conoscere l'*I.P.* di un utente implica identificare da quale gesrore di accesso proviene il contatto telematico, e quindi rappre-

di Internet abbiano ad esempio scritto nei c.d. *guestbook* ([8]), o nell'ambito della compilazione di questionari elettronici, sono frequentemente registrate, archiviate, analizzate o sfruttate per elaborare proiezioni di consumo, o comunque per acquisire altre più o meno lecite utilità.

Così, la materia della tutela della riservatezza, di per sé già estremamente delicata, soprattutto con riferimento al coordinamento con quella del diritto all'informazione, viene influenzata da Internet sotto due diversi punti di vista: da un lato, per quanto riguarda le intercettazioni e la sorveglianza elettronica, sia relativamente alle intercettazioni ed agli eventuali controlli da parte di soggetti pubblici (si pensi alle forze di polizia impegnate in attività di indagine), sia a quelli svolti da soggetti privati (come ad esempio nel caso del datore di lavoro rispetto all'uso della Rete da parte del dipendente); dall'altro, con riferimento all'attività di trattamento dei dati riguardanti la persona. Ed in entrambi i casi deve essere verificata l'adeguatezza o meno della normativa che disciplina la tutela dei dati personali nel nostro Paese, a rispondere alle mutate esigenze di protezione dell'individuo sollevate dal nuovo *media*: e non solo con riferimento all'attività dei privati, ma anche nei confronti della Pubblica Amministrazione. Infatti, sempre più numerosi sono gli apparati dello Stato che, con diversa rilevanza, hanno attivato una loro presenza su Internet: dai Ministeri agli uffici giudiziari, dal Parlamento agli enti locali, si registrano numerosi siti *web* « pubblici » che forniscono talvolta semplici servizi informativi, mentre altre volte permettono di svolgere veri e propri servizi e operazioni, dalla richiesta di certificati alla presentazione di documentazione fiscale. In questi casi la P.A. si pone sulla Rete come un vero e proprio « *content provider* », e sarà quindi soggetta a tutte le problematiche che si presentano a chi svolge attività su Internet. Ma allo stesso tempo si trova anche a dover affrontare i problemi del controllo *on-line* dei propri funzionari ed addetti, che usano sempre più le nuove metodologie comunicative, e che presto (una volta data piena attuazione al pro-

senta una prima informazione, anche se molto sintetica, relativamente all'urente. Sul punto si veda comunque oltre nel testo, al paragrafo 1.

([8]) I *guestbook* sono dei « registri elettronici » messi talvolta a disposizione dei visitatori dal gestore di un determinato sito *web* di Internet, al fine di permettere loro di scrivere un proprio commento, o semplicemente un saluto, visibile o meno a tutti gli altri successivi visitatori: spesso è possibile effettuare tale operazione solo dopo aver compilato una scheda contenente informazioni personali. Si veda comunque sull'argomento il primo paragrafo dedicato ai pericoli insiti nell'utilizzo della rete Internet.

getto della Rete Unitaria della Pubblica Amministrazione ([9])) si troveranno a prestare la propria opera essenzialmente attraverso collegamenti telematici.

Tali differenti aspetti verranno esaminati nel presente scritto, senza procedere comunque ad inquisitorie prese di posizione nei confronti del nuovo mezzo di comunicazione: ed anzi, da una parte, dando per scontata nel lettore la conoscenza relativa a che cosa sia Internet, e quali attività e servizi è possibile svolgere attraverso essa, e dall'altra analizzando comunque innanzitutto l'effettiva valenza lesiva della « Rete delle reti » al di là di facili semplificazioni sensazionalistiche a cui si è abituati nel leggere gli articoli, specialistici o meno, sull'argomento.

([9]) Il progetto Rete Unitaria della Pubblica Amministrazione (c.d. R.U.P.A.), avviato nel 1995 dall'Autorità per l'Informatica nella Pubblica Amministrazione (c.d. A.I.P.A.), trova il suo fondamento in un Dpcm del 5 settembre 1995, ed è stato concretizzato da uno « Studio di Fattibilità » pubblicato nel 1997: sua finalità è quella di rendere possibile l'interconnessione tra i diversi uffici della Pubblica Amministrazione (si calcola circa 10.000 postazioni di lavoro in tutta Italia), affinché, a prescindere dalle specificità del singolo sistema informatico della singola amministrazione, venga permessa la trasmissione e la condivisione, tra uffici diversi, di dati ed informazioni di natura contabile e/o amministrativa. L'architettura di rete è stata pensata dall'A.I.P.A. su modalità *I.P.*, le stesse che sono alla base di Internet. E proprio con la « Rete delle reti » è previsto che debba interagire R.U.P.A., sia per consentire ai pubblici amministratori di accedere al nuovo *media*, sia per rendere facilmente individuabili dai cittadini le risorse pubbliche a loro necessarie: ottenendo quindi una P.A. maggiormente efficiente e con minori sprechi di risorse ed economici, e un apparato-Stato effettivamente funzionante, al fine di conseguire una reale trasformazione dei rapporti tra Stato e collettività. La Rete Unitaria, che dovrebbe entrare in funzione in entrambi i suoi aspetti, quello del trasporto delle informazioni e dei dati (e quindi relativo alle telecomunicazioni ed alla telematica) e quello della interoperabilità tra uffici (e quindi relativo ai servizi informativi, informatici e telematici grazie ad essa usufruibili), nei prossimi mesi, avrà oggi una maggiore probabilità di successo grazie all'introduzione del sistema della firma digitale; sistema che andrà a risolvere il problema del fondamento giuridico dell'attività di documentazione elettronica, una delle due grosse difficoltà sulla strada del rinnovamento dell'apparato pubblico (l'altra riguarda l'aspetto culturale con riferimento alle nuove tecnologie, nel nostro Paese estremamente basso, soprattutto da parte degli operatori professionali non coinvolti nel settore). Su R.U.P.A. si veda direttamente lo *Studio di Fattibilità* pubblicato dall'A.I.P.A. nel gennaio 1996, e i vari bollettini della stessa Autorità, dal titolo *Informazioni*, ed in particolare il n. 10 dell'ottobre 1997, oltre alle notizie reperibili presso il suo sito web, all'indirizzo *http://www.aipa.it/progetti/rupa[1/* consultato il *4 gennaio 1999*; si veda poi MINERVA M., *Verso l'integrazione dei sistemi informativi pubblici: la rete unitaria della Pubblica Amministrazione*, in *Il diritto dell'informazione e dell'informatica*, 1998, 3, pp. 623-650, e IASELLI M., *La Rete Unitaria della Pubblica Amministrazione*, Simone Ed., *1999*, pp. 1-123.

2. – La rete Internet e la lesione della riservatezza dell'individuo.

Infatti, come per altre applicazioni che vengono giornalmente usufruite attraverso o sulla rete Internet, anche con riferimento agli aspetti di tutela della *privacy* nel mondo dei nuovi *media* spesso sono state riportate, dai vari organi di informazione, notizie errate circa la valenza negativa degli stessi: così, in diverse occasioni si sono registrate allarmanti notizie circa la presenza di fantomatici « Grandi Fratelli » che controllano la collettività attraverso la Rete, o di pericolosi *hacker* impegnati a intercettare le informazioni personali di coloro che utilizzano i servizi di messaggistica elettronica, o ancora di smaliziati « commercianti elettronici » che riescono a carpire i più reconditi desideri degli utenti del *wold wide web*.

In realtà, un'attenta lettura di tali notizie, chiaramente svolta anche attraverso un riscontro delle stesse su una base tecnica, permette di ridimensionare notevolmente i pericoli che sembrano correre gli utenti di Internet: come si dimostrerà nel presente paragrafo, in cui si esamineranno proprio le fattispecie comunemente riportate come lesive della *privacy* del navigatore *on-line* ([10]) per riscontrarne l'effettiva pericolosità, o comunque per un loro più corretto inquadramento.

Come è noto, comunicare, reperire, veicolare e diffondere le informazioni senza barriere di tempo e di spazio sono le principali attività che Internet ha trasformato in una realtà facile ed accessibile a tutti ([11]). In tale ambito occorre distinguere tra Internet come rete di telecomunicazione, di telematica, quindi come « connessione », dai servizi che sono resi possibili da tale

([10]) Una delle similitudini più comuni usata da coloro che si interessano del fenomeno presenta l'utente dei servizi offerti dalla Rete, di quello informativo del *web* in particolare, come un « navigatore » nello sconfinato mare del *cyberspazio*, passando da un luogo all'altro attraverso i collegamenti (*link*) ipertestuali e ipermediali attivati da un semplice *clic* del mouse (« navigatore »).

([11]) Per non generare ambiguità, e conseguenti confusioni, una dottrina ritiene che sia opportuno guardare questa rete di reti come una combinazione di tre spazi, ciascuno con la sua configurazione e architettura o topologia: 1. lo spazio fisico, ovvero l'*infrastruttura*, 2. lo spazio digitale, ovvero la *piattaforma di memoria*, 3. lo spazio semantico, ovvero il *cyberspazio*. La combinazione di questi tre spazi rende possibile l'implementazione di tre funzioni essenziali: la posta elettronica (*e-mail*), il controllo a distanza di altri computer, e la piena creazione/gestione/comunicazione di archivi di documenti. Queste tre funzioni trasformano Internet in uno straordinario strumento di comunicazione e gestione di qualsiasi informazione digitale a livello globale (così Floridi L., *Internet*, Il Saggiatore, Milano, 1997, p. 1).

rete, applicazioni informatiche per svolgere diverse funzioni, comunque riferibili alla trasmissione di informazioni ([12]): e rilevanti ai fini del presente scritto perché comprendenti anche lo scambio di dati riguardanti la persona, nonché le tecniche che consentono di acquisire tali informazioni personali ([13]).

L'integrazione tra i servizi di telecomunicazione (la connessione) e i servizi informatici (siano essi informativi o telematici) ha reso possibile la realizzazione di una forte interazione tra chi offre e chi utilizza i contenuti posti in linea ([14]). L'interattività propria delle nuove realizzazioni, rispetto alla « passività » caratteristica dei *media* tradizionali, ha portato al loro successo ed all'esponenziale diffusione ovunque nel mondo: matrice originaria della rivoluzione nel settore dell'informazione (e non solo) che stiamo vivendo in questi anni ([15]). Ma a fronte di tale evoluzione nel modo di fare e di usufruire dell'informazione, certamente non mancano alcuni inconvenienti correlati alle possibilità offerte dalle nuove tecnologie.

([12]) Tra i principali servizi di Internet si ricordano la posta elettronica, i gruppi di discussione, il *World Wide Web* (o semplicemente *Web*, la « ragnatela ipermediale » rivoluzionario mezzo di informazione e di conoscenza), le conversazioni in tempo reale (le c.d. « *chat* »), il trasferimento di *file*, la possibilità del collegamento remoto a computer lontani: per un'esposizione sulle caratteristiche di Internet e dei suoi servizi si vedano le pubblicazioni richiamate nella nota 4.

