La nuova legge sulla privacy

PROTEZIONE DEI DATI PERSONALI E PROBLEMI DI INTERNET

La tanto attesa legge sulla protezione dei dati personali è una realtà, o lo sarà tra poco tempo. Le norme specifiche per gli operatori telematici arriveranno con il previsto decreto legislativo, ma è già possibile tracciare un quadro d'insieme degli adempimenti che saranno necessari e dei problemi che dovranno essere risolti.

di Manlio Cammarata

10 dicembre 1996: secondo fonti ben informate, la Camera dei Deputati si appresta ad approvare definitivamente, senza modifiche, il disegno di legge governativo «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali» licenziato dal Senato il 20 novembre. Secondo altre fonti, la Camera dovrebbe correggere alcuni punti dell'articolato e quindi rispedire il testo a Palazzo Madama per l'approvazione definitiva. Comunque vada, è ragionevole pensare che la tanto attesa disciplina sulla *privacy* sia in dirittura d'arrivo.

I tempi di preparazione di una rivista mensile come MCmicrocomputer non consentono di dare un'informazione sempre aggiornata, ed è possibile che questo articolo sia in qualche punto superato quando il numero sarà in edicola. Ma le linee generali del provvedimento sono ormai acquisite e non dovrebbero esserci sorprese; eventuali aggiornamenti saranno tempestivamente pubblicati nelle «Attualità» del Forum multimediale «La società dell'informazione», alla URL ***<http://www.mclink.it/inforum/attual.htm>.***

I punti fondamentali della legge sono arcinoti e riproducono il disegno tracciato dall'Unione Europea (ne abbiamo parlato in queste pagine molte volte, e in particolare nei numeri 147 e 148 - gennaio e febbraio 1995). Dopo anni e anni di discussioni i principi generali sono ormai accettati: viene istituita una figura di «Garante», al cui ufficio dovranno essere comunicate tutte le operazioni di raccolta ed elaborazione di dati personali, da chiunque effettuate. Dovranno essere seguite regole molto rigide per la raccolta, la conservazione, l'elaborazione, la comunicazione a terzi e la diffusione delle informazioni, con particolare attenzione ai cosiddetti «dati sensibili», che sono quelli relativi alla salute, alle abitudini sessuali, alle idee politiche e religiose e così via (il testo della legge è in Net_Lex, alla URL **<http://www.mclink.it/inforum/netlex/netlex.htm>).**

Sono passati due anni da quando l'ennesima elaborazione del testo è stata presentata al Senato, nella passata legislatura, due anni di dibattiti e di critiche, che però non sono serviti per ottenere miglioramenti sostanziali. La legge rimane inutilmente complicata, anche se alcuni articoli sono stati modificati o spostati, e alcune disposizioni appaiono troppo severe (se ne parla nel riquadro). È stato addotto il motivo, reale, dell'urgenza di varare la legge per far entrare l'Italia nell'accordo di Schengen, per mettere a tacere le voci di dissenso e spingere l'approvazione del testo con poche modifiche, frutto più di pressioni interessate che di un serio tentativo di miglioramento.

Quali «dati» in rete?

Rimandiamo l'analisi dettagliata del testo al momento in cui sarà varata l'intera normativa, che comprende anche un decreto legislativo da emanare dopo la legge principale e che conterrà le disposizioni più importanti dei sistemi telematici. Ma, dal momento che le linee fondamentali della normativa si possono considerare comunque acquisite, cerchiamo di capire quali adempimenti, sostanziali e formali, saranno richiesti a chi gestisce un sistema telematico, in particolare a un ISP (Internet Service Provider). Prima di tutto facciamo una ricognizione delle «banche dati» presenti normalmente nel sistema.

La prima, è più ovvia, è l'**elenco degli abbonati**, che comprende di solito i dati anagrafici e

l'*username* (cioè l'identificativo pubblico assegnato all'utente, che può anche essere uno pseudonimo o un nome di fantasia, il cosiddetto *nickname*). Questo elenco in molti casi è accessibile al pubblico e costituisce quindi una sorta di rubrica telefonica, in alcuni casi è riservato.

