VINCENZO CARIDI

LA TUTELA DEI DATI PERSONALI IN INTERNET: LA QUESTIONE DEI LOGS E DEI COOKIES ALLA LUCE DELLE DINAMICHE ECONOMICHE DEI DATI PERSONALI

1. Premessa.

L'avvento delle reti telematiche, ed in particolare la diffusione di Internet, ha influenzato la tutela dei dati personali da un duplice punto di vista: da una parte, sotto un profilo che potremmo definire statico, ha fornito a soggetti pubblici e privati nuove possibilità di intercettazione e di sorveglianza elettronica ovvero di raccolta « occulta » dei dati personali[1]; dall'altra, introducendo una dimensione dinamica del problema, ha reso difficilmente controllabile la circolazione, lo scambio e l'aggregazione delle informazioni[2].

Un accenno al dato tecnico chiarirà questa affermazione.

Il termine « Internet« vale ad indicare sia la rete di comunicazione telematica, ossia l'infrastruttura, sia l'insieme di applicazioni informatiche — a loro volta distinguibili in servizi informativi e servizi telematici — mediante tale rete accessibili[3].

[1] Si pensi, per fare alcuni esempi, al fenomeno dei *log* e dei *cookies* (sui quali mi soffermerò diffusamente nelle pagine seguenti), al *mail grabbing*, ossia alla raccolta di indirizzi *e-mail* mediante *software*, detti *spamware*, appositamente immessi nella Rete, alle sollecitazioni commerciali non richieste attuate mediante l'invio di messaggi di posta elettronica (*mail spamming*), alle « cimici web » (per la descrizione delle quali si rinvia alla nota 8), alle informazioni raccolte tramite i motori di ricerca, ovvero, su altro versante, alle possibilità di controllo del datore di lavoro rispetto all'utilizzo della Rete da parte del dipendente, ovvero ancora in ambito pubblico, agli strumenti di intercettazione e sorveglianza forniti dalla Rete alle forze dell'ordine nello svolgimento dell'attività di indagine

[2] Per una completa analisi sulle effettive potenzialità lesive della rete Internet in tema di riservatezza cfr. Ciacci G., *La tutela del dei dati personali su Internet*, in *Trattato di diritto amministrativo diretto da Giuseppe Santaniello*, vol. XXVI, Cedam, Padova, 2000.

[3] Tra i principali servizi (applicazioni informatiche) di Internet basti qui citare la posta elettronica, i gruppi di discussione, il World Wide Web, le conversazioni in tempo reale (le c.d. chat), il trasferimento di file e la possibilità di collegamento a computers remoti. In relazione alla distinzione tra servizi informativi e servizi telematici, si ricorda che la distinzione è attuata sulla

A differenza di altri sistemi di comunicazione, la rete telematica Internet conferisce al suo utilizzatore la possibilità di interagire in tempo reale e di scambiare simultaneamente molteplici informazioni con una pluralità di stazioni comunicanti. Mentre, infatti, le reti tradizionali sono caratterizzate dalla passività e dalla unicità della trasmissione dei dati, il sistema di comunicazione a commutazione di pacchetto utilizzato dall'Internet è caratterizzato dalla interattività e dalla tendenziale illimitatezza di comunicazioni simultaneamente attuabili[4].

Ciò comporta, sotto il profilo che poc'anzi ho definito statico, una grande facilità nel raccogliere e nel cedere informazioni dal momento che il collegamento bi-direzionale tra le stazioni comunicanti permette un flusso informativo incrociato, in parte palese in parte occulto.

D'altra parte, sotto un profilo dinamico, i servizi informatici (siano essi informativi o telematici) annullano limiti e condizionamenti spazio-temporali nel trasferimento, nella scomposizione e nella selezione delle informazioni, per un verso rendendole facilmente « trattabili »[5], per altro verso

base del fatto che mentre nei primi lo strumento informatico è un mezzo di diffusione delle informazioni (come nel caso del Web), nei secondi l'applicazione informatica costituisce l'oggetto del servizio (si pensi ad esempio ai motori di ricerca).

[4] Le reti di comunicazione possono essere distinte, a seconda della tecnica di trasmissione dei dati, in due tipi: a commutazione di circuito e a commutazione di pacchetto. Nelle reti che adottano la prima tecnica, il collegamento mittente-destinatario — per tutto il tempo in cui la connessione rimane aperta — è continuo ed esclusivo, con la conseguenza che una stessa stazione non potrà svolgere più comunicazioni contemporaneamente. Il sistema più comune di rete a commutazione di circuito è la rete telefonica, nella quale la chiamata effettuata da un utente provoca un collegamento dedicato. La comunicazione a commutazione di pacchetto non implica l'esclusività del collegamento tra un computer ed un altro, permettendo, al contrario, che una stessa stazione comunicante svolga contemporaneamente più trasmissioni di dati. Inoltre, la commutazione di pacchetto è caratterizzata dal fatto che i dati da trasmettere vengono scomposti (*demultiplexing*) in pacchetti di dimensioni molto piccole (*datagram*), i quali, muniti dell'informazione necessaria per raggiungere la destinazione (che insieme a molte altre informazioni è contenuta nell'*header* aggiunta al *datagram*), vengono individualmente inoltrati nella rete per poi giungere, e lì essere riassemblati (*multiplexing*), sul computer di destinazione. Sia nelle reti di comunicazione a commutazione di circuito che in quelle a commutazione di pacchetto, nel percorso dal mittente al destinatario i dati viaggiano attraverso nodi intermedi (*gateways*), nel primo caso, però, l'informazione trasmessa viaggia su un unico percorso che viene occupato — per tutto il tempo della trasmissione — interamente, continuamente ed in maniera esclusiva da una sola comunicazione; nel secondo, invece, i pacchetti in cui sono scomposti i dati da trasmettere seguono percorsi differenti ed occupano i nodi intermedi per il solo tempo necessario al loro passaggio. Proprio questa differenza permette che una pluralità di computers connessi possano condividere tutti simultaneamente la capacità trasmissiva della rete. Il protocollo di trasmissione di Internet — oggi adottato, grazie alla sua economicità ed efficienza, dalle principali reti di computers — è il protocollo TCP/IP (*Trasmission Control Protocol/Internet Protocol*) il quale permette ai computers collegati in rete (nodi) di condividere risorse. In particolare TCP fa si che, prima della loro trasmissione, i dati vengano scomposti (*demultiplexing*) in una pluralità di *datagram* e che, una volta giunti a destinazione vengano riassemblati (*multiplexing*). Il protocollo IP si occupa, invece, di trasportare I singoli *datagram* (pacchetti) da un computer all'altro seguendo l'indirizzo contenuto nell'*header* (intestazione) di ogni *datagram*.

[5] L'art. 1, comma 2, lett. *b*), della legge 31 dicembre 1996, n. 675 definisce « trattamento » « *qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione,*

permettendone la diffusione (World Wide Web) e la comunicazione (posta elettronica) a prescindere da ambiti territoriali definiti e dalle normative che nei singoli Stati presidiano la riservatezza degli individui.

Gia queste prime generali considerazioni danno la dimensione dell'incidenza dello strumento tecnologico in analisi sul nucleo fondamentale della tutela riconosciuta ai dati personali dall'attuale impianto normativo europeo e nazionale[6]. Internet, infatti, non si pone semplicemente come un nuovo e più efficace mezzo di lesione del « diritto ad essere lasciato solo » (*right to be let alone*) — modello di tutela in verità già da tempo rivelatosi insufficiente rispetto alla portata dei flussi informativi che ci riguardano[7] — ma estende la propria incidenza sul più attuale « diritto all'autodeterminazione informativa » ponendo in discussione in più di un caso l'effettività dei principi, dei poteri e degli obblighi sanciti dalla direttiva 95/46/CE e recepiti nel nostro ordinamento con la l. n. 675/1996.

Nella realtà (*rectius* nella « virtualità ») dell'interconnessione telematica globale il nucleo forte della nuova tutela dei dati personali di matrice europea — che trova espressione nella legge n. 675 del 1996 nei principi di liceità, correttezza, trasparenza e pertinenza (art. 9), negli obblighi di informativa e di consenso preventivo (artt. 10 e 11), nei diritti di accesso, rettifica, opposizione e cancellazione (art. 13), nelle garanzie rafforzate previste per il trattamento dei dati sensibili (art. 22) e nelle prescrizioni per il trasferimento dei dati all'estero (art. 28) — si scontra con il fenomeno dei *logs*, dei famigerati *cookies*, con i *software* (*spamware*) immessi in Rete per raccogliere indirizzi *e-mail* (*mail grabbing*), con il « bombardamento » delle caselle di posta elettronica mediante messaggi commerciali non richiesti (*mail spamming*), con le « cimici web »[8], con la raccolta di dati personali tramite i motori di ricerca e con tutte le problematiche connesse alla genetica globalità di Internet.

---

la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati ».

[6] L'indagine che verrà svolta in queste pagine avrà in primo luogo quale referente normativo la disciplina italiana sulla tutela dei dati personali contenuta nella Legge n. 675 del 31.12.1996. Naturalmente in più di un caso il discorso verrà svolto con riferimento anche alla Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati a carattere personale e alla libera circolazione di questi dati, di cui la Legge italiana è attuazione.