([13]) Questi servizi, informativi o telematici (distinzione attuata sulla base del fatto che lo strumento informatico sia un semplice mezzo per la distribuzione di informazioni, oppure l'oggetto del servizio: esempio del primo caso è il *web*, mentre del secondo i motori di ricerca), possono essere distinti a seconda che la comunicazione attraverso essi avvenga in maniera ristretta o ampia: nella prima ipotesi è possibile effettuare una scelta relativamente al destinatario del messaggio; nella seconda, invece, la comunicazione è destinata ad un pubblico indifferenziato e non selezionabile. Esempio di servizio che configura una comunicazione « ristretta » è chiaramente la posta elettronica, mentre si ha una comunicazione « ampia » nel caso del *world wide web*.

([14]) « La diffusa disponibilità di collegamenti elettronici bidirezionali avrà un impatto rivoluzionario su ogni aspetto della nostra vita. La Rete sottrarrà potere ai governi centrali, ai *mass media* ed alle grandi industrie. (...). È quasi impossibile che i governi centrali riescano a regolamentarla, ma ha un grande bisogno di essere controllata dall'interno (...) »: così Dyson E., *Release 2.0. Come vivere nell'era digitale*, Mondadori, Milano, 1997, p. 8.

([15]) È proprio questa caratteristica, la possibilità di instaurare un collegamento diretto tra chi fornisce il servizio e chi lo utilizza, a rendere necessaria una profonda riflessione in coloro che gestiscono i *media* informativi, sulle modalità necessarie per affrontare il cambiamento: cambiamento che porterà probabilmente ad una integrazione tra i differenti strumenti di comunicazione. Sul punto si veda Zambardino V. e Berretti A., *Avviso ai naviganti*, Donzelli, 1996, p. 112.

Infatti il collegamento bi-direzionale tra chi offre e chi usufruisce delle informazioni permette non solo il passaggio tipico dei dati *al* « lettore », ma anche l'applicazione di tecniche informatiche che consentono al fornitore di acquisire informazioni sul contatto telematico che consulta il proprio servizio, e quindi il passaggio di dati *dall'*utente: aspetto che ha suscitato un certo allarme fra gli utilizzatori della Rete, e relativamente al quale maggiori sono state le impressioni da parte degli organi di informazione, o comunque gli equivoci da parte della dottrina sull'argomento (16). È il caso dei c.d. *log*, cioè delle registrazioni automatiche delle principali informazioni relative ai collegamenti, generati automaticamente dal sistema, che se molto dettagliati possono consentire di ricostruire un preciso profilo del « navigatore » di Internet, utile magari per le promozioni commerciali (17); è ancora il caso dei c.d. *cookie*, specifici *software* che è lo stesso fornitore dell'informazione ad inviare insieme a queste, in maniera invisibile all'utente, e che lavorando sulle memorie del suo computer sono in grado di acquisire informazioni di diverso genere (dall'ultima visita al sito del fornitore, alle pagine più viste nel *web*, o anche ai programmi registrati nell'*hard disk* dell'utente). Allo stesso modo, proprio dalla componente tecnica, questa volta con riferimento alle applicazioni comunicative ristrette, quelle della posta elettronica in

(16) Si veda a tale proposito TORRANO O., PARISE S., *Internet e diritto*, Sole 24 Ore Ed., 1997, pp. 33 e ss., e TOSI E., *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in *Dir. Inf.*, Giuffrè, 1999, 3, pp. 594 e 603.

(17) Permettendo infatti di indirizzare un determinato messaggio pubblicitario ad un destinatario selezionato, sia attraverso i nuovi *media* (ad esempio la posta elettronica, fenomeno del c.d. « *spamming* »), sia con modalità più tradizionali. A tale proposito deve segnalarsi (anche se la sua applicabilità ad Internet non è pacifica) la disciplina stabilita nel d.lgs. 13 maggio 1998, n. 171, recante « 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, e in tema di attività giornalistica », il cui articolo 10, intitolato « *Chiamate indesiderate* », dispone al primo comma 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 »; mentre al secondo comma, con riferimento a sistemi di telecomunicazioni più generalizzati, viene previsto che « Le chiamate per le finalità di cui al comma 1°, effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 11 e 12 della legge ». Sul punto si veda ATELLI M., *Privacy e telecomunicazioni*, Jovene Ed., 1999, pp. 1-335.

particolare, può giungere la possibilità di lesione della *privacy*: così nel caso di intercettazioni di terzi, come nell'ipotesi di intercettazioni delle comunicazioni dei propri dipendenti da parte del datore di lavoro, o delle autorità di pubblica sicurezza nello svolgimento di indagini giudiziarie.

Ma occorre ora verificare la reale capacità lesiva di tali strumenti, ad incominciare dalla possibilità concreta di intercettazione delle comunicazioni in transito sulla Rete, e poi dall'effettiva configurabilità da parte di terzi del profilo dei gusti personali dell'utente di Internet attraverso un monitoraggio del suo utilizzo del nuovo *media*.

2.1. – LE POSSIBILITÀ DI VIOLAZIONE DELLA POSTA ELETTRONICA.

Per quanto riguarda innanzitutto la riservatezza della posta elettronica, si deve immediatamente specificare che i maggiori pericoli per l'utente non derivano dalla fase dinamica, quella della trasmissione del messaggio, ma dai momenti statici, quelli cioè in cui il messaggio è residente nell'elaboratore elettronico di colui che trasmette, di colui che riceve, o dei *provider* che gestiscono le caselle postali elettroniche degli utenti (18). Infatti, nella fase dinamica, le possibilità di intercettazione da parte di terzi del messaggio sono minime a causa delle stesse peculiarità tecniche di Internet, e della sua enorme diffusione: dal primo punto di vista, le caratteristiche tecniche, è proprio il protocollo di trasmissione che è alla base della Rete, il *TCP/IP* (*Transmission Control Protocol/Internet Protocol*), a rendere estremamente difficile l'intercettazione (19); dal secondo punto di vista, la diffusione del nuovo *media*, calcolando che ogni secondo vengono trasmessi su Internet più di 4.000

(18) Il servizio di *e-mail* si svolge infatti attraverso la necessaria intermediazione del gestore del servizio, in genere il provider (oggi anche coloro che permettono di avere caselle postali aggiuntive a prescindere dall'abbonamento alla connessione, come ad es., Hot Mail, all'indirizzo *http://hotmail.com*), che dedica uno spazio di memoria del proprio elaboratore ad ogni suo utente. Il messaggio che si invia ad un determinato destinatario non viene quindi recapitato direttamente nel suo computer, ma prima giunge in quello del gestore: solo successivamente, quando il destinatario si collegherà al proprio fornitore del servizio, e controllerà la sua posta elettronica, riceverà il messaggio (in genere a questo punto cancellandolo da quello del gestore).

(19) Tramite il *TCP/IP* infatti il messaggio viene scomposto in pacchetti, inviati indipendentemente l'uno dall'altro su percorsi probabilmente diversi: così, anche riuscendo ad intercettare un pacchetto, non si riuscirebbe a ricostruire l'intero messaggio.

messaggi [20], porta le possibilità di individuare l'*e-mail* che si desidera acquisire quasi a zero [21]. Invece, come si è detto, sono più concreti i pericoli di violazione della riservatezza dei messaggi elettronici nella fase statica: sia attraverso eventuali accessi abusivi di terzi negli elaboratori dei vari soggetti coinvolti nell'attività di messaggistica [22], sia ad opera dello stesso gestore del servizio, che eccede i suoi compiti e le sue funzioni andando ad aprire le caselle postali elettroniche dei propri utenti al di fuori di specifici motivi di servizio [23].

2.2. – La possibilità di ricostruire il profilo dell'utente: il problema dei « data log ».

Con riferimento poi alla possibilità di ricostruire il profilo dell'utente di Internet, occorre distinguere le ipotesi in cui questo è consapevole delle informazioni personali che volontariamente immette sulla Rete, da quelle in cui tale immissione avvenga abusivamente e in maniera non trasparente: aspetto quest'ultimo che maggiormente ha attirato gli interessi scandalistici degli organi di informazione. Nel primo caso è lo stesso navigatore, per ac-

[20] Così in Resnick R. e Taylor D., *The Internet business guide: riding the information superhighway to profit*, Sams Publishing, 1994, p. 25.

[21] Affermazione da precisare collegandola allo stato attuale della tecnica e con riferimento a normali investimenti volti all'intercettazione.

[22] E tra i terzi che accedono abusivamente alla posta elettronica devono essere considerati anche i responsabili dei sistemi nelle reti c.d. aziendali, cioè coloro che, per motivi tecnici o « amministrativi » (gli addetti alla manutenzione del sistema informatico e telematico dell'azienda, ma anche i dirigenti della stessa per controllare i propri dipendenti), dispongono della possibilità di aprire, leggere ed eventualmente modificare le *e-mail* degli impiegati.

[23] Infatti il *provider* spesso è obbligato, sia per la manutenzione ordinaria del sistema, sia per eventuali interventi straordinari, ad accedere allo spazio di memoria del proprio computer dedicato ad un determinato utente, la sua « casella postale ». Motivo per cui è oramai pacifica in genere la sua esenzione dai divieti posti a tutela della segretezza della corrispondenza elettronica, quando le eventuali ingerenze sono motivate da specifici e dimostrabili motivi tecnici (si veda ad esempio, con riferimento agli U.S.A., quanto riportato in Lance R., *NetLaw*, McGraw-Hill, 1995, pp. 119 ss.). Non così nel nostro Paese, dove è stata approvata, nell'ambito della disciplina della firma digitale, una norma che impedisce espressamente al gestore del servizio di procedere in tal senso (è l'art. 13 del D.P.R. 10 novembre 1997 n. 513, su cui si veda Ciacci G., *Firma digitale*, Sole 24 Ore Ed., 1999, pp. 126 ss.), su cui si veda oltre nel testo.

cedere ad un determinato servizio (si pensi agli abbonamenti gratuiti a specifici siti *web*, o alle richieste di rimanere informati sugli aggiornamenti di determinati argomenti nei gruppi di discussione), oppure per acquistare un bene, o ancora al fine di scrivere nei c.d. *guestbook* un proprio commento o semplicemente un saluto, a fornire i propri dati personali, in genere attraverso la compilazione di un modulo o di un questionario: e quindi l'acquisizione delle informazioni avviene da parte del fornitore attraverso il consenso del soggetto titolare delle stesse.