Collegato all'elenco degli abbonati è il delicatissimo **archivio delle password**, cioè delle chiavi private che, in combinazione con l'username consentono l'accesso al sistema o a parti di esso. L'archivio delle password dovrebbe essere sempre crittografato con algoritmi *one way* e superprotetto contro le intrusioni (vedremo più avanti le precauzioni che dovrebbero essere rese obbligatorie per la sicurezza minima dei sistemi).

Terzo, importantissimo archivio, è quello dei log, cioè delle registrazioni automatiche dei principali dati dei collegamenti, generate automaticamente dal sistema. È compito del responsabile del sistema stesso decidere quali informazioni debbano essere raccolte e in che modo vadano archiviate e protette. L'utilizzo più comune dei log è per gli addebiti dei collegamenti, quando sono praticate tariffe a tempo o è previsto un tempo massimo giornaliero o mensile; si possono generare log molto dettagliati o ridotti all'essenziale, ma l'importante è che possano essere utilizzati in caso di contestazioni degli abbonati e anche per ricostruire collegamenti sospetti nel caso di tentativi di accesso illecito al sistema o la commissione di altri reati telematici. Dal punto di vista della protezione dei dati personali l'archivio dei log è delicato quanto quello delle password, perché può contenere informazioni molto delicate: i tempi di collegamento di ciascun utente, a quali ore si collega, quali siti visita più di frequente, quali prodotti acquista e via discorrendo. Un log molto dettagliato permette di costruire un profilo dell'abbonato che può essere utilissimo per le promozioni commerciali, ma anche per diffamazioni, ricatti, estorsioni e altre poco nobili attività.

Con questi tre punti si esaurisce la rassegna degli archivi «strutturali» di un sistema telematico, archivi che vanno considerati sotto una serie di aspetti funzionali: la raccolta delle informazioni, la loro conservazione, l'elaborazione, la comunicazione a terzi, la diffusione e il cosiddetto «trasferimento all'estero».

La **raccolta delle informazioni** può avvenire in forma esplicita, come nella compilazione delle schede anagrafiche, o «in background», come nella registrazione dei log. Un caso a parte è costituito dall'archivio delle password, il cui aggiornamento è di fatto nelle mani degli utenti, ma la cui gestione e protezione spetta al gestore del sistema.

La **conservazione delle informazioni** è rilevante soprattutto per la protezione della riservatezza: se l'archivio degli abbonati può essere pubblico, quelli delle password e dei log devono essere difesi dalle intrusioni non autorizzate con tutti i mezzi messi a disposizione dalla tecnologia: collocazione in zone protette del sistema, crittografia, password di accesso e via discorrendo, senza dimenticare la protezione fisica dei locali e del sistema (badge di accesso, serrature affidabili, ecc.).

E siamo all'aspetto dell'**elaborazione dei dati**. Essi sono normalmente elaborati per scopi amministrativi, per la fatturazione dei consumi, per scopi statistici e commerciali, per scopi tecnici o quando si devono analizzare le prestazioni dei sistemi. Un caso a parte è l'elaborazione delle password, sotto l'aspetto della crittografazione e del confronto automatico che autorizza l'accesso: la raccolta, la conservazione e l'elaborazione del dato costituiscono momenti inscindibili di un processo unico, con particolari implicazioni dal punto di vista giuridico.

Infine la **comunicazione e la diffusione**. La prima consiste nella trasmissione delle informazioni a determinati soggetti, la seconda si risolve di fatto nella pubblicazione. E qui incominciano i veri problemi per gli operatori telematici, perché la diffusione dei dati su Internet, come vedremo tra poco, configura anche il trasferimento dei dati all'estero, che la nuova legge regola con norme molto severe.

Esportare verso dove?

Ora dobbiamo considerare due aspetti.