[7] L'inadeguatezza rispetto alla società dell'informazione del *right to be let alone* è chiaramente espressa da SANTANIELLO G., *Il sistema delle garanzie della privacy*, in *Trattato di diritto amministrativo diretto da Santaniello G.*, vol XXVI, il quale afferma: « *La salvaguardia della sfera personale, esclusivamente quale ambito privato, riservato all'individuo senza alcun collegamento con il circuito di rapporti sociali, economici, partecipativi, tradiva un approccio di tipo proprietario, alla stregua di qualsiasi bene che il titolare aveva diritto di godere in modo esclusivo. Senonché il legame tra la persona e la sua sfera privata si è andato via via allentando con l'avvento delle tecnologie dell'informazione, traducendosi da potere di esclusione in un ben più rilevante potere di controllo del flusso di informazioni che la riguardano* ».

[8] Si tratterebbe di immagini invisibili poste su una pagina web che si comportano come *cookies*, tenendo traccia della navigazione degli utenti e permettendone l'identificazione. Secondo il *Los Angeles Times*, del 5 giugno 2001, nei siti web del Dipartimento della difesa USA si utilizzerebbero tali meccanismi per la raccolta occulta di dati personali dei visitatori. Cfr. sull'argomento la *newsletter* del 4-10 giugno 2001 del Garante per la protezione dei dati personali dal titolo « *USA: il sito della difesa USA raccoglie dati sui navigatori* », consultabile sul sito web www.garanteprivacy.it.

Tuttavia, la riconduzione alla disciplina di tutela della privacy, almeno in via teorica, non è egualmente problematica per tutte le citate tecniche. Rispetto ad alcune — mi riferisco in particolare a *mail grabbing*, *mail spamming* e motori di ricerca dei *newsgroups* — non è seriamente argomentabile che i trattamenti di dati personali mediante esse posti in essere pongano dubbi in relazione all'applicazione della l. 675/1996.

Il trattamento degli indirizzi di posta elettronica, ad esempio, — consista esso nella loro raccolta (*mail grabbing*) ovvero nell'utilizzazione per l'invio non sollecitato e massiccio di materiale pubblicitario (*mail spamming*) — è senza dubbio illecito se attuato senza prima aver fornito una puntuale informativa e senza aver acquisito il consenso espresso dell'interessato conformemente al disposto degli artt. 10 e 11 l. 675/1996[9]. Allo stesso modo integra un trattamento di dati personali la ricostruzione del profilo, degli interessi e della personalità di un utente attuata sulla base delle interrogazioni dallo stesso proposte al motore di ricerca di un *newsgroup*, trattandosi in questo caso di dati sensibili — opinioni politiche, convinzioni religiose, ecc. — il cui trattamento deve essere preceduto dal consenso scritto dell'interessato e dall'autorizzazione del Garante, *ex* art. 22, comma 1, l. 675/1996[10].

Rispetto a questi trattamenti[11] le questioni problematiche riguardano, più che la disciplina applicabile, l'effettiva individuazione dei comportamenti illeciti o dei loro autori, ovvero la genuinità del consenso troppo spesso carpito dietro l'offerta di un servizio « gratuito » per essere poi « ingabbiato » in clausole contrattuali del tutto illegittime[12].

---

[9] In relazione al fenomeno detto *mail spamming*, inoltre, si tenga presente la disciplina dettata dal d.lgs n. 171 del 13 maggio 1998, 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, ed in materia di attività giornalistica (*G.U.* serie gen. - n. 127 del 3 giugno 1998). In particolare l'art. 10 (chiamate indesiderate) di tale d.lgs richiede che l'invio di comunicazioni commerciali mediante un sistema automatizzato di chiamata debba essere preceduto dal consenso espresso dell'interessato. Inoltre, si ricorda come il medesimo sistema del consenso preventivo (tecnica dell'*opt-in*) sia previsto, per l'utilizzo della posta elettronica da parte di un fornitore, nell'art 10 del d.lgs. n. 185 del 22 maggio 1999, attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza (*G.U.* serie gen. - n. 143 del 21 giugno 1999). Si segnala, poi, la direttiva 2000/31/CE sul commercio elettronico, in corso di recepimento nel nostro ordinamento, la quale all'art. 7, scegliendo la tecnica dell'*opt-out*, prevede che « *gli Stati membri adottano i provvedimenti necessari per far si che i prestatori che inviano per posta elettronica comunicazioni commerciali non sollecitate consultino regolarmente e rispettino i registri negativi in cui possono iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni commerciali* ». Infine, il tema è oggi oggetto di ampio dibattito nell'ambito del travagliato iter di approvazione della proposta di direttiva sul trattamento dei dati personali nelle comunicazioni elettroniche, il cui art. 13 disciplina proprio l'*unsolicited mail*.

[10] A questa conclusione mi pare conducano le riflessioni di Ciacci G., *La tutela dei dati personali in Internet*, *op. cit.*, *pag. 381*.

[11] Riguardo alle « cimici web », funzionando esse come *cookies*, si rinvia ogni valutazione alle pagine dedicate a questo specifico argomento.

[12] Mi riferisco ai contratti di accesso « gratuito » ad Internet, nei quali, nonostante sia intervenuto sul punto il Garante per la protezione dei dati personali con una decisione del 13 gennaio 2000 (caso Libero di Infostrada), si continua in alcuni casi ad utilizzare informative che non chiariscono la facoltatività del consenso ai trattamenti a fini commerciali, e d'altra parte si inseriscono clausole risolutive di chiusura che rendono di fatto il consenso al trattamento dei dati personali il corrispettivo del servizio prestato.

Veri e propri problemi di applicazione della normativa europea e nazionale sui dati personali presentano, invece, seppure sotto distinti profili, due tecniche di raccolta e conservazione dei dati relativi al traffico Internet: i *logs* e i *cookies*. Tali meccanismi, vuoi per il loro funzionamento tecnico, vuoi per le esigenze di carattere ultraindividuale che in alcuni casi possono indirettamente soddisfare, vuoi per la loro utilità ai fini di una più veloce « navigazione », richiedono un maggiore sforzo interpretativo per essere ricondotti alla categoria dei trattamenti di dati personali e per essere assoggettati alla relativa disciplina.

Nelle pagine successive si tenterà di delineare in che misura la normativa a tutela della privacy sia ad essi applicabile, non prima però di aver accennato alle dinamiche economiche che oggi interessano i dati personali. È questo un aspetto di grande rilevanza nell'indagine relativa all'incidenza di Internet sulla riservatezza dell'individuo, che acquisisce ancor maggiore importanza e centralità nell'analisi degli aspetti problematici dell'applicazione della normativa europea e nazionale sui dati personali. La proliferazione di tecniche e meccanismi di raccolta, conservazione ed, in generale, di trattamento dei dati personali dell'utente della Rete trova, infatti, la sua principale giustificazione nella rilevanza economica del dato personale, generandone nuove dinamiche in cui tecnologia Internet e esigenze del mercato trovano un punto di incontro potenzialmente lesivo per la riservatezza dell'individuo.

2. Le dinamiche economiche dei dati personali.

Nell'ultimo decennio le modalità di raccolta e di diffusione dei dati ed, in generale, le modalità di circolazione delle informazioni sono profondamente mutate, così come pure è mutato il ruolo della conoscenza di informazioni nel contesto socio-economico. A tali cambiamenti ha contribuito certamente lo sviluppo delle tecnologie dell'informazione e della comunicazione (ICT) quale settore trainante dell'economia[13], che ha attivato dinamiche produttive nelle quali i fattori tradizionali sono stati affiancati e spesso superati, in termini di redditività e conseguentemente di investimenti, da nuove fonti di ricchezza. Si è assistito, in pratica, ad un processo di progressiva dematerializzazione delle fonti di produzione che trova la propria massima espressione nell'enorme importanza oggi assunta dal « capitale intellettuale »[14].

[13] In un recente studio dell'OSCE denominato « *Progetto Crescita* », che verrà presentato alla prossima riunione dell'Organizzazione dei Paesi più industrializzati, emerge con chiarezza, seppure in base a dati aggiornati al 2000, il ruolo fondamentale assunto dalle tecnologie dell'informazione e della comunicazione nella crescita dell'occupazione e della produttività del lavoro. In particolare, la ricerca giunge a tali conclusioni analizzando le ragioni delle differenze in termini di crescita del PIL pro capite degli Stati Uniti rispetto ai principali Paesi europei (fonte: *Il Sole 24-Ore*, 25 maggio 2001, inserto New Ecomomy, articolo « *Le Telecomunicazioni fonte di crescita* », a firma Antonio Perucci)

[14] Cfr. l'ampia analisi svolta da Thomas; A. Stewart, Il capitale intellettuale, Milano, 1999. Sulle nuove tendenze economiche dell'era che stiamo vivendo di particolare interesse è anche il recente lavoro di Jeremy Rifkin, *L'Era dell'accesso*, Milano, 2000.

In tale quadro generale la conoscenza è interessata da nuove dinamiche economiche alla luce delle quali svolge un ruolo propulsivo nella c.d. *new economy* e ciò non solo per il fatto che genera ricchezza al pari delle fonti tradizionali, ma anche in quanto costituisce essa stessa un prodotto scambiato nel mercato, soprattutto quando si atteggia come conoscenza specialistica ovvero come informazione specifica.