La seconda ipotesi si verifica invece a livello tecnico, attraverso particolari programmi utilizzati nella gestione ordinaria dei servizi offerti in Rete: si rientra quindi nei già citati casi dei c.d. *log* e dei *cookie*, ma anche in quello dei motori di ricerca, specificamente di quelli che lavorano nell'ambito dei gruppi di discussione. Rispetto ai primi due esempi, occorre però precisare la loro concreta valenza lesiva, probabilmente troppo esagerata alla luce dell'effettivo funzionamento tecnico degli indicati programmi [24]. Infatti, per quanto riguarda il problema dei « *data-log* » [25], deve essere distinta la posizione del fornitore dell'accesso, l'unico che possa effettivamente associare l'identità dell'abbonato connesso in un preciso momento (anche se in realtà è l'identità del titolare dell'abbonamento, e non di chi effettivamente utilizzi l'elaboratore elettronico) all'*I.P.* concessogli per navigare, da quella del gestore dello specifico sito *web*, per il quale è impossibile sapere a chi corrisponda il determinato contatto telematico che naviga nella propria risorsa informativa.

Quindi il titolare di uno specifico servizio commerciale può sapere quali

[24] « ... Per conoscere esattamente cosa fa un operatore sulla Rete, bisogna disporre contemporaneamente dei *log-file* del *Service Provider* e dei *log-file* del *Content Provider*, per individuare quali contenuti siano visitati. Ma se non viene realizzata questa corrispondenza non sarà possibile tracciare l'attività in Rete dell'operatore » (così Barbuti M., intervento alla Conferenza *Internet e* privacy*: quali regole?*, tenuta a Roma l'8 maggio 1998, in *Supplemento n. 1 al Bollettino n. 5*, p. 132).

[25] I *data-log* sono le registrazioni generate antomaticamente dal sistema del fornitore dell'accesso ad Internet relative alle principali informazioni sui collegamenti alla Rete effettuate dai propri clienti: ogni volta cioè che l'utente si connette, il *provider* memorizza data e ora, durata del collegamento, numero di *I.P.* assegnato per quella determinata connessione, ed altre informazioni tecniche utili per diversi scopi (non ultimo il costituire prova del corretto adempimento delle obbligazioni relative al servizio offerto da parte del fornitore dell'accesso). A proposito dei *data-log* si veda Tosi E., *op. cit.*, pp. 594 ss., Torrani O. e Parise S., *Internet e diritto, cit.*, pp. 35-36.

pagine del proprio sito sono state visitate, e quante volte (ed in questo modo determinare ad esempio l'interesse per un prodotto piuttosto che per un altro), al limite da quale *provider* o da quale Paese giunge l'accesso, ma non certamente chi sia l'individuo a cui corrisponde il singolo contatto: gli è quindi preclusa la possibilità di ricostruire il fantomatico « profilo » dei gusti e delle preferenze dei propri utenti. Invece il fornitore dell'accesso ad Internet, memorizzando nel registro dei *log* l'associazione nome dell'utente – numero *I.P.* concessogli, può ricostruire questa identità, ma non l'attività svolta in Rete dal suo abbonato (26). È chiaro che associando le informazioni a disposizione di entrambi i soggetti diventa possibile il monitoraggio dell'attività svolta dal soggetto nell'ambito della sua connessione ad Internet: e proprio il configurarsi di questa ipotesi ha provocato di recente l'intervento dell'Autorità Garante nel nostro Paese per dettare le regole da rispettare per evitare abusi nei confronti degli utenti (27).

2.3. – Le possibilità lesive dei c.d. « cookie » e dei motori di ricerca.

Per quanto riguarda poi i programmi dedicati a far interagire il sistema del gestore del servizio con l'elaboratore elettronico dell'utente (ad esempio al fine di visualizzare le informazioni relative alla data del luogo di colui che accede al sito, oppure permettere una più veloce visualizzazione delle pagine, o una loro personalizzazione, ...), i c.d. *cookie*, anche in questo caso, ipotizzando che tali *software* giungano fino al punto di comunicare al fornitore il contenuto dell'*hard disk*, o altre informazioni relative al « navigatore », tali informazioni porterebbero però ad acquisire dati in realtà anonimi, cioè non collegabili alla persona (28).

(26) In realtà il *provider* può anche giungere a conoscere in quali siti ha navigato il proprio utente, ma non in maniera semplice (si immagini le risorse impegnate soprattutto nel caso di fornitori di grandi dimensioni con numerosissimi abbonati), e non sulle singole pagine consultate, ma solo a livello più generale dei domini visitati.

(27) Si fa riferimento alla pronuncia del Garante rispetto al ricorso presentato dall'Associazione Alcei contro Infostrada avente ad oggetto il contratto per usufruire del servizio « Libero », abbonamento gratuito alla Rete: nella prima versione di tale contratto veniva stabilita proprio la possibilità per il *provider* di acquisire informazioni sui siti visitati dai propri clienti. Sul punto si veda oltre nel testo.

(28) Il *cookie* è un piccolo *file* inviato da parte di un *server web* al programma del computer dell'utente dedicato alla navigazione su Internet (il c.d. *browser*), al fine di memorizzarci sopra specifiche informazioni (ad esempio la durata e le modalità dell'ultima visita a quel sito *web*, o qualsiasi altra notizia gli sia stata fornita volontariamente dallo stesso utente) per poterle poi recuperare successivamente. Il *browser* conserva questa richiesta in un *file* (chiamato appunto « *cookie.txt* »), fino a quando non si cambia sito o si interrompe il collegamento: a questo punto il *file* viene salvato sul disco rigido dell'utente e verrà inviato ad ogni successiva richiesta allo stesso *server* che identificherà così il visitatore. In effetti i *cookies* tengono traccia non dei singoli utenti, ma più precisamente dell'accesso a singoli documenti da parte di singoli *browser*. Per quanto riguarda la sicurezza, sono stati stabiliti dei limiti precisi: ogni *cookie* non può essere più grande di 4 Kb, ogni *browser* non può conservare più di 300 *cookie* contemporaneamente, inoltre ogni singolo *server web* non ne può avere più di 20 per i suoi scopi. Questo significa che la cosa più dannosa che possa essere fatta attraverso questi *software* è occupare dello spazio sull'*hard disk* dell'utente, ma comunque non più di 1.2 Mb (se tutti i 300 *cookie* fossero stati creati e fossero di 4 Kb), mentre di solito non si superano i 50 Kb totali (dato che in media sono lunghi circa 100 byte).

Una maggiore valenza lesiva della *privacy* dell'individuo sembrerebbero invece avere quei programmi che svolgono la funzione di consentire la ricerca di informazioni sui più differenti argomenti nell'enorme banca dati costituita dai milioni di siti *web* pubblicati nei diversi Paesi del mondo, i c.d. motori di ricerca: questi, in pochi secondi, permettono di trovare una o più parole presenti all'interno dei siti collegati alla Rete, con metodi di ricerca più o meno evoluti, ma in genere di sicura efficacia. Tra tali specifici *software* deve registrarsi l'esistenza di motori che svolgono le loro ricerche nel settore dei gruppi di discussione, o *Newsgroup*, cioè di quelle risorse che raccolgono i messaggi scritti da persone che partecipano agli scambi di opinioni in Rete aventi ad oggetto numerosissimi temi, talvolta anche delicati (con riferimento cioè ad argomenti riguardanti la politica, la religione, oppure la salute o i gusti sessuali): alcuni di questi motori consentono, in periodi di tempo anche estesi, di selezionare tutti i messaggi inviati al *gruppo* su uno specifico tema, oppure da un determinato utente, permettendo in tale modo di ricostruire effettivamente il profilo, gli interessi, la personalità dello stesso (29).

Da questi brevi esempi è possibile trarre comunque conferma, una volta condotti ad una corretta dimensione gli aspetti tecnici della Rete che in qualche modo vanno ad influire con il trattamento dei dati personali, dell'ulteriore capacità lesiva della riservatezza dell'individuo che hanno acquisito le nuove

(29) Il principale motore di ricerca che permette questo tipo di applicazione è *Deja News*, consultabile all'indirizzo *web http://www.dejanews.com*, ed in particolare le sue funzioni di ricerca evolute.

tecnologie in seguito all'avvento in Internet, le cui implicazioni e conseguenze a livello giuridico verranno esaminate nei prossimi paragrafi. Tenendo presente che la *privacy* viene influenzata da Internet sotto due diversi punti di vista: da un lato, per quanto riguarda le intercettazioni e la sorveglianza elettronica (sia da parte di soggetti pubblici, sia da parte di privati); dall'altro, con riferimento all'attività di trattamento dei dati riguardanti la persona, argomento del prossimo paragrafo.

3. – Internet e la disciplina dell'elaborazione informatica di dati personali.

Pur ridimensionando l'eccessivo allarme suscitato in genere dalla disinformazione tecnica sul nuovo *media*, è stato in ogni caso accertato che le enormi potenzialità di Internet accrescono comunque il pericolo di ledere la vita privata degli individui coinvolti in diverso modo nell'attività che si svolge nel *cyberspazio*, per motivi ludici o professionali, occasionalmente o sistematicamente (30).

La creazione di archivi contenenti dati strettamente personali è infatti molto semplice attraverso la Rete: le informazioni relative ai propri « visitatori », da essi stessi comunicate volontariamente (come si è detto attraverso la compilazione di questionari elettronici), oppure acquisite mediante l'opera invisibile dei *cookie*; le coordinate degli indirizzi *I.P.*, ottenute magari in seguito all'iscrizione spontanea nei *guestbook*; o anche solo i dati dei collegamenti conosciuti dal *provider* grazie alla memorizzazione del *log* (31), sono informazioni che vengono registrate, archiviate, analizzate ed elaborate per diversi fini, alcuni dei quali potenzialmente lesivi per l'individuo.

A tali attività si debbono quindi applicare le regole proprie delle leggi (o quelle elaborate dalla giurisprudenza, nei sistemi di *common law*) in materia

(30) « Questi problemi relativi alla *privacy* non sono cominciati con Internet, e non possono essere risolti controllando quello che accade in tutti, o quasi, i siti. Le difficoltà insorgono quando le informazioni si spostano tra siti, o al di fuori di essi in luoghi dove persone o aziende formano archivi con dati presi da siti, *mailing list*, elenchi telefonici, notiziari, ... »: così Dyson E., *Release 2.0. Come vivere nell'era digitale*, Mondadori, Milano, 1997, p. 205.