Il primo è che l'informazione in rete comprende per sua natura una quantità enorme di dati personali, che vengono diffusi materialmente dagli Internet provider, ma che sono immessi da una moltitudine di soggetti per finalità connesse all'informazione stessa, anzi, sono spesso connaturati alle informazioni. Pensiamo a un classico sito universitario, con l'elenco delle facoltà, delle materie di insegnamento e dei docenti: ai sensi delle norme sulla protezione dei dati personali si tratta di vere e proprie «banche dati», dalle quali si ricavano le informazioni sull'attività di alcune persone. Si apprende, per esempio, che il professor Tal dei Tali insegna la tale materia in tale facoltà, e questa è un'informazione personale protetta dalla legge. Per fare un esempio più immediato, personalissimo, «sfogliando» MC-link chiunque può sapere che Manlio Cammarata è un giornalista, che collabora alle riviste MCmicrocomputer e MC-link, si occupa di diritto delle tecnologie dell'informazione, è coordinatore del Forum multimediale «La società dell'informazione». Notizie banali, certo, ma si tratta di informazioni la cui raccolta, conservazione, elaborazione, diffusione e trasferimento all'estero sono regolate dalla legge. Aggiungiamo che una semplice elaborazione delle informazioni reperibili nel Forum può portare alla costruzione di un elenco di rapporti interpersonali tra i partecipanti alla discussione, che sono magistrati, avvocati, docenti universitari, funzionari pubblici. In un'indagine penale del tipo di quelle che vengono riportate dalle cronache più recenti, nella quale si indagasse su uno qualsiasi dei partecipanti al Forum, questi rapporti interpersonali potrebbero addirittura far sorgere ipotesi di collusioni in attività illecite...

Il secondo aspetto è ancora più problematico: Internet è, per sua natura, un sistema globale, pri-

vo di confini fisici e politici, che si sovrappone al sistema politico disegnato dal diritto internazionale. Non è facile inquadrare questo concetto dal punto di vista giuridico, perché quando un'informazione viene immessa in Internet non si verifica un passaggio da uno stato a un altro stato, come quando un individuo o un bene attraversano una frontiera, ma si realizza il passaggio di beni immateriali da un territorio fisico e giuridicamente delimitato a uno spazio illimitato e ancora non definito da norme di diritto positivo. È qualcosa che assomiglia alla situazione in cui si trova un natante che supera il limite delle acque territoriali di uno stato e si trova in uno spazio «di nessuno». Ma, mentre ci sono accordi tra gli stati che regolano il passaggio e l'attività nelle acque internazionali, nessuna legge regola il ciberspazio. È necessario che ci si renda conto che la definizione di «ciberspazio» non è soltanto una suggestiva invenzione letteraria, ma corrisponde a una realtà precisa, della quale è urgente definire i contorni giuridici.

Dunque quando un'informazione è pubblicata in un sito di Internet, essa è a disposizione di chiunque in qualunque parte del mondo.

Ora consideriamo il fatto che l'art. 28 della legge sui dati personali afferma che *Il trasferimento anche temporaneo fuori del territorio nazionale, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento deve essere previamente notificato al Garante, qualora sia diretto verso un Paese non appartenente all'Unione europea* (comma 1) e che *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* (comma 3). Prima di tutto si dovrebbe notare l'incongruenza del concetto di «dato» con quello di «trasferimento temporaneo», perché il dato viene trasferito solo se viene comunicato a terzi o diffuso, e questo «trasferimento» è irreversibile. Come faccio a comunicare «temporaneamente» a qualcuno il mio nome o la mia professione? *Voce dal sen fuggita, più richiamar non vale...* Ma se mi reco all'estero per qualche giorno con in tasca la mia agenda e non comunico a nessuno i dati che contiene, e poi torno in Italia, si può parlare di «trasferimento temporaneo di dati»? È contro il più elementare buonsenso! Il fatto è che anche in questo caso si confonde l'informazione con il supporto che la contiene (vedi l'articolo precedente) e si cerca di applicare a un elemento immateriale una norma riferibile solo a qualcosa di fisico.

