Privacy e furto d'identità

Napoli, 28 maggio 2011

Michele Iaselli

Come è noto il 1° gennaio 2004 è entrato in vigore il Codice per la protezione dei dati personali che ha notevolmente irrobustito il sistema della protezione dei dati personali, ormai solidamente collocata nel quadro dei diritti fondamentali.

Difatti viene riconosciuto nel nostro ordinamento l’autonomo diritto alla protezione dei dati personali in armonia con quanto già previsto nella Carta dei diritti fondamentali dell’Unione europea e nel progetto di Costituzione europea.

In tale quadro fortemente garantista non poche sono le difficoltà applicative di tale normativa nel campo della tutela dei diritti, delle misure di sicurezza, dei trattamenti in ambito pubblico, delle innovazioni tecnologiche e specialmente in campo giudiziario, sanitario e professionale.

Ma cosa si intende per privacy?

La privacy è un termine inglese traducibile all'incirca con riservatezza, è il diritto alla riservatezza delle informazioni personali e della propria vita privata: *the right to be let alone* (lett. "il diritto di essere lasciati in pace"), secondo la formulazione del giurista statunitense Louis Brandeis che fu probabilmente il primo al mondo a formulare una legge sulla riservatezza.

In realtà comunemente per privacy si intende il diritto della persona di impedire che le informazioni che la riguardano vengano trattate da altri, a meno che il soggetto non abbia volontariamente prestato il proprio consenso.

Con l’introduzione dei primi strumenti tecnologici gli studiosi si sono posti il problema della necessità o meno di una specifica tutela avuto riguardo al rapporto tra “riservatezza-computer”; l’impiego dell’elaboratore elettronico, infatti, consente di impadronirsi ed archiviare informazioni che riguardano l’individuo, comprese quelle della sua vita privata sottoponendolo, così, ad una nuova forma di dominio, che si potrebbe chiamare “*il potere informatico*".

Il "*right to privacy*" ha quindi acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa: questo ora consiste nel diritto, riconosciuto al cittadino, *di esercitare anche un controllo sull'uso dei propri dati personali inseriti in un archivio elettronico*.

Il diritto alla riservatezza, per effetto della nuova dimensione acquisita, non viene, infatti, più inteso in un senso puramente negativo, come facoltà di ripulsa delle intromissioni di estranei nella vita privata, o di rifiutare il consenso alla diffusione di informazioni sul proprio conto, di rinuncia alla partecipazione nella vita sociale; ma in senso positivo, come affermazione della libertà e dignità della persona, e come potere di limitare il potere informatico, controllandone i mezzi ed i fini di quel potere.

e dal punto di vista normativo?

Da un punto di vista normativo già la Convenzione europea dei diritti dell'uomo, all'art. 8, stabiliva che non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Oltre che negli Accordi di Schengen, il concetto è stato riportato nella Carta dei diritti fondamentali dell'Unione europea all'art. 8, che recita:

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

Per quanto attiene alla legislazione italiana, al di là della normativa fondamentale, i fondamenti costituzionali sono ravvisabili negli art. 14, 15 e 21 Cost., rispettivamente riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero; ma si può fare anche riferimento all'art. 2 Cost., incorporando la riservatezza nei *diritti inviolabili dell'uomo*.

La nuova dimensione della privacy e la nascita del furto d’identità

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Indubbiamente in ragione delle peculiarità del settore e dell'estrema rapidità con cui la tecnologia va evolvendosi, sono opportunamente destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici e di buona condotta previsti da ultimo dal d.lgs. 30 giugno 2003, n. 196.

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero.

Anche sul fronte dell'e-government esistono indubbie difficoltà non solo in Italia ma anche in Europa e in un documento recentemente reso pubblico i Garanti europei hanno analizzato la situazione corrente e le prospettive di sviluppo in tema di e-government, sottolineandone le implicazioni in chiave di protezione dei dati personali e richiamando l'attenzione sui possibili rischi del mancato coordinamento fra governi nazionali e autorità di protezione dati.

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso, quindi, necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale.