Ai fini della nostra analisi rileva evidenziare, in particolare, l'esponenziale crescita dell'importanza economica della conoscenza di dati relativi alla persona, quali informazioni specifiche utili alle imprese per delineare il mercato di un determinato prodotto o servizio.

Le notizie idonee ad identificare un soggetto, dalle più semplici e scarne quali quelle anagrafiche, a quelle che ne delineano il profilo come consumatore, quali attitudini al consumo, gusti e capacità reddituale, sino a quelle più intime e personali, quali quelle attinenti alla salute ed alle attitudini sessuali o alle opinioni politiche e religiose, divengono oggetto di raccolta, di selezione, di aggregazione e di stoccaggio in banche di dati. Il fine è quello di arrivare ad un profilo del consumatore-utente quanto più completo possibile ed in ogni caso tale da offrirgli proprio il prodotto o il servizio che egli è più propenso ad acquistare[15].

La tecnologia telematica fornisce gli strumenti tecnici per la gestione delle informazioni alla luce del loro nuovo valore socio-economico, agevolandone la fruibilità e lo sfruttamento con effetti talmente pervasivi da determinare quello che è stato definito un mutamento genetico del trattamento dei dati[16]. Mediante essa, infatti, la promozione commerciale viene agevolata e resa più incisiva sia nella fase di diffusione del messaggio promozionale, sia nella fase propedeutica della raccolta delle informazioni sugli utenti-consumatori.

Si pensi ad una campagna pubblicitaria attuata mediante l'invio di *e-mail* commerciali.

In questo caso l'impresa che vuole pubblicizzare il proprio prodotto, utilizzando le applicazioni informatiche accessibili mediante la Rete, potrà agevolmente ed efficacemente svolgere tutte le fasi del processo promozionale. In primo luogo avrà la possibilità di raccogliere direttamente tramite il proprio sito (*rectius* tramite il server su cui è memorizzato il proprio sito web) i dati relativi alle preferenze ed alle abitudini d'acquisto dei visitatori — esplicitamente, richiedendo la compilazione di un formu-

---

[15] È questa la finalità del *direct marketing*, ossia della tecnica di promozione di prodotti e servizi presso quei consumatori-utenti di cui si conoscono, per averle previamente acquisite sulla base di indagini mirate, gusti e propensione all'acquisto. « La profilazione », ossia la definizione del profilo di un consumatore attuata mediante il monitoraggio e l'analisi della sua navigazione nella rete Internet, costituisce oggi uno dei mezzi di indagine strumentali al *direct marketing* più usati e più efficaci. Certo la profilazione degli utenti non è un fenomeno nato con la Rete, si pensi ad esempio alle *fidelity card* distribuite ai clienti di centri commerciali e supermercati quali strumenti utilizzati ai medesimi fini, ma la tecnologia Internet ha fortemente agevolato il raggiungimento di quegli scopi. Vedremo più avanti quali sono gli strumenti tecnici adoperati. Basti qui evidenziare che sono sempre più numerose le società che creano e sviluppano metodi di analisi sempre più sofisticati per fornire banche dati quanto più complete possibili alle imprese.

[16] Bersani C., *La privacy e la gestione di banche dati informatizzate: alcune problematiche emergenti*, in *Trattato di diritto amministrativo*, diretto da Giuseppe Santaniello, vol. XXVI, pag. 39.

lario elettronico, ovvero in maniera occulta, tramite il meccanismo dei *logs* e dei *cookies* —, oppure potrà acquistarli da terzi, i quali, a loro volta, li avranno previamente raccolti utilizzando i medesimi metodi; in secondo luogo sarà in grado di acquisire gli indirizzi *e-mail*, raccogliendoli direttamente durante la visita del proprio sito (proponendo la compilazione di un *guestbook* ad esempio), oppure operando la raccolta su spazi Internet pubblici, come *newsgroups* o *chat-rooms*, oppure ancora utilizzando quei *software*, detti *spamware*, che possono essere immessi in Rete proprio a tale fine. Infine, potrà procedere all'invio delle *e-mail* commerciali. Raggiungerà così un rendimento di gran lunga maggiore rispetto alle comunicazioni postali tradizionali (tra il 5 e il 15% contro lo 0,5-2%), a costi ridotti rispetto ai metodi di *direct marketing off-line* ed infine con una più elevata percentuale di risposte rispetto ai *banners*[17] (18% contro lo 0,65%)[18].

Nasce, dunque, un mercato dei dati personali, il quale trova nelle tecniche di raccolta dei dati in Rete una fonte di approvvigionamento[19].

Si tratta però di un mercato singolare, in cui ad una « domanda » consapevole e mirata si contrappone una « offerta » nella migliore delle ipotesi caratterizzata dall'inconsapevolezza di cedere un prodotto avente un valore economico (come accade quando si forniscono i propri dati compilando un formulario elettronico per accedere ad un servizio o quando si compila un semplice *guestbook*) ovvero, nelle ipotesi più gravi ed ancora purtroppo frequenti, caratterizzata dalla totale inconsapevolezza di cedere dati personali (come avviene in occasione di ogni connessione alla Rete e di ogni visita di siti che utilizzano i *cookies*).

In questo mercato *sui generis* non possono dirsi autentici offerenti coloro i quali cedono dati personali nell'inconsapevolezza di essere in un mercato e, d'altra parte, non può individuarsi una « domanda » nelle tecniche più o meno lecite di raccolta del prodotto « dato personale ». Un mercato, dunque, falsato a cagione del fatto che la circolazione del prodotto avviene sulla base delle sole esigenze di una parte e non in base al suo fisiologico funzionamento che prevede, invece, il libero e cosciente confronto dei protagonisti della domanda e dell'offerta.

Il rispetto della disciplina a tutela dei dati personali può costituire un efficace correttivo a questa « società della classificazione », come la definisce lo stesso Garante per la tutela dei dati personali[20], nella quale si ricer-

[17] Si tratta di un altro metodo per veicolare il messaggio pubblicitario in Rete. Il termine, letteralmente bandiera o striscione, indica uno « cartellone elettronico », in genere rettangolare, posto sulla *home page* o sulle pagine interne di un sito per pubblicizzare una azienda o un suo prodotto.

[18] I dati sono desunti dallo Studio della Commissione europea — DG XV Mercato Interno — pubblicato a gennaio 2001, sulle comunicazioni commerciali indesiderate attuate mediante posta elettronica.

[19] Il fenomeno della commercializzazione dei dati personali è particolarmente vivo negli USA (cfr. sul punto la newsletter del Garante per la protezione dei dati personali del 3 dicembre 2000, nella quale si evidenziano i rischi per la privacy derivanti dalla vendita dei dati negli U.S.A.). Tuttavia, anche negli Stati Uniti, le reazioni dei consumatori ad una pubblicità aggressiva e non richiesta ha indotto alcune società a mutare la propria privacy policy, mirando ad una cosciente e corretta cessione-acquisizione dei dati.

[20] Cfr. il discorso di presentazione della « Relazione annuale 1999 » del Presidente dell'Autorità Garante per la protezione dei dati personali, Prof. Stefano Rodotà.

cano « voracemente » dettagliate informazioni sulle persone e sui loro comportamenti mediante pratiche palesi ed occulte atte a sollecitare la cessione di dati personali, richiedendola quale contropartita di un servizio ovvero stimolandola con la promessa di un beneficio[21].

3. La questione dei logs e dei cookies.

3.1. *Rilievi introduttivi.*

Tra i meccanismi più efficaci ed insidiosi per la raccolta e la conservazione dei dati personali in Rete vi sono i *logs* e i *cookies*. In sostanza tramite essi, seppure con modalità diverse, si acquisiscono informazioni relativamente ai tempi di ogni sessione di connessione, alle pagine web visitate, alle parole chiave e *all'user ID* e a quant'altro valga a definire il profilo di un utente. Sembrerebbe, dunque, pacifico che si tratti di fenomeni soggetti alle disposizioni nazionali e comunitarie sui dati personali. Tuttavia, per quanto vi siano, sugli uni come sugli altri, diffuse opinioni che si esprimono in termini assoluti, sostenendone il carattere *tout court* lesivo della privacy dell'internauta, ovvero, all'opposto, l'assoluta irrilevanza offensiva, in ambedue i casi il tema rifugge da una soluzione netta e richiede, invece, un'attenta riflessione capace di operare distinzioni nell'ambito di categorie apparentemente omogenee e, soprattutto, di contemperare il dato tecnico dei fenomeni, l'input economico sotteso al loro concreto atteggiarsi e la ratio giuridica delle norme da applicare.

L'analisi che verrà svolta nelle pagine seguenti tenterà di individuare in che termini ed in che misura la disciplina di tutela dei dati personali oggi vigente sia ad essi applicabile.