(31) Come già indicato in precedenza nel testo, il c.d. *log* è la registrazione automatica delle principali informazioni relative ai collegamenti effettuati dall'utente che, se molto dettagliati, consentono di ricostruire un preciso profilo del « navigatore » di Internet.

di trattamento di dati personali, oramai presenti in tutti i Paesi maggiormente industrializzati. E relativamente alle quali si è svolto un acceso dibattito tra gli operatori del settore, la cui intensità è stata direttamente proporzionale all'aumento del numero degli utenti di Internet nel mondo, allo sviluppo del commercio elettronico, alle applicazioni delle discipline in materia di tutela della *privacy* alle attività svolte in Rete. Le posizioni contrapposte nell'ambito di tale dibattito sono state essenzialmente due, riconducibili a precise scelte di politica commerciale dei singoli Paesi (32): da una parte, quella che reputa più opportuno lasciare all'autoregolamentazione da parte degli stessi protagonisti dei sistemi comunicativi la protezione della privacy, posizione assunta essenzialmente dagli U.S.A.; dall'altra quella che prevede invece la costituzione di un sistema che attraverso regolamentazioni legislative e convenzioni internazionali arrivi a garantire la protezione dei dati personali in ogni attività *on-line*, scelta attuata in genere nei Paesi dell'Unione Europa. Alla luce di tali posizioni contrapposte l'Italia ha ritenuto di sostenere l'opportunità di seguire una terza via che, pur considerando preminente la necessità dell'intervento normativo nel delicato settore, tuttavia non trascuri anche il valore dei codici di autodisciplina, sia pure quale momento integrativo (33) del primo.

Non avendo ancora portato l'interessante dibattito appena esaminato una soluzione definitiva al tema oggetto del presente studio, occorre allo stato in ogni caso verificare se e come la disciplina dettata in materia di trattamento dei dati personali, e quindi nel nostro Paese la legge n. 675/96, possa applicarsi ai trattamenti che avvengono a distanza, o comunque attraverso la rete Internet o in situazioni strettamente connesse a Internet.

3.1. – Applicabilità della legge n. 675/96 all'attività di trattamento di dati personali connessa ad Internet.

Alla luce dell'indicata verifica, si può affermare che in ogni caso la legge n. 675/96 non sembra subire particolari forzature nella sua applicazione alle attività indicate di trattamento nel loro momento c.d. « statico », relativo

(32) Si veda a tale proposito Santaniello G., *La privacy telematica: problemi e prospettive*, in *Iter Legis*, R.I.S.L. Ed., 1998, pp. 9-12.

(33) Così Buttarelli G., *Una terza via per la tutela*, in *Il Sole 24 Ore*, 9 maggio 1998.

cioè all'attività di trattamento in sé (34): il *provider* quindi che svolge attività nel nostro Paese, nel momento in cui compia un trattamento di dati personali nell'ambito di applicazione della legge n. 675, dovrà dunque rispettare la disciplina (35). Né d'altro canto si rilevano grosse differenze nell'ipotesi in cui l'attività di fornitura del servizio o delle informazioni sia prestata da una Pubblica Amministrazione (si pensi alla pubblicazione sulla Rete della graduatoria di un concorso, oppure dell'elenco dei dipendenti di un determinato ufficio): anche in tale ipotesi, infatti, si applicheranno le regole stabilite nella legge n. 675, e nelle sue modificazioni successive, tra cui quelle del d.lgs. 11 maggio 1999 n. 135. Soluzione coerente con la concezione di Internet quale semplice strumento di comunicazione ed informazione, come prospettata nel paragrafo 1 del presente scritto (36).

Così, in materia di raccolta delle informazioni, avvenga essa in forma esplicita o implicita (37), se coinvolge dati personali (38), sarà necessario ri-

(34) Contrapposta a quella dinamica, cioè quella in cui l'attività di trattamento avviene attraverso il passaggio dei dati personali tra i diversi punti della Rete, rispetto alla quale, a causa delle caratteristiche proprie di Internet, sorgono delle effettive difficoltà, come si vedrà nel prossimo paragrafo.

(35) « La legge sulla *privacy* regola la diffusione dei dati personali in maniera uniforme, a prescindere dal mezzo utilizzato. Essa infatti prevede un'analoga disciplina sia per la diffusione di un elenco di dati personali attraverso una pubblicazione, sia per la messa a disposizione dell'elenco su Internet mediante una pagina *web* consultabile da chiunque si colleghi in rete.

Le norme sulla tutela dei dati personali si applicano, infatti, a tutte le operazioni di trattamento effettuate con o senza ausilio di mezzi elettronici » (da GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Comunicato n. 6, La diffusione di un elenco di dati su Internet deve rispettare la legge sulla* privacy, 14 giugno 1999, in *Cittadini e società dell'informazione*, giugno-settembre 1999, p. 84).

(36) Anche le difficoltà relative all'individuazione, tra i soggetti coinvolti nei trattamenti di dati personali che avvengono su o tramite Internet, di coloro a cui rivolgono le disposizioni della legge n. 675, in realtà sono non difficilmente superabili procedendo ad un esame attento della realtà tecnica con cui si opera sulla Rete.

(37) Sul punto si vedano le considerazioni ed esempi fatti nelle altre parti del testo.

(38) Nell'art. 1, comma 2°, lett. c) della legge n. 675, si definisce il dato personale come « 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 », e l'attività di trattamento come « qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati »: concetti quindi notevolmente ampi che estendono di molto le ipotesi in cui la trasmissione delle informazioni rientri nell'ambito di applicazione della legge.

chiedere il consenso del soggetto cui le informazioni si riferiscono, consenso che dovrà essere « espresso liberamente in forma specifica (termine da controllare) e documentato per iscritto » (si veda a tale proposito l'art. 11 della legge n. 675), successivamente comunque all'informativa prestata all'interessato circa i propri diritti, i fini e le modalità del trattamento, l'indicazione del responsabile dello stesso (elementi previsti dall'art. 10): norme che devono essere rispettate anche nel caso di predisposizioni di un formulario elettronico da parte del gestore di un determinato servizio offerto sulla Rete, ma anche per la conservazione dei dati personali che ne risultano, rispettando precise modalità di sicurezza, e per la loro eventuale comunicazione e diffusione.

Così, ancora, con riferimento al trattamento dei dati maggiormente lesivi della riservatezza e dell'identità personale dell'individuo, quelli c.d. sensibili (39), sarà necessario, oltre al consenso, anche l'autorizzazione del Garante. Ma se il trattamento collegato all'attività su Internet avviene « nell'esercizio della protezione di giornalista e per l'esclusivo perseguimento delle relative finalità » (40), rispettando in genere « i limiti del diritto di cronaca, ed in particolare quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico », oppure nel caso in cui si tratti di « dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico » (art. 25 legge n. 675/96) (41), non ci sarà bisogno né di consenso, né di autorizzazione: a meno che non si verifichi l'ipotesi di dati idonei a rilevare lo stato di salute e la vita sessuale, per i quali torna la necessità del consenso dell'individuo.

(39) I dati sensibili sono quelle informazioni che hanno una particolare capacità di incidere sulla riservatezza dei singoli individui e di determinare discriminazioni sociali particolarmente rilevanti. Sulla loro disciplina si veda altro intervento del presente volume.

(40) Si pensi a quei siti *web* nei quali viene fornito un servizio informativo di tipo giornalistico.

(41) Testo risultante dalle modifiche introdotte dal d.lgs. 13 maggio 1998, n. 171, recante « 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, e in tema di attività giornalistica ». La nuova formulazione, relativamente al comma in esame, ricalca essenzialmente quella precedente, tranne per la ricordata ipotesi dei « dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico ».

Così, infine, rispetto ai nuovi obblighi introdotti, ad integrazione della disciplina in materia di trattamento dei dati relativi alla persona, dal d.lgs. 13 maggio 1998, n. 171: ed in particolare rispetto alla sicurezza ed alla riservatezza del servizio di telecomunicazione (art. 2, comma 1°), al trattamento dei dati personali relativi al traffico ed alla fatturazione del servizio (art. 4) o all'elenco degli abbonati (art. 9) (42). Ma anche con riferimento all'ipotesi in cui su Internet vengano trattati dati sensibili della persona da parte di un soggetto pubblico, ipotesi che vedrà applicare, come si è detto, la disciplina del d.lgs. n. 135/99: ad esempio il suo art. 3 (« Dati trattati »), che impone l'obbligo di « trattare i soli dati essenziali per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di natura diversa », o ancora rispetto alle misure minime di sicurezza disciplinate dal D.P.R. 28 luglio 1999, n. 318.

3.2. – La posizione del Garante in materia di offerta di accesso gratuito ad Internet.

Ultimamente in Italia si è avuta una netta crescita degli abbonati ad Internet, in parte perché è maturata l'esigenza di partecipare al nuovo rivoluzionario fenomeno del mondo della comunicazione, ma soprattutto perché diverse società che operano nel settore hanno iniziato ad offrire con grande successo sul mercato la possibilità di collegamento gratuito (cioè senza abbonamento annuale al fornitore dell'accesso) ad Internet. Il rientro economico per tali società, a copertura delle spese per gestire un servizio che comunque deve essere efficiente a prescindere dalla sua gratuità, è rappresentato dallo sfruttamento della pubblicità: o direttamente per gli ulteriori servizi offerti in proprio dalle stesse, o indirettamente attraverso la vendita dell'opportunità di far conoscere le offerte di altri fornitori mediante Internet. In entrambi i casi il vero valore aggiunto della pubblicità sulla Rete è dato dalla possibilità di indirizzare con maggiore precisione il messaggio pubblicitario al presunto interessato allo stesso. Le modalità per acquisire tale precisione sono diverse, talvolta non esattamente trasparenti: come nel caso di un noto *provider* che recentemente offriva sì l'accesso gratuito ad Internet, ma facendo sottoscrivere ai suoi utenti un contratto in cui veniva espressa-

(42) Su tale decreto si veda il recente scritto di Atelli M., *Privacy e telecomunicazioni*, *cit.*

mente prevista (e conseguentemente obbligatoriamente accettata) la sua facoltà di acquisire tutte le informazioni relative all'uso della Rete da parte dell'utente (43).

In seguito ad un ricorso proposto da un'associazione di categoria, il Garante ha intimato al fornitore dell'accesso di eliminare le clausole illegittime (44), e nello stesso tempo ha dettato alcuni princìpi che devono essere seguiti da tutti i gestori dei servizi su Internet.

Così, il fornitore del bene o servizio che tratti dati personali dei propri clienti dovrà chiarire i termini del contratto prima di chiedere le generalità di colui che ha effettuato la domanda di abbonamento; riepilogare in maniera chiara e sintetica, in un unico paragrafo, il modo con cui verranno trattate le informazioni fornite dal navigatore; ricordare i diritti del cittadino stabiliti dalla legge n. 675/96, ed in particolare: collocare il messaggio che informa l'utente prima della richiesta di registrazione dei propri dati, riferire tutti gli aspetti del trattamento svolto dal fornitore, riepilogando in maniera chiara e sintetica le notizie che sono magari sparse nel contratto, integrarlo con un richiamo ai diritti di accesso attribuiti agli interessati dalla legge n. 675.