Ma il punto essenziale è un altro, ed è un paradosso che si basa su due elementi. Primo: la pubblicazione di informazioni personali su Internet configura senza dubbio la strana fattispecie del «trasferimento di dati all'estero»; secondo: non essendoci confini nella diffusione delle informazioni su Internet, e non potendo il gestore del sistema determinare verso quali stati le informazioni vengono trasferite, e per i quali possono transitare, si ricade inevitabilmente nella previsione del terzo comma, cioè il trasferimento o il transito in stati che non assicurano un *livello di tutela delle persone adeguato*. Il che è vietato. Ed ecco il paradosso: se consideriamo che il trasferimento dei dati all'estero è insito nella natura stessa di Internet, dobbiamo concludere che «Internet è vietata»!

Ma, come vedremo tra poco, il problema può essere risolto abbastanza facilmente.

La soluzione è nel contratto

A questo punto è opportuno richiamare un concetto che spesso i tecnici non tengono presente: la legge sui dati personali non «vieta» la raccolta e il trattamento dei dati, ma li sottopone a determinate condizioni, che in sostanza si riducono al consenso dell'interessato e alla notificazione al Garante. Questa deve essere comunque presentata e deve contenere la descrizione di tutti gli archivi, del modo in cui vengono raccolti i dati e delle elaborazioni che vengono svolte. Un elemento non trascurabile riguarda il tempo di conservazione dei dati, che deve essere precisato: per le informazioni anagrafiche si può ipotizzare un certo tempo dopo la fine dell'abbonamento, per esempio un anno, ma per i log la questione è più complessa, perché essi possono rivelarsi importanti anche dopo molti anni, nel caso di indagini penali o cause civili in cui possono essere prodotti come elementi probatori. C'è da sperare che il futuro decreto legislativo chiarisca questo e altri aspetti ancora sfuggenti.

Siccome anche la comunicazione e la diffusione dei dati rientrano nel concetto di «trattamento», la notificazione deve contenere anche le indicazioni su quali dati sono accessibili dalla Rete e in quali forme. In linea di principio si può ritenere che le informazioni anagrafiche degli abbonati possano essere oggetto di diffusione, mentre tutte le altre informazioni vadano tenute strettamente riservate (e qui entrano in gioco le disposizioni sulla sicurezza, che saranno oggetto di altri provvedimenti normativi). Resta il problema dei dati diffusi all'interno delle pagine, che non sono sotto il controllo del provider e per i quali è difficile vedere una soluzione in linea con i principi della legge.

A questo proposito entra però in gioco un altro ordine di considerazioni: se i siti Internet, o una parte di essi, possono o devono rientrare nell'ambito delle disposizioni sulla stampa (vedi Informatica e Società del mese scorso), la diffusione di informazioni nelle pagine Web, nei *newsgroup* e nei BBS potrebbe essere regolata in parte con il codice deontologico previsto dal secondo comma dell'art. 25. Resta comunque il fatto che è urgente rivedere le disposizioni sulla responsabilità del direttore di una pubblicazione per le informazioni che non può materialmente controllare (questo comporta, ancora una volta, l'obbligo o l'onere di indentificare gli abbonati, affinché si possa sempre risalire agli autori di atti illeciti).

Ma il vero cardine della questione è nel consenso che l'interessato deve dare al titolare della banca dati, cioè al gestore del sistema, per la raccolta e il trattamento delle informazioni che lo ri-

guardano. E questo può essere ottenuto in maniera abbastanza semplice, con una attenta predisposizione del contratto di abbonamento. Il gestore deve inserire una serie di clausole che indichino quali dati sono raccolti e conservati e quali sono comunicati o diffusi, e anche quali sono i diritti dell'interessato, elencati dall'art. 13. Si deve tener presente che il consenso dell'interessato alla raccolta dei dati non è richiesto quando essa sia necessaria per l'esecuzione del contratto (art. 12). Non è pensabile che si possa chiedere un abbonamento e opporsi alla registrazione del proprio nome, cognome e indirizzo, ma è comprensibile che qualcuno non voglia che il proprio nome appaia in un elenco consultabile da chiunque. Il consenso espresso anche per il trasferimento dei dati all'estero, anche verso i paesi che non assicurano lo stesso livello di protezione, risolve il problema del «divieto di Internet» posto dal terzo comma dell'art. 28. È necessario però che nel contratto siano descritti in dettaglio i diversi aspetti del trattamento e che le relative clausole siano approvate con una firma separata. Infatti l'art. 10 prescrive che all'interessato siano comunicati tutti gli aspetti del trattamento dei dati, mentre l'art. 11, comma 3, recita: *Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 10.*