È però sin d'ora opportuno rilevare che la soluzione al problema non può essere ricercata con esclusivo riferimento al dato tecnico. Se è, infatti, vero che la cognizione del funzionamento dei meccanismi in discorso serve a fugare generici ed in parte immotivati allarmismi su Internet[22], è pur

[21] Negli U.S.A. la commercializzazione dei dati personali è una prassi consolidata e la raccolta di dati, complice un approccio autoregolamentare quasi mai efficiente, viene spesso attuata nella totale inconsapevolezza dell'utente. Si pensi, per citare uno dei molteplici esempi di una realtà vastissima, al caso della *Digital Convergence*, società di Dallas che ha regalato oltre un milione di lettori di codici a barre — denominati *CueCat* — a proprietari di computers in tutta America con la finalità di trarre profitto dalla commercializzazione delle informazioni sulle abitudini di consumo degli utenti ricavabili al momento dell'istallazione del software che permette il funzionamento di tali lettori. Le informazioni così raccolte dovevano essere poi correlate con quelle raccolte dalla *Digital Convergence* ad ogni scansione attuata mediante i lettori *CueCat*. La vicenda è stata riportata nella newsletter del 17 dicembre 2000 del Garante per la Privacy che può essere consultata sul sito web www.garanteprivacy.it.

[22] Ciacci G, *La tutela dei dati personali su Internet*, *op. cit.*, sostiene che: « *... 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...* », ma « in realtà *un'attenta lettura di tali notizie, chiaramente svolta anche attraverso un riscontro delle stesse su base tecnica, permette di ridimensionare notevolmente i pericoli che sem-*

vero che un'indagine che tenga conto del solo aspetto tecnico non potrà che giungere a conclusioni parziali.

Il discorso sulle dinamiche economiche dei dati personali in Rete mi pare abbia chiarito che i rischi per la privacy dell'utente Internet debbano essere valutati alla luce del connubio tra tecnologia e mercato e che, dunque, l'analisi dei flussi di dati personali, e le conseguenze sui diritti della personalità dei titolari, debba essere svolta tenendo in massimo conto anche, e sempre più, il dato economico.

3.2. *I logs*.

I logs, già da qualche tempo, animano, anche a livello istituzionale, un vivace dibattito dovuto alla contrapposizione di due fondamentali esigenze: quella della tutela della riservatezza, appunto, e quella della lotta al *cyber-crime*[23].

Ma partiamo dal dato tecnico.

I *logs* sono registrazioni — generate automaticamente dal sistema del fornitore di accesso alla Rete (*Internet access provider*)[24] in occasione di ogni connessione — relative ad alcuni dati quali l'indirizzo I.P. dell'*host computer*[25] utilizzato per la connessione, la data ed l'ora in cui il computer identificato da quell'I.P. ha effettuato il collegamento e il tempo di durata della connessione. In realtà l'*access provider* può anche conoscere —

brano correre gli utenti di Internet ». Tuttavia, come cercheremo di dimostrare, la rilevanza economica dei dati personali riacutizza i rischi per la privacy dell'utente, che alla luce dell'analisi tecnica appaiono, secondo l'ineccepibile ma parziale ragionamento dell'autore, ridimensionati.

[23] Il dibattito cui si fa cenno è quello tra il Gruppo di lavoro dei Garanti europei, istituito ai sensi dell'art. 29 della direttiva 95/46/CE, da una parte, e il Consigli d'Europa e la Commissione U.E. dall'altra, relativamente al progetto di Convenzione del Consiglio d'Europa ed alla proposta contenuta nella Comunicazione della Commissione del 30 gennaio 2001 [COM(2001)890], entrambi riguardanti la sicurezza delle infrastrutture dell'informazione e la lotta al *cyber-crime*. I Garanti europei, riunitisi ad Atene per la « Conferenza di primavera » dal 10 all'11 maggio 2001, hanno espresso forte preoccupazione per il progetto in base al quale i fornitori di servizi Internet — allo scopo di permettere l'eventuale accesso da parte delle forze di polizia impegnate nella lotta al *cyber-crime* — dovrebbero conservare i dati relativi al traffico in rete indipendentemente dagli obblighi di fatturazione.

[24] L'*Internet access provider* è il soggetto che professionalmente fornisce ai propri clienti il servizio di connessione alla rete Internet concedendo a questi ultimi, sulla base di un contratto di abbonamento, il diritto di collegarsi al proprio punto di accesso, detto POP (*point of presence*), il quale è permanentemente connesso alla rete Internet. In molti casi il *provider* fornisce anche altri servizi ai propri abbonati, quali una o più caselle di posta elettronica, l'iscrizione ad un newsgroup, uno spazio di memoria per mettere in linea una propria pagina web. In questo caso è più corretto definire il fornitore di tali servizi *Internet service provider*.

[25] Ogni computer collegato alla rete Internet (*host computer*) è dotato di un indirizzo univoco, I.P. *number*, mediante il quale è individuato. Tale indirizzo numerico è composto di quattro cifre decimali intervallate da punti. Gli indirizzi numerici così formati non sono però infiniti, degli oltre quattro miliardi di combinazioni possibili, molte sono già state assegnate. Ciò comporta che spesso gli Internet *access provider*, ossia i fornitori della connessione alla Rete, assegnino ad ogni utente un diverso I.P. per ogni singola connessione in modo da avere un numero maggiore di I.P. sempre a disposizione.

con uno sforzo tecnico mirato — i siti visitati durante ogni sessione di connessione tramite un proprio POP (*point of presence*)[26].

L'*Internet access provider* in forza di tali registrazioni è in grado di acquisire, in maniera invisibile, informazioni sui propri clienti sulla base dell'associazione cliente - indirizzo I.P..

Le medesime informazioni, arricchite da quelle relative alle singole pagine web consultate, vengono registrate automaticamente, ad ogni visita, nei *logs* dei *server* su cui sono memorizzati i siti visitati durante la navigazione.

Si verifica anche in questo caso la cessione di dati, vedremo più avanti se personali o meno, nell'inconsapevolezza del titolare degli stessi.

Il gestore di ogni sito web, o fornitore dei contenuti (*content provider*), potrà allora conoscere, rispetto ad ogni collegamento al proprio sito, informazioni utili a delineare le preferenze manifestate dal visitatore.

Il punto da chiarire è, a questo punto, quello della identificabilità del titolare dei dati registrati nei *files* di *logs* dell'*access provider* e del *content provider*.

L'*Internet access provider*, come rilevato poc'anzi, può associare l'indirizzo I.P. dell'*host computer* al proprio cliente, di cui possiede tutti i dati identificativi per averli acquisiti in sede di stipulazione del contratto di accesso alla Rete. Il *content provider*, invece, non avendo nessun rapporto contrattuale pregresso con il visitatore del sito, acquisirà informazioni anonime, in quanto non riferibili ad un utente identificato, ma relative solo ad un I.P. *number*, dal quale, al più, potrà desumere l'*access provider* utilizzato dal navigatore per connettersi alla Rete.

Ne discende che le informazioni contenute nei *files* di *log dell'access provider*, anche alla luce del solo dato tecnico, sono senza dubbio « personali », in quanto relative ad un soggetto — il cliente — individuabile mediante un numero di identificazione personale — I.P. number — assegnato dallo stesso fornitore di accesso.

Alla medesima conclusione non si perviene in relazione ai *files* di *log* del *content provider*. Ed in effetti, presi a sé, i dati relativi alla navigazione, contenuti nei *files* di *log* registrati sul *server* nel quale è memorizzato il sito visitato, non contengono informazioni relative ad un soggetto identificato o identificabile e quindi, almeno stando al dato tecnico ed alla definizione di « dato personale » contenuta nell'art. 1, comma 2, let. *c*), l. 675/96, non dovrebbero essere soggetti alle disposizioni nazionali (e comunitarie) sui dati personali.

Tuttavia, se — conformemente alle considerazioni premesse al presente discorso — ampliamo la prospettiva all'aspetto economico, possiamo avere contezza di come la conclusione che precede sia parziale, trascurando le effettive potenzialità lesive della privacy dell'utente connesse alle dinamiche economiche che interessano i dati personali in Rete.

I *files* di *log* del *content provider*, infatti, per effetto di accordi commerciali duraturi, vengono spesso incrociati con i *file* di *log* dell'*access provider*, acquisendo una marcata valenza lesiva della privacy dell'ignaro navigatore.

---

[26] Il *point of presence (*POP) è il punto di connessione permanente di un *service provider* alla Rete telematica Internet.

Sulla base di tali accordi — tutt'altro che infrequenti[27] — il fornitore di contenuti potrà ricondurre le informazioni a sua disposizione, altrimenti relativi ad un anonimo I.P. *number* ed utilizzabili al massimo in forma aggregata, ad un soggetto identificato[28].

Una volta chiarito in che termini ed in che misura si possa parlare di dati personali a proposito dei *logs*, si pone il problema di individuare la disciplina da applicare ai trattamenti su di essi effettuati.