Principi comunque ricavabili dalla disciplina in materia, anche a prescindere dal comunicato del Garante, a dimostrazione che considerando

(43) In particolare veniva riservata al fornitore la possibilità di monitorare la navigazione dell'utente, consentendogli quindi di conoscere le varie pagine *web* consultate dai suoi clienti. La gravità della questione non veniva certo limitata dall'impegno dello stesso a non divulgare le informazioni relative ai dati sensibili dei vari navigatori (tra l'altro anche perché per considerare tali le informazioni relative all'uso della Rete occorreva in ogni caso venirne a conoscenza). Sulla vicenda si veda l'articolo di Morgoglione C., *Free Internet, Rodotà detta le regole*, pubblicato nel quotidiano *on-line « La Repubblica.it »*, 20 gennaio 2000, all'indirizzo *http://www.repubblica.it/online/tecnologie-internet/free/free/free.html* consultato il 9 febbraio 2000.

(44) Alla luce delle numerose critiche riservate all'iniziativa da parte degli organi di informazione e delle associazioni di categoria, ma anche degli stessi utenti, il *provider* in questione ha preferito eliminare le indicate clausole, ma ha provato anche a proporre un'altra soluzione: l'analisi dei comportamenti *on-line* svolta non in assoluto su tutti i siti visitati, ma sulla base di un catalogo pre-definito (verrebbe cioè controllato se l'abbonato guarda, o meno, i siti presenti in un elenco stabiliro « a priori » dal fornitore, e rappresentativi di varie categorie di prodotti o servizi). Alla data di redazione del presente scritto il Garante deve ancora rispondere all'indicata proposta, che comunque non sembra variare di molto i termini del problema.

l'attività di trattamento in sé, anche se collegata ad Internet, in una fase che si è definita « statica », non sorgono particolari problemi per tutelare i dati personali dell'individuo.

3.3. – Applicabilità della legge n. 675/96 alla trasmissione di dati personali attraverso Internet.

Invece problemi nell'applicazione della disciplina sulla tutela dei dati relativi alla persona sorgono nel momento « dinamico » delle attività di trattamento di informazioni personali correlate alla Rete: quello cioè del passaggio di dati tra diversi « siti » di Internet (termine inteso questa volta in maniera generica, nel senso di « punto della Rete »), e quindi quello del passaggio di informazioni tra i diversi computer collegati telematicamente. Siano dunque essi elaboratori che stanno scambiando posta elettronica, oppure consultando informazioni rese disponibili sul *web*, o addirittura, e questa volta in maniera « invisibile » all'utente, svolgendo le istruzioni *software* impartite da un determinato *cookie*: attività che in ogni caso portano al passaggio di dati da un luogo ad un altro. Ipotesi in particolare collegata, nell'ambito delle leggi sui trattamenti dei dati personali, alle scelte normative relativamente alla comunicazione e diffusione transnazionale di dati (45), quando il passaggio avviene tra elaboratori dislocati in Paesi diversi.

Ed infatti, proprio a tale proposito, la legge italiana in materia non risulta essere molto chiara: anzi, forse più che di mancata chiarezza, si deve parlare di mancata coerenza con un sistema di distribuzione delle informazioni diventato di uso comune, Internet appunto, certamente non tenuto in considerazione quando si è redatto il testo delle disposizioni sull'argomento. Né in tal senso sembrano aiutare, se non apportando addirittura altri elementi di dubbio, le integrazioni approvate dal Governo in attuazione della legge del 31 dicembre 1996 n. 676, a fronte comunque della mancanza di una specifica produzione in tal senso, nonostante proprio l'esplicita previsione dell'art. 1, comma 1°, lett. n) della stessa, oggi in ogni caso scaduta (46). Ci si riferisce in particolare ai problemi diretta conseguenza (47) del sistema costruito dal combinato disposto da una parte degli artt. 2 e 6, relativi all'ambito di applicazione della stessa disciplina, dall'altra degli artt. 28 e 35, comma 2°, relativo al trasferimento di dati all'estero, della legge n. 675/96.

Così l'art. 2 e l'art. 6 della legge in esame (48), atti ad identificare e specificare l'ambito di applicazione della sua disciplina, stabilendone l'operatività ogni qual volta un trattamento di dati personali sia effettuato nel territorio dello Stato (49), oltre a suscitare seri dubbi di legittimità per contrasto con il diritto comunitario (50), diventano di non facile interpretazione, o

(45) Relativamente alle quali, con riferimento all'attività su Internet della P.A., si devono comunque tenere presenti anche le eccezioni stabilite per i trattamenti dei dati petsonali svolti dai soggetti pubblici.

(46) L'art. 1, comma 1°, lett. n), della legge n. 676 testualmente dispone, nell'ambito dei compiti che il Governo dovrà svolgere in esecuzione della delega, « stabilire le 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 cotrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale ».

(47) Si ricordi a tale proposito che Internet ha reso possibile una modalità comunicativa del tutto nuova, creando una forma di attività economica e sociale peculiare (tanto da condurre i maggiormente entusiasti del nuovo fenomeno ad immaginare scenari originali chiamati « *cyberspazio* », quale luogo, o non luogo, di esplicazione della propria petsonalità), e portando allo sviluppo di diverse applicazioni relative a fenomeni già esistenti: situazione, tra l'altro, in continuo divenire e che solleva, quale conseguenza immediata, la necessità di sottoporre a verifica le categorie tradizionali del pensieto umano, non ultime quelle giuridiche. E questo è l'approccio con cui ci si dovrebbe avvicinare all'esame della disciplina creata dalla legge n. 675/96 nel momento della sua applicazione alla « Rete delle reti ».

(48) Art. 2, *Ambito di applicazione*: « La presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato ».

Art. 6, *Trattamento di dati detenuti all'estero*, comma 1°: « 1. Il trattamento nel territorio dello Stato di dati personali detenuti all'estero è soggetto alle disposizioni della presente legge ».

(49) Indipendentemente dal fatto che si tratti di dati personali di cittadini italiani o di persone giuridiche aventi sede in Italia, ed anche se i dati sono detenuti all'estero (così Cerina P., *Trasferimento di dati all'estero: notifica al Garante, divieto di trasferimento, trasferimenti intragruppo e trasferimenti all'estero attraverso reti ed Internet*, intervento al Convegno Paradigma « *Applicazione della legge sulla privacy nelle imprese e nelle pubbliche amministrazioni* », Milano, 25 novembre 1997, p. 3).

(50) La Direttiva n. 95/46 infatti, recepita nel nostro Paese con la legge n. 675 del 1996, dispone l'applicazione delle leggi di attuazione ai trattamenti effettuati da soggetti stabiliti nel proptio territorio: fattispecie ben divetsa dal semplice svolgimento del trattamento nel territorio, a prescindere dall'effettivo « stabilimento », richiesto dall'art. 2 in esame (così Cerina P., *op. cit.*, p. 3).

comunque di difficile applicabilità nel momento in cui si inizia a svolgere un'attività anche solo in parte su Internet (51). Infatti, il combinato disposto degli indicati articoli, oltre all'ampia accezione data al concetto di « trattamento » nelle definizioni della legge, portano la stessa ad obbligare alle sue previsioni non solo il soggetto che acquisisce informazioni, ma anche il fornitore delle stesse, siano essi italiani o stranieri: unica condizione che il trattamento avvenga nel territorio dello Stato, e quindi la presenza di almeno uno dei due soggetti in tale territorio (52). Questo creando conseguenze estremamente onerose per l'utente della Rete (53), e dunque ponendo seri ostacoli alla diffusione del nuovo strumento di manifestazione del pensiero e di distribuzione della conoscenza, e quindi all'esercizio di diritti fondamentali dell'individuo (54).

(51) Delicati interrogativi circa la concreta possibilità di tutelare la riservatezza in termini suscettibili di reale applicazione, specie per ciò che riguarda l'ardua ripartizione del mondo « virtuale » in territori soggetti a distinte sovranità, sono riportati anche da BUTTARELLI G., *Banche dati e tutela della riservatezza*, Giuffrè, 1997, p. 447.

(52) Si consideri l'ipotesi in cui un determinato soggetto acceda dal nostro Paese ad un sito *web* residente sull'elaboratore (*server*) di un *provider* che si trovi all'estero, scaricando sul proprio computer dati personali di determinati individui: attività che certamente rientra nel « trattamento » previsto dall'art. 1, lett. b), della legge n. 675 (per l'utente, sotto le voci « raccolta », « registrazione », « estrazione », « utilizzo »; per il fornitore, nell'ambito delle voci « comunicazione » e « diffusione », oltre probabilmente a « interconnessione »), e che quindi, insieme a quanto previsto nell'art. 2 (per l'utente italiano) e dall'art. 6 (per il *provider* straniero), porta all'applicazione della disciplina italiana in materia di tutela dei dati personali, ad eccezione chiaramente delle ipotesi in cui tale applicazione è espressamente esclusa (come nel caso di trattamento per fini esclusivamente personali).

(53) Maggiormente opportuno sarebbe stato invece collegare i principi sull'applicabilità della legge n. 675 non ad un criterio « territoriale puro » (quello sancito negli artt. 2 e 6), quanto a criteri relativi alla residenza o allo stabilimento (seguendo in questo modo la Direttiva n. 95/46) del soggetto che effettua il trattamento (così CERINA P., *op. cit.*, p. 4).

(54) Sul concetto di Internet quale strumento di manifestazione del pensiero, e quindi quale mezzo che permette l'effettiva esplicazione di diritti fondamentali dell'individuo, si può fare riferimento a COSTANZO P., *Le nuove forme di comunicazione in Rete*, in AA.VV., *Il diritto nel cyberspazio* a cura di BRUGALETTA F., Simone Ed., 1999, pp. 91-135. In tal senso si vedano anche le conclusioni della motivazione della sentenza della Corte Federale U.S.A., Distretto della Pensylvania, 11 giugno 1996 (in *Dir. Inf.*, 1996, p. 640, con nota di ZENO ZENCOVICH V., e su Internet nei siti *web* citati alla nota 3): « Si può realisticamente definire Internet come una conversazione mondiale che non finisce mai (...), la forma di comunicazione di massa più partecipativa che sia mai stata realizzata ».

Stessa anomalia si riscontra con riferimento alla seconda situazione di inadeguatezza della legge n. 675/96 relativamente alle banche dati su, o attraverso, Internet: quella della disciplina dei flussi transfrontalieri dei dati personali.

Secondo infatti l'art. 28, di tale normativa, intitolato « *Trasferimento di dati all'estero* », il titolare del trattamento deve notificare al Garante per la tutela dei dati personali « qualsiasi trasferimento, anche temporaneo, fuori dal territorio nazionale, con qualsiasi forma e mezzo ». Ricevuta la notifica, il Garante deve verificare che nel Paese verso il quale si intende trasmettere i dati personali sia presente una normativa a tutela degli stessi, che consenta un livello di protezione *adeguato*, nel caso di dati personali in genere, *di grado pari a quello assicurato nell'ordinamento italiano*, nel caso si tratti di dati sensibili. In caso tali condizioni non vengano rispettate, può essere vietato il trasferimento (55): chi lo effettui lo stesso nonostante il divieto, oppure prima di ricevere il parere del Garante, si espone all'applicazione di sanzioni penali anche gravi, previste dall'art. 35, comma 2° (56).