Un'ultima annotazione per concludere: l'esame del testo della legge porta anche alla soluzione del problema dell'anonimato, che alcuni vorrebbero libero e totale, e altri vorrebbero escludere del tutto. A norma dell'art. 13 l'interessato può opporsi alla diffusione del suo nome o di altre informazioni, ma l'art. 12 stabilisce che il consenso non è richiesto *a) quando il trattamento riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) è 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 l'adempimento di un obbligo legale.* Dunque il legislatore accoglie implicitamente la formula del cosiddetto «anonimato protetto», per il quale il titolare della banca dati deve essere a conoscenza della vera identità dell'interessato, ma gli può essere impedito di divulgarla. MC

Attenti all'agenda!

No, il possesso dell'agenda personale non va notificato al Garante dei dati. Lo afferma l'art. 3, comma 1: *Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della presente legge, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione.* Meno male! Ma il comma successivo aggiunge: *Al trattamento di cui al comma 1 si applicano in ogni caso le disposizioni in tema di sicurezza dei dati di cui all'articolo 15, nonché le disposizioni di cui agli articoli 18 e 36.* Questo è strano, perché se la legge non si applica al «trattamento effettuato da persone fisiche per fini esclusivamente personali», come si fa ad applicarne singoli articoli? E che cosa dicono questi articoli? Il 15 parla di misure minime di sicurezza da adottare in *via preventiva che sono individuate con regolamento emanato con decreto del Presidente della Repubblica,* mentre il 18 dice: *Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.* E il 36 conclude: *Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni.*

A questo punto qualcuno vorrà sapere che cosa dice l'art. 2050 del codice civile.

Eccolo: *Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento se non prova di avere adottato tutte le misure idonee a evitare il danno.* In termini legali si chiama «inversione dell'onere della prova» e significa che, in determinati casi, non è il danneggiato che deve provare la responsabilità di chi ha causato il danno, ma è quest'ultimo che deve provare di aver adottato tutte le misure idonee a evitarlo. Insomma: se vi allontanate dalla vostra scrivania lasciando l'agenda sul tavolo, invece che chiuderla a chiave nel cassetto, e qualcuno vi legge informazioni compromettenti per qualcun altro, potete essere condannati a due anni di galera e risarcire i danni a un soggetto che non è neanche tenuto a provare la vostra responsabilità. Questo, evidentemente, perché *il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati...*

Questa non è la sola «perla» della legge sui dati personali. C'è, per esempio, l'art. 4, comma 1, che dice: *La presente legge non si applica al trattamento di dati personali effettuato: a) dal Centro elaborazione dati di cui all'articolo 8 della legge 1 aprile 1981, n. 121 [...].* Chi va a vedere la legge n. 121 resta di stucco, perché è quella che istituisce la banca dati delle forze di polizia, uno degli organismi più «chiacchierati» della Repubblica, il primo che ha bisogno di un deciso intervento del Garante! Questo comma capovolge il senso della legge, è il contrario del principio della protezione dei dati personali. Ma poi c'è il secondo comma: *Ai trattamenti di cui al comma 1 si applicano in ogni caso le disposizioni di cui agli articoli 9, 15, 17, 18, 31, 32, commi 6 e 7 e 36, nonché, fatta eccezione per i trattamenti di cui alla lettera b) del comma 1, le disposizioni di cui agli articoli 7 e 34...* Prima si dice che la legge non si applica, poiché si applicano le disposizioni di cui ecc., fatta eccezione per i trattamenti... Insomma, se il principio è che la legge si applica a tutte le banche dati, lo si scriva. E poi, se del caso, si elenchino le dovute eccezioni. Invece qui si parte dall'eccezione, che è gravissima in linea di principio, poi si fa l'eccezione dell'eccezione, fatta salva l'eccezione dell'eccezione dell'eccezione!

E pene «islamiche» per chi dimentica l'agenda.