Al riguardo, fermo l'obbligo di fornire le informazioni previste dall'art. 10 l. 675/1996, è necessario stabilire, anche in relazione alle posizioni spesso assunte dai *providers*, se le registrazioni in parola comportino trattamenti soggetti *in toto* agli obblighi sanciti nella l. 675/96, ovvero se, rispondendo ad una esigenza contrattuale o all'adempimento di un obbligo legale, regolamentare o comunitario, rientrino tra quei trattamenti per cui è escluso il consenso preventivo del soggetto interessato. Nel primo caso, infatti, sia il fornitore dell'accesso a Internet, sia il gestore di un sito web dovrebbero preventivamente acquisire il consenso espresso, rispettivamente, dei propri clienti e dei propri visitatori, in relazione alla registrazione e conservazione dei dati relativi alla navigazione, conformemente al disposto dell'art. 11, l. 675/96; nel secondo caso, invece, si avrebbe un trattamento per il quale non è necessario il consenso preventivo del soggetto interessato a norma dell'art. 12, lett. *a*) e *b*), della medesima legge.

A complicare la questione vi è poi il fatto che le registrazioni della traccia delle navigazioni dell'utente, siano esse considerate nel primo o nel secondo senso sopra prospettati, costituiscono il presupposto della profilazione dell'internauta attuata a fini commerciali, sicché i dati personali contenuti nei files di *log* vengono spesso ceduti a società specializzate le quali elaborano i dati facendoli oggetto del proprio *business*. Tale circostanza, integrando una comunicazione di dati personali, importerà in ogni caso la necessità del consenso del soggetto interessato a norma dell'art. 20, let. *a*), l. 675/96.

Il tema si pone, come spesso accade nell'ambito dei diritti della personalità, in termini di contrasto tra situazioni giuridiche soggettive[29].

In relazione al trattamento dei dati personali dell'utente Internet attuato tramite la registrazione di dati relativi al traffico (i *logs* appunto),

---

[27] Si pensi che tutti i più grandi fornitori di accesso alla Rete italiani forniscono il proprio servizio congiuntamente ad un sito (portale web) che offre servizi informativi e commerciali, riunendo, dunque, le due qualifiche di *access provider* e di *content provider* e rendendo lo scambio di informazioni un fatto non solo possibile, ma altamente probabile.

[28] Così BARBUTI M., intervento alla Conferenza *Internet e privacy: quali regole?*, svoltasi a Roma l'8 maggio 1998. Nello stesso senso CIACCI G., *La tutela dei dati personali su Internet*, *op. cit.*, pag. 378 e ss.

[29] La tutela della riservatezza e dell'identità personale quale tutela di diritti fondamentali ha, infatti, una caratterizzazione trasversale atteggiandosi come argine all'esercizio di una numerosa serie di interessi di settore. Si pensi all'interesse della Pubblica Amministrazione a conoscere i soggetti che compongono la collettività di cui deve soddisfare i bisogni; oppure alle esigenze della ricerca scientifica — in ambito sanitario, economico, previdenziale — la quale può avere necessità di conoscere informazioni relative ai soggetti determinati; si pensi, infine, ed è il nostro caso, all'interesse degli esercenti attività imprenditoriale per i quali la raccolta di informazioni quanto più dettagliate possibili sul pubblico dei consumatori è una dato di grande rilevanza economica.

la tutela della riservatezza dell'internauta viene in contrasto da una parte, con situazioni soggettive riconducibili agli *Internet provider*, ossia ai fornitori di servizi e di contenuti, dall'altra con le esigenze di sicurezza connesse alla repressione dei reati compiuti a mezzo dello strumento telematico in questione .

Proprio su questa linea, in genere, si sostiene che la registrazione e la conservazione dei files di *log* è necessaria per poter dimostrare la corretta esecuzione da parte dei fornitori di accesso ad Internet delle obbligazioni assunte nel contratto, oltre che per essere sempre in grado di fornire le informazioni in essi contenute all'autorità giudiziaria qualora questa ne faccia richiesta[30]. Se così fosse nessun consenso sulle registrazioni in discorso dovrebbe essere richiesto dall'*Internet access provider* al cliente che chiede di connettersi alla Rete tramite il proprio POP ed egli avrebbe solo l'obbligo di fornire l'informativa di cui all'art. 10, l. 675.

È però necessario distinguere il profilo dell'esclusione del consenso per motivi « contrattuali », da quello riconducibile all'esistenza di un obbligo legale; non solo in relazione all'evidente diversità di rango degli interessi ad essi sottesi, ma anche e soprattutto in relazione alle prospettive che, *de jure condendo*, si profilano a livello europeo sulla sicurezza delle infrastrutture dell'informazione e sulla lotta alla criminalità informatica.

Quanto al primo profilo, si deve osservare che l'esigenza di carattere para-probatorio, in virtù della quale si sostiene che la conservazione dei dati relativi al traffico sarebbe necessaria ai *provider* per dimostrare l'esatta esecuzioni delle obbligazioni assunte con il contratto di accesso ad Internet, non vale a ricondurre tale trattamento tra quelli elencati nell'art. 12, let. *b*), l. 675/1996. La conservazione dei *logs*, infatti, risponderebbe, secondo questa prospettiva, ad una esigenza successiva all'esecuzione del contratto, rispetto alla quale non può ritenersi strumentale e, in ogni caso, determinerebbe un trattamento finalizzato alla precostituzione di un mezzo di prova in relazione ad una fase patologica del tutto eventuale. Inoltre, anche a voler ritenere legittima tale finalità, come pare si sia fatto nella proposta di direttiva relativa al trattamento dei dati personali nelle comunicazioni elettroniche [COM(2000)385], ciò non legittima la conservazione dei data-logs, in quanto i dati in essi contenuti appaiono, per quantità e qualità, sproporzionati rispetto a quella finalità del trattamento. L'art. 5, comma 2 della citata proposta di direttiva, d'altra parte, ritiene non incompatibile con la riservatezza delle comunicazioni la registrazione dei dati relativi al traffico effettuata al fine di provare una transazione, solo quando essa sia « legalmente autorizzata ». Tale requisito sembra rimandare al quadro normativo comunitario e nazionale, nel quale, salvo

---

[30] Esemplificative sono al riguardo le dichiarazioni rese da un noto *provider* dinnanzi all'Autorità Garante per la protezione dei dati personali, la quale aveva avviato accertamenti ai sensi degli artt. 31 e 32, comma 1, della L. n. 675/1996. Il *provider* ha, in quella sede, affermato che l'inserimento nel modulo di iscrizione dei dati anagrafici relativi all'indirizzo dell'abbonato sarebbe necessario per « *ragioni di sicurezza* » e, in particolare, per ottemperare a richieste dell'autorità giudiziaria volte ad ottenere, per indagini penali in corso, « *la comunicazione dei dati associabili ad un certo User ID attraverso il quale in data e ora definiti si è realizzata una navigazione* ». La decisione citata è quella relativa al caso « Libero di Infostrada » del 13 gennaio 2000, consultabile all'URL http://www.garanteprivacy.it.

specifiche eccezioni, sono legalmente autorizzati i soli trattamenti che abbiano ricevuto il *placet* dell'interessato.

Sotto questo profilo, dunque, l'*access provider* non è legittimato a raccogliere e conservare i dati relativi al traffico generato dai propri clienti senza il loro consenso, né tanto meno sarà legittimato il *content provider*, il quale non abbia con il visitatore del proprio sito un rapporto contrattuale che esplicitamente preveda tale conservazione.

Quanto all'esclusione del consenso *ex* art. 12, let. *a*), l. 675/96, la norma prevede che « *il consenso non è richiesto quando il trattamento riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria* ».

Se, dunque, sussistesse un obbligo di comunicare all'autorità giudiziaria i dati relativi al traffico, certamente potremmo affermare la legittimità della raccolta e della conservazione di tali dati senza necessità di alcun consenso del soggetto interessato.

Tuttavia, nessuna di tali fonti normative impone agli *Internet providers* un tale obbligo. Ed anzi, le norme sulla responsabilità dei *providers* oggi in vigore tendono ad escludere ogni contegno positivo dei fornitori di accesso finalizzato all'individuazione di fatti criminosi posti in essere da soggetti che tramite essi si connettono ad Internet o che violino la legge penale utilizzando servizi informatici (*e-mail*, *newsgroup*, ecc.) da essi forniti.

Ciò è sancito chiaramente nella Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000. Nella sezione quarta di tale direttiva, intitolata « Responsabilità dei prestatori intermediari », si esclude la responsabilità dei fornitori dell'acceso ad Internet (*access provider*) (art. 12), dei fornitori di servizi Internet (*service provider*) (art. 13) ed anche dei fornitori del servizio di *hosting* (art. 14), a condizione che non intervengano in alcun modo sulle informazioni che, a seconda del servizio prestato, trasmettono (*mere conduit*), memorizzano temporaneamente (*caching*) ovvero permanentemente (*hosting*). L'articolo 15 della direttiva interviene poi ad eliminare ogni dubbio sulla necessità di trattamenti con finalità preventiva, quali quelli attuati mediante la registrazione delle informazioni relative alla navigazione (*log*), sancendo l'assenza di un obbligo generale di sorveglianza dei prestatori di servizi della società dell'informazione rispetto ad attività illecite[31].

Se questo è lo stato della normativa, in virtù del quale nessun obbligo legale, regolamentare o comunitario, grava sui fornitori di servizi Internet relativamente alla raccolta ed alla conservazione di informazioni sul traffico dei propri clienti, è pur vero che a livello comunitario, mentre in Italia la direttiva 2000/31/CE è in corso di recepimento, si profila un diverso ap-

[31] Art. 15 Dir. 2000/31/CE (Assenza dell'obbligo generale di sorveglianza): « *1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.* »

proccio nell'ambito della politica di sicurezza delle infrastrutture dell'informazione.