Ora, tenendo presente che « porre in linea » su Internet, nell'ambito magari di un sito *web*, un elenco di dati personali vuol dire sicuramente effettuare un « trattamento » secondo l'art. 2, lett. b), nel caso in cui le finalità che determinano tale attività non siano « esclusivamente personali », risulta essere dunque applicabile la legge n. 675/96; e che il metterlo « in linea » implica il suo trasferimento in Rete, e quindi verso tutti i Paesi collegati ad Internet, si può concludere circa la necessità di osservare anche in questo caso il disposto dell'art. 28. E lo stesso problema si pone per quanto riguarda il meccanismo dei c.d. *cookie*, che rilevano per la disciplina in esame non per la loro valenza lesiva della riservatezza (di cui si è già parlato in altra parte del presente scritto), quanto perché rappresentano un tipico caso di trattamento, rilevante per l'applicazione dell'intera legge n. 675, ed in

(55) Art. 28, comma 3°: « Il trasferimento è vietato qualora l'ordinamento dello Stato di destinazione o di transito dei dati non assicuri un livello di tutela delle persone adeguato ovvero, se si tratta dei dati di cui agli artt. 22 e 24 (n.d.r. dati sensibili e sanitari), di grado pari a quello assicurato dall'ordinamento italiano (...) ».

(56) Secondo l'art. 35, comma 2°, « Salvo che il fatto non costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri danno, comunica o diffonde dati personali in violazione di quanto disposto (...), ovvero del divieto di cui all'art. 28, comma 3°, è punito con la reclusione da tre mesi a due anni ».

particolare, anche in questo caso, di trasferimento di informazioni personali in genere all'estero (57).

Così, chiunque voglia compiere tale attività dovrà effettuare specifica notificazione al Garante, che a sua volta dovrà controllare le caratteristiche delle normative dei diversi Stati che hanno accesso ad Internet (che dovranno quindi, a seconda dei casi, essere adeguate, o uguali, a quella italiana) prima di decidere se continuare o vietare quel determinato « trattamento ». Per poi concludere vietandolo nei confronti di alcuni Paesi, nel caso i requisiti dell'adeguatezza o dell'equivalenza della disciplina dello Stato destinatario non vengano soddisfatti (58), oppure consentendolo in caso contrario.

La difficoltà, apparentemente insormontabile, sorge nel momento in cui si tiene presente che i Paesi collegati sono circa 170, portando quindi il compito dell'ufficio del Garante ad un impegno eccessivo, e forse non realizzabile (59); e soprattutto che, a livello tecnico, è impossibile impedire, o

(57) Se si tengono presenti le informazioni, talvolta personali, che il *cookie* memorizza quando il soggetto riceve il *file* nel proprio elaboratore durante la navigazione in un determinato sito (ad esempio il numero I.D. o la traccia delle pagine visualizzate nel corso dell'ultima visita allo stesso sito), e si considera che tale *cookie* viene poi trasmesso, senza che l'utente se ne accorga, al computer del gestore del servizio, risulta evidente che anche in questo caso si rientrerebbe nella previsione dell'art. 28.

(58) Un autore (CERINA P., *Commento all'art. 2 ed all'art. 28 della legge n. 675/96*, in AA.VV., *La tutela dei dati personali. Commentario alla l. 675/96*, a cura di GIANNANTONIO, LOSANO e ZENCOVICH, Padova, 1997, rispettivamente a p. 27 e p. 259) porta provocatoriamente l'interpretazione della norma ad applicazioni ancora più assurde, oltre a quella citata di un fornitore di informazioni del nostro Paese che pone in linea dati personali: così per l'ipotesi di un soggetto italiano, anche un semplice utente, che consulti un sito *web* estero (attività a cui si dovrebbe applicare la legge n. 675, perché in ogni caso si verifica il trattamento), ma anche quella di un soggetto straniero che gestisca un *server web* nel suo Paese (anche in questo caso si applicherebbe la legge n. 675, perché potrebbe considerarsi rientrare nel concetto di « trattamento » quell'attività che viene svolta con effetti nel nostro Paese).

(59) In tal caso potrebbe soccorrere il testo della legge, che infatti prevede comunque una serie di eccezioni, al comma 3° dell'art. 28 – ed in particolare alle lett. b) e g) –, ipotesi di trasferimento di dati all'estero « comunque consentito ». Alla lett. b) si riporta il caso in cui il trasferimento « sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'acquisizione di informative precontrattuali attivate su richiesta di quest'ultimo, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato ». Alla lett. g) invece si considera l'ipotesi in cui il trasferimento « sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto ». In entrambe le ipotesi non risulta però chiaro se e con quale estensione la disciplina possa essere applicata all'utente di Internet, e non diminuisce quindi la necessità di un intervento nella materia in esame che permetta di superare le riportate discrasie.

comunque gestire, la diffusione verso solo alcuni dei Paesi collegati alla Rete e non altri. Ed è proprio questo secondo punto a creare le maggiori difficoltà agli utenti di Internet. Infatti, nell'eventualità in cui il Garante vieti, *ex* art. 28 della legge n. 675/96, la trasmissione dei dati personali verso uno o più determinati Stati, il soggetto che ha effettuato la richiesta di autorizzazione, nell'impossibilità tecnica (almeno al momento attuale) di adeguarsi a tale decisione, sarà costretto a non osservare il provvedimento, oppure a cessare la sua attività in Rete (60).

Ed anche in questo caso occorre rilevare il serio pericolo di impedire l'esercizio di diritti fondamentali dell'individuo, tra i quali in particolare quello di manifestare liberamente il proprio pensiero.

4. – TUTELA DELLA RISERVATEZZA DI DOCUMENTI, CORRISPONDENZA, E COMUNICAZIONI IN TRANSITO SU INTERNET.

Oltre a quanto già detto relativamente all'applicazione della disciplina della legge n. 675 all'attività di trattamento svolto dal soggetto che utilizza Internet per diversi scopi (fornire o acquisire informazioni o servizi), uno dei problemi maggiormente avvertito con riferimento all'oggetto del presente studio, riservatezza ed Internet, riguarda la tutela della segretezza e sicurezza delle comunicazioni attraverso il nuovo *media*, problema sollevato fin dalle iniziali esperienze dei primi utilizzatori della Rete, in particolare, quindi, negli Stati Uniti.

Infatti la massima facilità ed efficienza nella corrispondenza delle proprie idee, acquisita proprio grazie all'invenzione dello strumento telematico, vede quale obbligata contropartita a livello tecnico la massima facilità di

(60) Con riferimento alla posizione di colui che effettua la notifica al Garante, nell'ambito della problematica in esame, occorre ricordare le ipotesi di consenso preventivo al trasferimento, previste nel comma 4° dell'art. 28, e riportare le considerazioni in materia di una dottrina che ritiene che per evitare problemi i *provider* si muniranno, in sede contrattuale, del consenso espresso dell'interessato al trasferimento dei suoi dati personali anche verso Paesi che non garantiscano i livelli di tutela richiesti dall'art. 28 (così BUTTARELLI G., *Banche dati e tutela della riservatezza, cit.*, p. 582). Ma questa soluzione non permette di superare l'indicata difficoltà per coloro che *provider* non sono.

accesso a tali idee anche da parte di soggetti estranei a quella determinata comunicazione: a partire dai gestori dei sistemi informatici atti a rendere possibile il servizio, considerando anche i diversi responsabili delle reti aziendali o comunque ad accesso controllato, fino ai casuali, o meno, intercettori dei messaggi (61). Da qui l'esigenza di proteggere in qualche modo la sicurezza e la segretezza delle corrispondenze elettroniche: non solo a livello tecnico, ma anche e soprattutto a livello giuridico.

A tale proposito si può distinguere il problema della tutela della riservatezza di documenti, corrispondenze ed informazioni in transito su Internet dalle ingerenze di soggetti pubblici (in questo caso ci si riferisce alle fattispecie correlate alle attività investigative), rispetto alla tutela della riservatezza di tali comunicazioni dalle ingerenze di soggetti privati (ipotesi che può comprendere anche l'attività di controllo della P.A. sui propri dipendenti che utilizzano le nuove forme di comunicazione).

4.1. – Intercettazioni e sorveglianza elettronica da parte di soggetti pubblici.

È possibile che la riservatezza delle informazioni in transito su Internet venga minacciata o violata da parte di soggetti pubblici.

In tutte le legislazioni dei Paesi più avanzati tecnologicamente è prevista una disciplina in materia, in genere mutuata, espressamente o in via interpretativa, da quella emanata con riferimento alle tecnologie di telecomunicazioni tradizionali, come la radio o il telefono.

Così, nel diritto statunitense, è stabilita la necessità per le forze di polizia di ottenere un preventivo mandato di perquisizione, o altra autorizzazione, sia nel caso di intercettazione di comunicazioni elettroniche, sia in quello di accesso alle informazioni archiviate nelle memorie di un computer (62). Eccezione a tale regola è ammessa quando si possa ragionevolmente ritenere che si sia commesso, o si stia commettendo, un reato, o quando l'intercettazione, o il sequestro del materiale, si riveli necessaria ad impedire che un essere umano sia gravemente ferito o ucciso (63).

(61) Sul punto si faccia riferimento a quanto già detto nel paragrafo 1.

(62) In tal senso la disciplina dell'*Electronic Communications Privacy Act (E.C.P.A.)* del 1986, ma anche, con riferimento al caso di editori elettronici, quella del *Privacy Protection Act* del 1980, che disciplina l'ipotesi particolare di perquisizioni e sequestri di materiali funzionali allo svolgimento del lavoro.

Nell'ambito dei diritti continentali, si può rinvenire un primo riferimento alla materia in esame nella Convenzione europea dei diritti dell'uomo, il cui art. 8 sancisce il diritto di ognuno alla riservatezza ed alla segretezza della corrispondenza: e conseguentemente crea il dovere per le autorità pubbliche di rispettare, e di far rispettare, tale diritto fondamentale (64). Diritto che è certamente estendibile anche ai casi di corrispondenza svolta in forma elettronica.

In tal senso la Francia ha emanato una legge il 10 luglio 1991, la n. 91/646, volta proprio a disciplinare l'ipotesi delle corrispondenze diffuse attraverso mezzi di telecomunicazioni; mentre in precedenza era stata l'Inghilterra (nel 1985 con l'*Interception Communication Act*) a prevedere una regolamentazione di tali casi.