Sul punto, in Italia, il Codice per la protezione dei dati personali ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

Naturalmente rimane il rischio che la diffusione dei documenti elettronici come la Carta Nazionale dei Servizi e l'interconnessione di archivi informatici possano comportare una riduzione dei diritti della persona e della riservatezza dei dati personali.

Ciò anche in considerazione del fatto che su questi profili l'Italia non è dotata di una legislazione in tutto idonea a contemperare le esigenze di semplificazione e razionalizzazione dell'attività economica e commerciale con quelle di tutela della persona, anche in attuazione delle prescrizioni e dei principi generali già contenuti nella normativa comunitaria.

Al riguardo, l'Autorità Garante per la tutela dei dati personali, nell'esercizio della funzione consultiva di cui è titolare, ha più volte segnalato, negli anni precedenti, la necessità di individuare con maggiore attenzione e proporzionalità la tipologia dei dati da inserire nei documenti elettronici, i soggetti che possono eventualmente accedere alle varie categorie di dati e le garanzie per gli interessati.

Oggi le potenziali aggressioni del diritto all'identità personale non provengono esclusivamente da atti, fisici o immateriali, che comportano un'invasione della propria sfera privata. L'evoluzione tecnologica, infatti, se da un lato ha reso sempre più semplici ed accessibili i meccanismi attraverso i quali la pretesa di solitudine dell'individuo tende ad essere compressa, dall'altro ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate che consentono di risolvere o quanto meno di attenuare in radice questo fenomeno. Cosicché diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto.

Difatti, nell'attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. *persona elettronica* attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

Tale situazione si è maggiormente complicata con lo sviluppo della Rete ed in particolar modo con l'avvento del web 2.0 inteso come evoluzione della rete e dei siti internet, caratterizzati da una maggiore interattività che pone l'utente al centro della rete.

Difatti Internet non è più una semplice "rete di reti", né un agglomerato di siti Web isolati e indipendenti tra loro, bensì la “summa” delle capacità tecnologiche raggiunte dall’uomo nell’ambito della diffusione dell’informazione e della condivisione del sapere.

I contenuti creati dagli utenti e resi pubblici attraverso il mezzo telematico, costituiscono un potenziale veicolo di violazioni degli interessi di terzi e in questo senso una minaccia per diritti quali l'immagine, l'onore e la reputazione, nonché la riservatezza. Come messo in risalto da alcuni interpreti, la rete, che per sua natura tende a connettere individui, formazioni sociali e istituzioni di ogni genere, pone questioni "inquietanti" in quanto risolvibili solo con nuovi approcci, soluzioni mai adottate prima e in taluni casi non ancora individuate.

In considerazione delle caratteristiche di accesso di particolari strumenti del web 2.0 (social network, second life, ecc.) legati alle tradizionali credenziali di autenticazione (user id e password) assume particolare rilevanza la problematica della clonazione dei profili: attraverso semplici procedure, peraltro illustrate in rete, è possibile accedere al profilo di un determinato utente e agire per conto di questo, lasciando messaggi e commenti contenenti pubblicità.

Le ipotesi di reato collegate a simili forme di abuso possono essere le più varie ma si riconducono tutte senz'altro al furto di identità che negli ultimi tempi sta preoccupando particolarmente l'Autorità per la protezione dei dati personali.

Altra tipica rappresentazione del furto d’identità è il phishing che è un tipo di frode ideato proprio allo scopo di rubare l'identità di un utente. Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa.

In concreto il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti Web noti o fidati come il sito della propria banca o della società di emissione della carta di credito.

I messaggi di posta elettronica e i siti Web in cui l'utente viene spesso indirizzato per loro tramite sembrano sufficientemente ufficiali da trarre in inganno molte persone sulla loro autenticità. Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali.

Per far sembrare tali messaggi di posta elettronica ancora più veritieri, un esperto di contraffazione potrebbe inserirvi un collegamento che apparentemente consente di accedere ad un sito Web autentico, ma che di fatto conduce ad un sito contraffatto o persino una finestra a comparsa dall'aspetto identico al rispettivo sito ufficiale.