Il riferimento è all'art. 5.2 della Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato economico e sociale e al Comitato delle Regioni del 30 gennaio 2001 [COM(2000)890], dal titolo « *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica* « , nonché agli artt. 20 e 21 del progetto di Convenzione sul *cyber-crime* (*Draft Convention on cyber-crime*)[32].

Il presupposto delle citate norme è che, contenendo i *files* di *log* informazioni di grande utilità per l'autorità giudiziaria e per le forze di polizia che indagano sui crimini informatici, sarebbe necessario prevedere la loro conservazione obbligatoria.

In particolare, gli artt. 20 (*Real-time collection of traffic data*) e 21 (*Interception of content data*) del progetto di Convenzione del Consiglio d'Europa disegnano un sistema nel quale, seguendo una direzione diametralmente opposta a quella scelta nella direttiva 2000/31/CE (artt. 12, 13, 14 e soprattutto 15), i *providers* dovranno raccogliere e conservare i *logs* di sistema ed ogni altra informazione rilevante a fini penali e dovranno mettere a disposizione i propri sistemi per l'effettuazione di attività di indagine.

È evidente che tali posizioni, pur prospettando un cambiamento di rotta, confermano secondo quanto siamo andati sostenendo l'inesistenza, allo stato attuale, di un obbligo di raccolta e conservazione dei dati relativi al traffico gravante sui fornitori di accesso ad Internet. Anzi, il presupposto è proprio quello che i fornitori di servizi di informazione debbano oggi eliminare ovvero rendere anonimi tali dati immediatamente dopo la fornitura del servizio, in adempimento al disposto della direttiva 95/46/CE[33] e alle più specifiche disposizioni della direttiva 97/66/CE[34], cui in Italia è stata data esecuzione con il d.lgs. 13 maggio 1998, n. 171[35]. Significative, al riguardo, sono le considerazioni contenute nell'art. 5.2 della Comunicazione COM(2000)890, le quali fanno discendere la necessità di imporre un obbligo di conservazione dei *files* di *log* dal fatto che sempre più fornitori del servizio di accesso ad Internet, applicando tariffe forfetarie ovvero concedendo accesso gratuito — col conseguente venir meno dell'obbligo di fatturazione connesso alle tariffe a tempo — non sono legittimati a svolgere alcun trattamento di dati personali relativi al traffico mediante essi generato.

In sostanza, l'intervenuto mutamento dei termini delle offerte di accesso alla Rete, ormai quasi tutte gratuite, non legittima più i fornitori di accesso

---

[32] L'ultima versione (revisione n. 27, adottata a Strasburgo il 25 maggio 2001) del progetto di Convenzione del Consiglio d'Europa è consultabile all'URL http://www.interlex.it.

[33] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati a carattere personale e alla libera circolazione di questi dati.

[34] Direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (*G.U.* L 24 del 30 gennaio 1998)

[35] Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento e del Consiglio, ed in tema di attività giornalistica.

alla conservazione dei dati relativi al traffico, consentita dall'art. 6.2 della direttiva 97/66/CE e dall'art. 4, comma 2 del nostro d.lgs. 171/98 ai soli fini di fatturazione. Onde evitare, quindi, che i dati vengano immediatamente cancellati o resi anonimi, ai sensi del primo comma delle norme citate, con effetti deleteri per le indagini sui crimini informatici, si è proposto di imporre ai *providers* un obbligo di conservazione.

Contro tale impostazione si è espresso, invece, il Gruppo di lavoro dei Garanti europei, i quali hanno sottolineato la contrarietà della conservazione indiscriminata dei dati relativi al traffico ai diritti fondamentali di cui all'art. 8 della Convenzione europea dei diritti dell'uomo ed alla Convenzione del Consiglio d'Europa sul trattamento automatizzato dei dati a carattere personale (Convenzione n. 108 del 1981), oltre che agli artt. 8 e 7 della Carta dei diritti fondamentali dell'Unione Europea[36].

Pur concludendo, dunque, per l'inesistenza di un obbligo attualmente in vigore che possa legittimare la raccolta e la conservazione dei *files* di *log* da parte dei fornitori di accesso e, con le specificazioni sopra evidenziate, dei fornitori di contenuti Internet senza lo specifico ed espresso consenso, rispettivamente, dei clienti e dei visitatori dei siti[37] si deve notare come alcune prospettive della disciplina della materia sembrano preannunciare contrasti con i principi di finalità e proporzionalità al cui rispetto la normativa in vigore subordina la liceità del trattamento di dati personali, nonché problemi di coordinamento con le disposizioni comunitarie in tema di obblighi generali di sorveglianza in capo ai *providers* (cfr. art. 15 direttiva CE 2000/31).

Le registrazioni *de quibus* dovranno essere, pertanto, salvo il consenso dell'interessato, immediatamente cancellate ovvero rese anonime ai sensi dell'art. 4, comma 1, d.lgs. 171/1998.

Per quanto riguarda il fornitore di accesso alla Rete vi è però l'eccezione, poc'anzi rilevata, prevista dall'art. 4, comma 2, d.lgs. 171/1998, il quale consente di trattare i dati personali relativi al traffico ai soli fini di fatturazione, per tutto il tempo per cui può essere contestata la fattura o preteso il pagamento.

Solo per questo specifico fine, dunque, il fornitore di accesso ad Internet può legittimamente conservare i dati desunti dalle registrazioni delle connessioni effettuate dai propri clienti, senza l'obbligo di procurarsi alcun consenso. Va ricordato, però, che nel caso in cui non gravi sul fornitore alcun obbligo di fatturazione, in ragione della « gratuità » del servizio ad

[36] Tale posizione è stata assunta dal Gruppo di lavoro dei Garanti europei sin dalla Raccomandazione 3/99 dal titolo « *La conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari* » del 7 settembre 1999, ed è stata poi ribadita nel marzo 2001 in relazione al progetto di Convenzione sulla lotta al *cyber-crime* (sul punto cfr. la *newsletter* del Garante del 16 aprile 2001) e nel maggio 2001 durante la « Conferenza di primavera » tenutasi ad Atene (per un resoconto della quale cfr. la newsletter del Garante 14 maggio 2001). Si segnalano, inoltre, gli interventi del Presidente dei Garanti europei Stefano Rodotà del giugno (cfr. la *newsletter* del Garante del 11 giugno 2001) e del luglio 2001 (cfr. *newsletter* n. 89 del Garante del 2-8 luglio 2001).

[37] Cfr. la decisione del Garante per la protezione dei dati personali del 13 gennaio 2001 »*Consenso consapevole e libero per il trattamento dati per l'erogazione del servizio Internet gratuito Libero di Infostrada s.p.a.* », consultabile sul sito dell'Autorità garante http://www.garanteprivacy.it.

esempio, come avviene nella quasi totalità dei contratti di accesso ad Internet oggi proposti, il secondo comma dell'art. 4 citato non è applicabile e vige la regola generale di cui al comma 1: « *I dati personali relativi al traffico …sono cancellati o resi anonimi al termine della chiamata* ».

Tuttavia, il discorso non può ritenersi concluso prima di aver trattato la questione dell'applicabilità a Internet del d.lgs. 171/1998 ed in particolare del suo art. 4.

Il decreto, infatti, è stato predisposto e tarato per il settore delle telecomunicazioni, così come la stessa lettera dell'art. 4 citato — che utilizza la locuzione « chiamata » — evidenzia.

L'interpretazione restrittiva di tale termine potrebbe portare a sostenere l'applicabilità della norma alle sole connessioni a commutazione di circuito (ossia alla telefonia vocale tradizionale), escludendo così dal campo di applicazione le connessioni a commutazione di pacchetto (sistema di trasmissione dei dati adottato dall'Internet)[38].

Invero, vi sono fondate ragioni per sostenere che la terminologia utilizzata dal legislatore comunitario prima (direttiva 97/66/CE) e dal legislatore italiano poi (d.lgs. 171/98), non possa valere a ridurre l'ambito di applicazione della disciplina.

Un primo valido ausilio interpretativo è costituito dall'opinione più volte espressa dal Gruppo di lavoro dei Garanti europei[39], secondo la quale il trattamento dei dati personali su Internet deve essere considerato alla luce di entrambe le direttive, quella generale (95/46/CE) e quella speciale (97/66/CE), dovendosi ricomprendere Internet tra le vari forme di comunicazione cui si applica il quadro giuridico delle telecomunicazioni. Inoltre, anche con riferimento all'ordinamento nazionale, si può notare come vi sono altri casi nei quali il riferimento ai « servizi di telecomunicazioni » non esclude l'applicabilità della disciplina ai fornitori di accesso alla rete Internet[40]. Infine, argomentando *a contrario*, se si accogliesse l'interpretazione restrittiva dei termini « servizi di telecomunicazioni » e « chiamata » di cui alla direttiva 97/66/CE e al d.lgs. 171/98, l'art. 4 del d.lgs. ultimo citato proteggerebbe i dati sul traffico generati dalle chiamate telefoniche, ma non quelli generati dalle connessioni alla rete Internet, creando una disparità di tutela nei confronti di dati personali del tutto analoghi.