In Italia la disciplina delle intercettazioni « di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione » è prevista nell'art. 266 del cod. proc. pen., che le ammette nelle ipotesi di procedimenti relativi a reati di particolare gravità (quelli, ad esempio, per cui è prevista la pena della reclusione superiore nel massimo a 5 anni). Disciplina che è stata poi integrata dalla legge 23 dicembre 1993 n. 547, in tema di criminalità informatica, che ha inserito nello stesso codice un articolo 266 *bis*, dal titolo « Intercettazione di comunicazioni informatiche o telematiche »:

(63) Una recente applicazione di questi principi (la fattispecie riguardava l'arresto di un pedofilo) che ha trovato risalto nella stampa specializzata nel settore, si è avuto da parte del Tribunale di Pokane County, nello Stato di Washington, che in una discutibile pronuncia ha affermato che non costituisce un illecito la registrazione di eventuali messaggi inviati da un soggetto su Internet (*e-mail*, o comunque messaggi di partecipazione a *Newsgroup*); a differenza di quanto avviene per le più comuni conversazioni telefoniche, per le quali addirittura si configurano ipotesi di reato (si veda l'articolo di Morgoglione M., *USA, è legale registrare le conversazioni online*, presso il sito *web* del quotidiano telematico La repubblica, all'indirizzo *http://www.repubblica.it/online/tecnologie-internet/viamail/viamail/viamail.htlm* consultato il 7 febbraio 2000).

(64) È poi la Corte di giustizia dei diritti dell'uomo, il 6 settembre del 1978, nel caso Klass, ad estendere per la prima volta (ma la statuizione sarà più volte affermata nello stesso senso in seguito) tali principi alle ipotesi delle corrispondenze telefoniche. E considerando che il diritto alla riservatezza delle proprie comunicazioni non viene certo meno quando il messaggio è diffuso elettronicamente, la tutela stabilita nella Convenzione si può certamente applicare anche ai casi di comunicazione interpersonale su Internet.

estendendo in questo modo la possibilità di perseguimento dei reati enumerati nel citato art. 266, a cui è stata aggiunta un'ipotesi specifica, quella dei reati « commessi mediante l'impiego di tecnologie informatiche o telematiche » (65). Anche in questo caso l'intercettazione è consentita solo nell'ambito di procedure relative a reati di particolare gravità, o compiute mediante tecnologie di pari livello rispetto a quelle impiegate per effettuare concretamente l'intervento (66).

4.2. – Intercettazioni e sorveglianza elettronica da parte di soggetti privati.

L'ipotesi in cui i soggetti che procedono all'intercettazione ed al controllo delle informazioni in transito sulla Rete siano dei privati è disciplinata in genere in maniera più rigida, spesso anche con la previsione di sanzioni penali in capo a chi viola il segreto o la riservatezza della comunicazione telematica.

Dal diritto americano (abbia esso fonte nella Costituzione o nel diritto giurisprudenziale), a quello canadese, dal diritto francese a quello inglese, sanzioni pecuniarie o detentive vengono comminate in particolare a chi acceda illecitamente alle informazioni memorizzate in un sistema informatico, intercetti o tenti di intercettare intenzionalmente qualsiasi comunicazione elettronica, divulghi o sfrutti volontariamente il contenuto dei messaggi in transito sui sistemi telematici (67).

Eccezione a tale disciplina, pur con le dovute precisazioni (68), viene ten-

(65) Secondo un autore (Buonomo G., *Metodologia e disciplina delle indagini informatiche*, in AA.VV., *Profili penali dell'informatica*, Giuffrè, Milano, 1994, p. 138) l'ipotesi aggiunta configura in realtà la possibilità di estendere la portata della disciplina a tutti i casi in cui il procedimento abbia ad oggetto l'accertamento di reati commessi con le nuove tecnologie, e non solo ai reati enumerati nell'art. 266 cod. pen. Sull'art. 266 *bis* si veda anche Galdieri P., *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, Milano 1997, pp 200 ss.; Sarzana C., *Informatica e diritto penale*, Giuffrè, Milano, 1994, pp. 223 ss.

(66) Sul concetto di « tecnologie informatiche e telematiche » si veda Buonomo G., *op. cit.*, p. 143.

(67) Addirittura secondo l'art. 368 del codice penale francese l'attività di annotare, registrare, o anche semplicemente ascoltare discorsi di una persona senza il suo consenso, integra la fattispecie di « attentato alla vita privata », sanzionato penalmente.

(68) Sul punto si veda anche l'art. 13 del recente D.P.R. 10 novembre 1997, n. 513, « Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2°, della legge 15 marzo 1997, n. 59 » (pubblicato in G.U. 13 marzo 1998, serie generale, n. 60), intitolato « Segretezza della corrispondenza trasmessa per via telematica », che dispone: « 1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche; 2. Agli effetti del presente regolamento, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario ». Norma la cui interpretazione ed effettività è sicuramente ancora tutta da verificare, ma che in base ad una sua prima lettura sembra portare diversi problemi all'attività degli *Internet provider*, e sicuramente pone il nostro Paese su posizioni molto anomale in tale materia rispetto alle altre realtà giuridico-economiche: con riferimento a tale argomento mi sia consentito il rinvio a quanto scritto in Ciacci G., *La firma digitale, cit.*, pp. 126-128.

(69) L'art. 13 del D.P.R. n. 513/97, su cui si veda la nota 68, sembra però non consentire tale tipo di eccezione, ponendo espressamente in capo agli « addetti alle operazioni telematiche », e tra questi rientra sicuramente il *provider* e la sua struttura, il divieto di « prendere cognizione della corrispondenza telematica » in genere, e quindi anche di quella dei propri clienti. Sarà quindi compito degli interpreti, a fronte della usuale mancata chiarezza e dell'apparente inappropriatezza a livello tecnico delle normative in materia di informatica giuridica, fornire agli operatori di settore le indicazioni su come concretamente adeguarsi alla nuova disciplina.

denzialmente stabilita con riferimento all'attività del gestore dei servizi telematici su Internet, in genere il *provider*, per gli aspetti tecnici, o il *webmaster*, per quelli contenutistici, per diversi motivi: quando l'intercettazione ed il controllo sia funzionale per l'amministrazione ottimale dello stesso sistema informatico, per la tutela dei diritti e della proprietà del gestore, quando sia espressione del monitoraggio occasionale necessario ai controlli sul buon funzionamento meccanico o qualitativo del servizio (69).

Ipotesi particolare è poi quella del datore di lavoro nei confronti dei propri dipendenti. In parte vengono applicate le stesse eccezioni dettate per il caso precedente, quello dei controlli ed intercettazioni effettuate dal gestore del servizio. A queste si somma poi l'ulteriore caso del consenso implicito del lavoratore al controllo delle proprie comunicazioni, ipotesi ammissibile quando quest'ultimo sia stato avvertito dell'esistenza di una politica di controllo in tal senso nell'impresa, oppure quando si tratti di un sistema informatico e telematico predisposto esclusivamente ai fini dell'esercizio della

stessa ([70]). Disciplina che si può ritenere applicabile anche nel caso di rapporto di pubblico impiego, sia sulla base dell'identità di *ratio* a prescindere dalla specifica fattispecie lavorativa, sia sulla base del d.lgs. 3 febbraio 1993, n. 29, che ha « privatizzato » il rapporto di lavoro degli impiegati pubblici.

Nel diritto italiano il divieto di intercettazioni delle informazioni in genere, di quelle elettroniche in particolare, è stabilito nel codice penale, modificato ed integrato dalla già ricordata legge 23 dicembre 1993, n. 547, in tema di criminalità informatica. Così, per quanto riguarda il nuovo testo dell'art. 616, che disciplina la « violazione, sottrazione e soppressione di corrispondenza » ([71]) (assoggettando il reo ad una pena variabile a seconda che il contenuto della stessa sia o meno rivelato), il cui quarto comma è stato sostituito con una nuova redazione che prevede l'ampliamento del concetto di « corrispondenza », tale da ricomprendere anche quella « ... informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza » ([72]). Così, per l'introduzione dei nuovi reati di « intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche » (art. 617 *quater* cod. pen, con pene variabili da sei mesi a cinque anni di reclusione), di « installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche » (art. 617 *quinquies* del codice, pena la reclusione variabile da uno a cinque anni), e di « falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche » (art. 617 *sexies*, anche qui punito con la reclusione da uno a cinque anni). Così, infine, anche per un'altra ipotesi di

([70]) Seppure si possa quindi considerare difficoltosa la posizione del lavoratore il cui messaggio sia stato intercettato, costretto a dimostrare non solo il carattere confidenziale e riservato della comunicazione rispetto al proprio datore di lavoro (e quindi di essere al di fuori dei casi indicati nel testo a favore dell'imprenditore), ma anche la possibilità che tale confidenzialità venisse percepita dai terzi, è sempre meglio per il datore di lavoro, che vuole sistematicamente sorvegliare le comunicazioni dei propri dipendenti sulla Rete, rendere note tale politica dell'impresa e la decisione di considerare i messaggi dei dipendenti quali messaggi della stessa impresa. La sorveglianza « elettronica » potrà allora essere ritenuta giustificata e non arbitraria (così HANCE O., *Internet e la legge*, McGraw-Hill, 1997, pp. 86-88).

([71]) Sul concetto di « corrispondenza informatica e telematica » si veda GALDIERI P., *op. cit.*, p. 45.

([72]) Sul punto si veda CORASANITI G., *La tutela della comunicazione informatica e telematica*, in AA.VV., *Profili penali dell'informatica, cit.*, p. 112, e GALDIERI P., *op. cit.*, pp. 115-119.

reato introdotta dalla legge citata, integrando una disposizione già presente nel testo originario (il reato di rivelazione del contenuto di documenti segreti, art. 621 cod. pen.), mediante l'estensione del concetto di documento a « qualunque supporto informatico contenente dati, informazioni o programmi », e quindi ai documenti elettronici: il reato in particolare collegato all'attività di chi rivela il contenuto di documenti che, pur non costituendo « corrispondenza », e non riguardando quindi l'intercettazione delle comunicazioni elettroniche, consiste comunque in un comportamento che incide sul diritto alla riservatezza dell'individuo (la sanzione in questo caso prevede la reclusione fino a tre anni o la multa fino a due milioni) ([73]).

4.3. – LA DISCIPLINA INTRODOTTA DALL'ART. 3 DEL D.LGS. 13 MAGGIO 1998, N. 171.

Di recente il legislatore italiano, recependo la Direttiva 97/66/CE del Parlamento europeo e del Consiglio sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, ha emanato il decreto legislativo 13 maggio 1998, n. 171, recante « Disposizioni 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 ». Nell'ambito dell'argomento esaminato nel presente scritto, alcune norme di tale decreto risultano essere di particolare interesse, essenzialmente con riferimento alla materia della corrispondenza elettronica su Internet, da una parte, e in materia di obblighi in capo a coloro che svolgono servizi informativi o telematici attraverso la Rete, dall'altra. Di questo aspetto si è già trattato nel precedente paragrafo, mentre nel presente si deve esaminare il disposto dell'art. 3 in materia di « Riservatezza delle comunicazioni ».