In ogni caso, un dubbio interpretativo quale quello richiamato, soprattutto nella materia che ci occupa già così povera di certezze normative, rischia di essere pericoloso. Ecco perché la proposta di direttiva del Parla-

---

[38] Cfr. la descrizione dei sistemi a commutazione di pacchetto e a commutazione di circuito contenuta nella nota 4.

[39] Tra gli altri si vedano il documento di lavoro *Trattamento dei dati personali su Internet*, del 23 febbraio 1999, il Parere 2/2000, presentato dall'Internet Task Force il 3 febbraio 2000 e il Parere 7/2000, del 2 novembre 2000, tutti consultabili all'URL http://www.garanteprivacy.it.

[40] Si pensi, in ambito nazionale, alla disciplina dettata dall'art. 6, comma 1, D.P.R. 19 settembre 1997, n. 318, che subordina « *l'offerta al pubblico di servizi di telecomunicazioni diversi dalla telefonia vocale, dall'installazione e dalla fornitura di reti pubbliche di telecomunicazioni, comprese quelle basate sull'impiego di radiofrequenza* » ad autorizzazione generale, quale disciplina sulla base della quale si ritiene che gli *Internet access providers* siano tenuti, per svolgere la propria attività, a presentare una dichiarazione preventiva all'Autorità per le garanzie nelle comunicazioni, ai sensi dell'art 3, della delibera 467/00/CONS dell'Autorità stessa.

mento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [COM(2000)385], sostituisce l'espressione « inoltrare chiamate » contenuta nell'art. 6, n. 1 della direttiva 97/66/CE, con quella tecnologicamente neutrale « trasmettere una comunicazione »[41], eliminando così ogni dubbio sull'estensione della protezione dei dati personali relativi al traffico che discende dall'attuale formulazione dell'art. 6, appena richiamato e, nel nostro ordinamento, dell'art. 4, d.lgs. 171/1998.

Affermata l'applicabilità di tale ultima disposizione anche ai trattamenti di dati relativi al traffico Internet, non sembra sussistano altre questioni controverse tali da impedire di affermare che il fornitore di accesso alla rete Internet, il quale conceda gratuitamente la connessione ovvero applichi una tariffazione forfetaria, possa effettuare il trattamento dei dati relativi al traffico solo previo benestare del cliente.

Infine, un'ultima notazione è necessaria in relazione al fatto che il meccanismo dei *logs*, consistendo in una registrazione automatica di alcune informazioni relative alla connessione, potrebbe comportare la registrazione di dati personali sensibili ai sensi dell'art 22, l. 675/96, tutte le volte che la navigazione dell'utente sia relativa a siti web di argomento politico, religioso, sessuale, ecc. In questi casi — ma su ciò non vale soffermarsi oltre, essendo logica conseguenza degli esiti del discorso appena svolto — il fornitore di accesso alla Rete potrà effettuare il trattamento solo rispettando la disciplina prevista all'art. 22, l. 675/1996.

3.3. *I cookies*.

Passando all'analisi della seconda tecnica oggetto della presente indagine, va subito detto che il termine (letteralmente traducibile con « biscottino ») non dà ragione della potenzialità di tali piccoli file. Essi vengono inviati dal *server* del sito web visitato al *browser* (programma dedicato alla navigazione in Internet) istallato sull'*host computer* utilizzato per la connessione, al fine di memorizzare sull'*hard disk* di tale *computer* informazioni utili ad una più veloce navigazione in caso di successive visite allo stesso sito[42]. In realtà è questa la finalità tecnica, alla quale però si af-

[41] Nella proposta di direttiva [COM(2000)385] si sottolinea come la normazione nell'ambito dei servizi di comunicazione elettronica debba passare per regole neutrali rispetto alla tecnologia, sì da garantire ai consumatori ed utenti un livello di tutela indipendente dalla tecnologia con la quale viene fornito un determinato servizio.

[42] Il meccanismo di funzionamento dei *cookies* si basa su un software comunemente utilizzato nel Web mediante il quale si acquisiscono informazioni quali *username*, *password* e preferenze dell'utente desunte dalle pagine visitate, sì da rendere più facile la navigazione. In pratica ad ogni collegamento da parte dell'internauta, unitamente alla copia della pagina web richiesta mediante la connessione, il server web invia al browser dell'utente (*rectius* dell'host computer utilizzato per la connessione) una richiesta di informazioni che viene da questo conservata su un file chiamato « *cookie.txt* » il quale, terminato il collegamento al server da cui il *cookie* è stato inviato, viene salvato sul disco rigido dell'host computer dell'utente. Tale file renderà l'host computer nel quale è memorizzato riconoscibile nei successivi accessi tramite il medesimo server. Per una approfondita descrizione del funzionamento dei *cookies* cfr. la decisione della *District*

fianca spesso una utilizzazione di tali applicazioni a fini direttamente ed indirettamente commerciali. Infatti, i *cookies*, oltre che rendere veloce la connessione e la consultazione dei siti memorizzati sul server web dal quale sono stati inviati sul computer dell'utente, rendendo questo immediatamente riconoscibile, forniscono al gestore del sito visitato informazioni utili all'invio di pubblicità personalizzata ovvero funzionali all'offerta di specifici prodotti di cui si è verificata la preferenza dell'utente nelle precedenti connessioni.

In altre parole, i *cookies* fungono da raccoglitori di informazioni quali durata della connessione, *username*, *password*, pagine visitate e finanche contenuto dell'*hard disk* del computer del navigatore. Tali informazioni, analizzate alla luce della frequenza con la quale si ripetono, costituiscono dati utili ad uno sfruttamento commerciale.

Anche in questo caso si deve precisare che la raccolta di dati così attuata non è relativa ad un utente identificato o identificabile (a meno che a porla in essere non sia lo stesso fornitore di accesso — *Internet access provider* — che svolga anche attività di *content provider*)[43] ma è relativa ad una macchina identificata da un I.P. *number*, ossia fornisce informazioni relativamente ai collegamenti attuati mediante l'*host computer* a cui i *cookies* vengono inviati e nel cui *hard disk* vengono memorizzati.

Alla luce di ciò, sulla base di una interpretazione letterale del concetto di identificabilità del titolare dei dati[44], si dovrebbe concludere che, in questo caso, non si pongono problemi di lesione della riservatezza (l'identità anagrafica dell'utente potrebbero non essere mai conosciuti dal gestore del sito visitato).

Tuttavia, quella del funzionamento tecnico, come già rilevato, è una prospettiva troppo limitata per una completa indagine sui meccanismi di raccolta occulta dei dati in Rete.

Così come nel caso dei *files di log* registrati dal c*ontent provider*, i quali, come detto, acquisiscono una connotazione potenzialmente lesiva della privacy degli utenti solo qualora vengano integrati e confrontati con gli analoghi files registrati dai fornitori dell'accesso alla rete, anche nel caso dei *cookies*, la privacy può essere influenzata a seguito della convergenza tra le tecnologie Internet applicate alla raccolta dei dati e le dinamiche economiche degli stessi.

Court of New York, *DobleClick Inc. Privacy*, del 28 marzo 2001, nella quale è contenuta una meticolosa descrizione tecnica dei meccanismi di funzionamento dei *cookies* utilizzati dalla *DobleClick Inc.*. La sentenza (consultabile *on line* all'URL http://www.internetlex.kataweb.it), pur ricostruendo le modalità con le quali *DobleClick* utilizzava il meccanismo dei *cookies* per raccogliere informazioni sugli utenti di migliaia di siti ad essa affiliati per finalità di *direct marketing*, finisce per affermare la conformità dei *cookies* alle disposizioni *dell'Electronic Comunications Privacy Act*. Si ricorda, comunque, che i cookies possono essere cancellati dalla memoria del computer e che per ragioni di sicurezza sono stati stabiliti limiti alle dimensioni dei *cookies* (4 Kb), alla capacità di conservazione di *cookies* da parte dei *browser* (non più di 300) ed al numero di *cookies* utilizzabili da ciascun server web.

[43] Cfr. nota 27.

[44] Interpretazione che non è condivisa dal gruppo dei Garanti europei, i quali, nella raccomandazione del 17 maggio 2001 indirizzata al Consiglio d'Europa, alla Commissione, al Parlamento europeo e agli Stati membri, nel fissare i requisiti minimi per la raccolta dei dati personali *on line*, prevedono che tra le informazioni che debbono essere fornite a chiunque si colleghi ad un sito web che attui la raccolta di dati personali, vi debbano essere anche quelle relative all'utilizzo di procedure automatizzate per la raccolta dei dati quali i *cookies*.

Ed, infatti, le informazioni assunte da un *server web* mediante il meccanismo dei *cookies*, seppure di per sé non qualificabili come dati personali ai sensi dell'art. 1, comma 2, let. *c*), l. 675/96, lo diventano qualora vengano integrate con altre informazioni acquisite *on-line* ovvero *off-line*, idonee ad identificare i soggetti titolari dei dati tramite quel meccanismo raccolti.

Si pensi, per esempio, e non è certamente un caso limite, ai dati ceduti volontariamente dallo stesso utente al gestore di un sito tramite la sottoscrizione di un *guestbook* o di un formulario elettronico[45]. Certamente, l'integrazione tra questi dati e le informazioni relative al medesimo navigatore fornite dal *cookie* (inviato nell'*hard disk* dell'utente) genera dati personali riferiti ad un individuo identificato.

Si pone, in questo caso, il problema di stabilire in quale momento del processo il trattamento dei dati faccia sorgere in capo al gestore del sito gli obblighi di cui alla l. 675/96. Posto, infatti, che i dati acquisiti per effetto del meccanismo dei *cookies*, almeno alla luce di una interpretazione letterale dell'art. 1, comma 2, let. *c*), l. 675/96, non possono qualificarsi dati personali in quanto non riconducibili ad un utente identificato, non può sostenersi che gli obblighi di informativa di cui all'art. 10 e di richiesta di consenso di cui all'art. 11, sorgano al momento della connessione da parte dell'utente[46]. In tale frangente, seppure il meccanismo dei *cookies* è operante, esso genera dati riconducibili ad un anonimo *username* lasciando ancora illesa la sfera personale del soggetto che si cela dietro quel nome-utente.

Momento certamente rilevante è, invece, quello in cui l'utente fornisce i propri dati anagrafici al gestore del sito, per esempio compilando un *guestbook* o un formulario per accedere ad un servizio. Bene, in questo caso, il fatto che i dati vengano ceduti volontariamente per ottenere un servizio — fattispecie astrattamente riconducibile all'art. 12, let. *b*), l. 675/96 — risulta irrilevante ai fini dell'adempimento degli obblighi di cui agli artt. 10 e, soprattutto, 11 della l. 675.

Infatti, qualora vengano utilizzati cookies, le informazioni cedute volontariamente dall'utente nella compilazione di un formulario, quali nome, indirizzo, e quant'altro valga ad identificarlo, assumono ben diverso valore rispetto a quello di meri dati identificativi di una parte del rapporto contrattuale. Fornendo quei semplici dati anagrafici l'utente, infatti, si svela al gestore del sito (che utilizzi i *cookies*) rendendo conoscibile a quest'ultimo ben più che il proprio nome e indirizzo.

Si può, pertanto, senz'altro sostenere che il gestore di un sito che utilizzi i *cookies*, all'atto della raccolte di informazioni anagrafiche del visitatore, oltre che adempiere agli obblighi connessi al trattamento di queste, debba fornire un'informativa che indichi chiaramente l'uso di tali pratiche per l'acquisizione dei dati, e debba richiedere il consenso specifico dell'utente anche in relazione a tale trattamento, segnalandone il carattere facoltativo.

---

[45] Si pensi anche alla possibilità che il gestore del sito stabilisca accordi con uno o più *access provider*, al fine di ricondurre ad un utente identificato le informazioni di cui è venuto in possesso per effetto dell'azione dei *cookies*.

[46] Sembra essere questa, invece, la conclusione espressa dai Garanti europei nella raccomandazione di cui alla nota 44.

È il caso, inoltre, di sottolineare come, a differenza dei *logs*, i quali comportano un trattamento di dati personali che potremmo definire non « invasivo », consistendo in una registrazione automatica di alcune informazioni personali sul server dell'*access provider*, i *cookies*, memorizzandosi sull'*hard disk* dell'*host computer* utilizzato dall'utente, hanno una valenza lesiva della sfera privata che prescinde dalla considerazione sopra riportate. Da ragione di ciò il fatto che le tipologie più sofisticate possono arrivare a svelare il contenuto dell'*hard disk* del computer dell'utente captando, nell'inconsapevolezza di quest'ultimo, informazioni di intuibile rilevanza commerciale.

Si pensi, ad esempio, alla lesione della sfera privata dell'utente Internet connessa alle già citate « cimici web » le quali si istallano sull'*hard disk* dell'*host computer* senza la possibilità di poter essere individuate e, dunque, eliminate. Viene qui in evidenza, accanto all'esigenza di tutela dei dati personali, la tutela del domicilio informatico il quale, ai sensi dell'art. 615-*ter*, comma 1, c.p., viene violato da chiunque si introduca in un sistema informatico o telematico, o vi si mantenga contro la volontà esplicita di chi ha il diritto di escluderlo. Sotto questo profilo mi pare che si possa pensare, in relazione ai cookies, ad un trattamento ancor più rigoroso di quello proposto in queste pagine.

4. Considerazioni conclusive.

L'analisi svolta ha dimostrato che l'indagine circa l'incidenza sulla riservatezza dell'internauta di *log* e *cookies* deve tenere in conto sia il dato tecnico, sia il valore economico oggi assunto dal dato personale. Solo vagliando l'uno e l'altro aspetto si riesce, infatti, a discriminare le fattispecie e, nell'ambito di esse, le specifiche situazioni alle quali sono applicabili i precetti della l. 675/96 dai trattamenti di dati che ne restano esclusi.

Si pensi, ad esempio, al caso dei dati relativi al traffico acquisiti dal *content provider*, i quali, facendo riferimento al solo dato tecnico, dovrebbero essere a rigore esclusi dall'ambito di applicazione della legge 675.

In vero, le dinamiche economiche che coinvolgono i dati personali determinano spesso l'incrocio di quei dati con quelli di analoga derivazione dell'access *provider* sulla base di accordi commerciali duraturi.

La prassi dei contratti di accesso ad Internet evidenzia l'offerta congiunta del servizio di connessione alla Rete e di ulteriori servizi informativi e commerciali da parte di un portale web[47]. In tutti questi casi, ovvero nei casi in cui l'*access provider* scambia informazioni sugli utenti con una serie di siti rappresentativi delle principali categorie merceologiche, la questione posta cessa di essere un'ipotesi di scuola per divenire una prassi concretamente lesiva della privacy, qualora non attuata conformemente alle disposizioni della l. 31.12.1996, n. 675[48].

---

[47] Si tratta di un sito con il quale si forniscono al navigatore una serie di servizi utili: informativi, commerciali, ludici. Lo scopo di un portale web è quello di indurre il navigatore a sceglierlo come sito iniziale di tutte le navigazioni, sì da aumentare il numero degli accessi e, di conseguenza, la raccolta pubblicitaria.

[48] A sostegno di quanto affermato si riporta di seguito una parte (modalità del

In definitiva, mi pare di poter concludere che il trattamento di dati relativi al traffico, sia esso il frutto di meccanismi automatici di raccolta e conservazione dei dati (*log*), ovvero dell'azione di *file* inviati appositamente nel computer dell'utente (*cookies*), pur non costituendo di per sé, ed in ogni caso, un trattamento di dati personali, sia soggetto, nella pratica, alle disposizioni della direttiva 95/46/CE ed a quelle più specifiche della direttiva 97/66/CE — e, dunque, alle discipline nazionali di recepimento — per effetto delle dinamiche economiche della Rete.

Così, avverrà che, quando il funzionamento tecnico con cui avviene tale trattamento evidenzia la non identificabilità del titolare dei dati raccolti, come abbiamo visto accadere nel caso dei *cookies* e dei dati registrati nei *data-log* del *content provider*, gli obblighi previsti nella normativa europea e nazionale sorgeranno in capo al titolare del trattamento solo nel momento in cui le dinamiche economiche dei dati generano integrazioni, raffronti e scambi di informazioni tali da rendere quei dati, prima anonimi, associabili ad un soggetto identificato o identificabile[49].

trattamento) dell'informativa di uno dei maggiori *providers* italiani: *« (Il provider) adotterà un sistema di analisi degli accessi limitatamente ad una lista predefinita di siti che meglio rappresentano gli interessi del Cliente da un punto di vista strettamente ed esclusivamente commerciale. La lista si compone dei siti più rappresentativi sotto il profilo commerciale. Tali siti saranno scelti tra i più popolari e stabili per ogni categoria merceologica »*.

[49] Nelle more della pubblicazione del presente scritto la Convenzione del Consiglio d'Europa sul cyber-crime è stata approvata e dal 23 novembre 2001 è aperta alla firma. Nello stesso periodo, la proposta di direttiva [COM(2000)385] sulla privacy nelle comunicazioni elettroniche ha proseguito il suo travagliato *iter*, da una parte, oscillando tra *opt-in e opt-out system* e, dall'altra, ampliando il dibattito ai *cookies*. Al momento in cui vengono licenziate le bozze di questo scritto, le scelte adottate dal Parlamento europeo nella seduta del 13 novembre 2001 sulla sollecitazione commerciale via e-mail e sull'utilizzo dei *cookies*, ossia nel primo caso l'*opt-out system* e nel secondo l'*opt-in system*, sono state entrambe bocciate dal Consiglio del Ministri delle Telecomunicazioni dell'Unione europea nella seduta del 6 dicembre 2001. Intanto, sul fronte interno, il Consiglio dei Ministri n. 31 del 21 dicembre 2001 ha approvato il d.lgs. (non ancora pubblicato sulla G.U.) recante disposizioni correttive e integrative in materia di dati personali, a norma dell'art. 1 della l. 127/2001, in esecuzione della delega della l. 676/1996. Il tema, pertanto, stimola nuove riflessioni e propositi di sviluppo del discorso sin qui svolto.