Tale norma introduce un obbligo di informazione in capo ai vari soggetti coinvolti nell'invio di messaggi di posta elettronica nel caso tale attività non garantisca la sicurezza della riservatezza delle comunicazioni ([74]). E nonostante

([73]) Si veda, a proposito del concetto di documento informatico rispetto alla nuova disciplina introdotta dalla legge n. 547 del 1993, BORRUSO R., *La tutela del documento e dei dati*, in AA.VV., *Profili penali dell'informatica, cit.*, pp. 1-39. Sul reato citato si veda anche CORASANITI G., *op. cit.*, p. 128.

([74]) L'obbligo relativo all'adozione delle misure idonee a garantire la sicurezza del servi-

che non venga prevista alcuna conseguenza nel caso di violazione di tale obbligo, risulta già importante di per sé la sua affermazione, in ogni caso ricondotta alla più generale disciplina introdotta dalla legge n. 675/96, in un settore che sembrava essere stato dimenticato da quello « statuto dell'informazione » che il legislatore ha voluto costruire con l'introduzione della normativa in materia di trattamento dei dati personali.

In particolare, gli obblighi di informazione vengono previsti nel citato art. 3 in capo a tre distinti soggetti: il fornitore del servizio di telecomunicazioni accessibile al pubblico, l'abbonato e l'utente ([75]). Infatti, il primo deve informare « 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 conservazioni da parte di soggetti a esse estranei ». Anche l'abbonato deve poi 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 ». Infine l'utente deve « informare l'altro utente quando nel corso della conversazione vengono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti ».

In questo modo il legislatore, insieme a quanto previsto negli artt. 6, 7 e 10 del d.lgs. n. 171/98, rispettivamente in materia di « identificazione della linea chiamante » il primo, di « chiamate di disturbo » il secondo e di « chiamate indesiderate » il terzo ([76]) (anche se poi rimane tutta da verifica-

zio è sancito nel precedente art. 2, comma 1°, che testualmente dispone: « 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* (n.d.r. legge 31 dicembre 1996 n. 675) *per salvaguardare la sicurezza del servizio e dei dati personali* ».

([75]) Definiti in maniera esplicita dalla stessa legge, ad eccezione del fornitore, all'art. 1: così « *abbonato* » è « 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 »; mentre « *utente* » è la « persona fisica che utilizza uno o più servizi di telecomunicazioni accessibili al pubblico, indipendentemente dall'eventuale qualità di abbonato ». Per il fornitore si può fare riferimento alla lett. d) dell'art. 1, che definisce il « servizio di telecomunicazioni » come « un servizio la cui fornitura consiste, in tutto o in parte, nella trasmissione e nell'instradamento di segnali su teti di telecomunicazioni, ivi compreso qualunque servizio interartivo anche se relativo a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi »: « *fornitore* » sarà quindi colui che presta tale servizio.

([76]) Per quanto riguarda la prima ipotesi, l'art. 6 prevede la facoltà per l'utente, che

re l'effettiva applicabilità di tali disposizioni, dettate per la fonia vocale o al massimo per il *telefax*, anche ai servizi comunicativi resi disponibili da Internet), ha esteso al mondo delle comunicazioni intersoggettive, effettuate attraverso il telefono o i servizi telematici, i principi informatori delle disposizioni in materia di trattamento di dati personali recentemente introdotte dalla legge 31 dicembre 1996, n. 675.

4.4. – La posizione del Garante in materia di corrispondenza elettronica.

In assenza di una produzione legislativa sul tema esaminato nel presente paragrafo, risulta interessante esaminare una recente pronuncia del Garante per la protezione dei dati personali in materia di corrispondenza elettronica ([77]).

chiama o riceve, di escludere la possibilità di identificare la linea chiamante, o di non accettare le telefonate che la eseludono (oltre all'obbligo del fornitore del servizio di informare gli stessi utenti di tale possibilità). Invece, con riferimento alle chiamate di disturbo, l'art. 7 al comma 1° prevede che « 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 ». Con riferimento infine alle chiamate indesiderate, l'art. 10 dispone 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 »; mentre al comma 2° rinvia agli artt. 11 e 12 della legge n. 675/96 in materia di consenso al trattamento, nel caso vengano adottati mezzi tecnici diversi da qnelli indicati al comma 1°: ipotesi che sembrerebbe più delle altre applicabile ai casi di invio di posta elettronica su Internet per finalità commerciali, come nelle ipotesi di c.d. « *spamming* » (sullo *spamming* si veda su Internet il numeroso materiale disponibile al seguente indirizzo *http://www.ljx.com/internet/iremail.html* consultato il 24 gennaio 2000).

([77]) Si veda in particolare Garante per la protezione dei dati personali, *Comunicato n. 23,* Privacy *e posta elettronica*, 12 luglio 1999, in *Cittadini e società dell'informazione*, giugno-settembre 1999, p. 96, e Morgoglione C., E-mail, *liste* e newsgroup *non possono essere violati*, in *La Repubblica.it* all'indirizzo *http://www.repubblica.it/online/internet/lettere/lettere/lettere.html* consultato il 9 febbraio 2000.

La fattispecie riguardava il ricorso al TAR di un impiegato statale censurato per avere espresso giudizi negativi sull'operato della struttura in cui prestava la propria opera: giudizi contenuti di una *e-mail* con cui il lavoratore aveva partecipato ad una *mailing list* a carattere para-sindacale, e che era stata però recapitata ai responsabili dell'ufficio. Motivo per cui l'impiegato aveva denunciato la violazione della propria *privacy*.

Il Garante, nell'indicato Comunicato, ha affermato innanzitutto la totale equiparazione della posta elettronica, delle *mailing list* e dei *newsgroup* (solo però di quelli « chiusi », quelli cioè per la cui partecipazione è necessario essere abilitati, ricevendo una *password* che consente la partecipazione allo stesso) alla normale corrispondenza cartacea. Per quanto riguarda poi la posta elettronica aziendale, il Garante non si è espresso relativamente all'assimilazione o meno dell'*account* del singolo dipendente presso la propria azienda o istituzione alla corrispondenza personale, privata, ma ha comunque dettato le modalità con cui tale aspetto debba essere disciplinato. Così, fino a quando il datore di lavoro non comunica ufficialmente, e senza possibilità di equivoci, che tutti i messaggi inviati tramite l'indirizzo aziendale di ciascuno vengono considerati nella disponibilità della stessa azienda (e quindi essere accessibili dallo stesso datore, o comunque visibili da tutti e in qualsiasi momento), ciascun utente ha diritto alla più assoluta tutela della riservatezza della propria casella postale elettronica. Nulla impedisce, però, alla società, di esplicitare questo vincolo: ma solo nel momento in cui tale principio viene comunicato i diritti alla riservatezza del lavoratore decadono (78).

5. – Conclusioni.

L'esame delle problematiche connesse alla tutela dei dati personali con riferimento alla rete Internet ed ai servizi da essa resi possibili, svolto nel presente scritto, permette di rilevare due diverse situazioni. Da una parte quella degli aspetti problematici che possono comunque essere risolti applicando le norme esistenti alle fattispecie concrete (che sono state ricomprese nei momenti definiti « statici » dell'attività di trattamento connessa ad Internet): chiaramente correttamente inquadrando tali fattispecie nella loro dimensione generalmente tecnica. Approccio che implica sicuramente uno sforzo da parte dell'interprete, teso alla formazione di una cultura delle nuove tecnologie proprio per compiere tale opera di adattamento in modo adeguato, ed evitare quindi di giungere ad errate conclusioni, anche giuridiche.

(78) Rientrando in questo modo nei principi già espressi anche in altri Paesi, e richiamati nei precedenti paragrafi.

Dall'altra quella delle ipotesi in cui il trattamento dei dati personali avvenga in relazione agli aspetti « dinamici » della rete Internet, che si è visto hanno sollevato le maggiori difficoltà connesse in genere all'applicazione degli obblighi stabiliti nella legge anche agli utenti del nuovo *media*, acquisitori o fornitori di informazioni e servizi, italiani o stranieri; ma anche, ed in particolare, con riferimento alle ipotesi di trasferimento dei dati personali all'estero (disciplinate dal più volte ricordato art. 28 della legge n. 675). Rispetto a tali problematici aspetti del rapporto tra tutela della riservatezza dell'individuo e utilizzo della rete Internet, occorre quindi trovare specifiche soluzioni che permettano di conciliare le diverse esigenze degli utenti, sia quelle ad ottenere il massimo di informazione, sia quelle a vedere corrispondentemente tutelati i propri dati personali.

In questo ambito si ritiene corretta la scelta di non escludere aprioristicamente le soluzioni adottate in Paesi tecnologicamente più avanzati del nostro, ma soprattutto con maggiore esperienza nel settore della comunicazione e dell'informazione *on-line*. Infatti il rilevante ritardo nel dettare una specifica disciplina legislativa in materia, o l'inappropriatezza talvolta delle norme già emanate nella loro applicazione al nuovo *media*, dimostrano come la strada dell'autoregolamentazione degli operatori del settore, o comunque le regole stesse del mercato dei servizi telematici che si è sviluppato, non debba essere scartata in assoluto (79). Strada che certamente deve essere percorsa con serietà e impegno da parte dei vari soggetti coinvolti a diverso livello nell'attività che si svolge in Internet, e comunque sotto il controllo

(79) « La risposta del mercato e del governo è allora quella di mettere a punto dei sistemi per salvaguardare la privacy. Come in una qualunque società, non possiamo garantire la privacy di ognuno; ma possiamo creare una situazione in cui i cittadini possano scegliere il grado di privacy che vogliono in base a compromessi stabiliti autonomamente; inoltre possiamo dare loro gli strumenti per protestare se le promesse vengono disattese » (così Dyson E., *Release 2.0. Come vivere nell'era digitale, cit.*, p. 206). Nel momento cioè in cui l'utente viene a conoscere l'approccio del *provider* di cui si è parlato nel par. 2.2., sarà per lui automatico scegliere un altro fornitore che maggiormente garantisca la sua *privacy*.

dell'organismo preposto a vigilare sulla corretta applicazione della disciplina in materia di tutela dei dati personali ([80]).

([80]) A tale proposito possono essere riportate le parole di uno dei membri dell'Autorità Garante che, in un'intervista rilasciata al *Sole 24 Ore* il 24 ottobre 1997, affermava che « Il principio che sta maturando è quello di garantire il rispetro della *privacy* nell'ambito delle reti aperte attraverso una strategia in quattro punti: – autodifesa da parte degli utenti, che devono accertarsi del livello di sicurezza offerto dal fornitore di servizi cui si rivolgono; – sviluppo di nuove tecnologie informatiche che assicurino elevati livelli di sicurezza e di protezione della privacy; – norme di disciplina concordate dai provider, non certo imposte dagli Stati; – diffusione della consapevolezza che Internet, per quanto in frenetica evoluzione e con capacità altamente diffusive, è pur sempre un *media* e, dunque, agli abusi commessi in Rete si possono applicare tutte le leggi e le regole dei codici ».