Queste imitazioni sono spesso chiamate siti Web "spoofed".

Una volta all'interno di uno di questi siti falsificati, è possibile immettere involontariamente informazioni ancora più personali che verranno poi trasmesse direttamente all'autore del sito che le utilizzerà per acquistare prodotti, richiedere una nuova carta di credito o sottrarre l'identità dell'utente.

Il Garante sta esaminando questo problema del furto d'identità con viva preoccupazione ponendo la sua attenzione in tutti quei settori particolarmente delicati collegati alle nuove tecnologie come le manipolazioni genetiche e l'utilizzo dei sistemi biometrici nel campo della sicurezza.

Come è noto le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare.

In tema di accessi informatici i sistemi biometrici rappresentano la ricerca più avanzata nel campo della sicurezza. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Di fronte alla rapida ascesa di tali metodologie il Garante sta assumendo un atteggiamento particolarmente rigido in quanto spesso le finalità di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano resa possibile dall'innovazione tecnologica.

Del tutto drammatiche sarebbero poi le conseguenze se il furto d'identità dovesse riguardare materiale che consente di ottenere informazioni genetiche. Se, infatti, grandi sono le opportunità offerte dalla genetica, altrettanto grandi sono i rischi di utilizzazioni dei dati genetici che possono determinare discriminazioni nell'accesso al lavoro o al credito, nella conclusione di contratti di assicurazione vita o malattia, o attraverso forme di schedatura genetica di massa.

Vanno garantiti sempre il rispetto della dignità della persona, il rispetto dell'identità personale, il rispetto dei principi di finalità e di proporzionalità ed infine la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ma ciò che più preoccupa è che il problema della protezione dell'identità dai suoi possibili "furti", già imponente nel settore del commercio elettronico e che esige cautele particolari per le impronte digitali, con il phishing si estende ad altri settori coinvolgendo in particolar modo il mondo bancario, postale ed assicurativo, in breve tutto il settore economico-finanziario.

Ma il phishing come si è detto in precedenza è innanzitutto una vera e propria frode di carattere informatico e si ricorda che l'art. 10 della Legge 547/93 ha inserito nel corpo delle norme penali in tema di truffa la specifica ipotesi di frode informatica.

Lo stesso non si può dire per altre tipologie di furti d'identità in rete che non vengono inquadrate in specifiche figure di reato riconosciute dal nostro ordinamento e solitamente si fanno rientrare nell'ambito del Capo IV del Titolo VII del Codice penale: Dei delitti contro la fede pubblica – falsità personali.

E’ opportuno quindi che il legislatore preveda e punisca con disposizioni specifiche questa odiosa figura di reato senza ricorrere ad interpretazioni estensive di norme penali nate in contesti diversi dove la Rete non era minimamente concepita.

Non bisogna dimenticare che il furto d’identità è comunque possibile a prescindere da Internet e dall’uso di nuove tecnologie. Si pensi ad esempio:

Bin-raiding -. Ogni giorno, dettagli che voi ritenete non essere rilevanti, come vecchie bollette del gas, della luce o del telefono, estratti conto e persino lettere personali e le buste in cui sono contenute, forniscono, in realtà, informazioni preziose che possono essere raccolte semplicemente rovistando nella vostra immondizia.

Cambiamento di indirizzo - I truffatori possono ricevere un’ingente quantità di informazioni sul vostro conto se a seguito di un trasferimento di residenza, ci si dimentica di comunicare la variazione dell’indirizzo alle Poste Italiane, alla Banca e a tutte le altre organizzazioni con cui si è in contatto.

Contatti indesiderati - Fate molta attenzione a chi vi contatta: spesso i truffatori si dichiarano incaricati di una banca e vi chiedono di aggiornare i vostri dati personali. Accade la stessa cosa con coloro che si presentano come ricercatori di mercato e vi richiedono informazioni personali.

Furto o smarrimento del portafoglio - Generalmente i portafogli contengono bancomat, carte di credito e documenti di identità come la patente di guida e le tessere di iscrizione a determinate associazioni.

Skimming – Lo Skimming consiste generalmente nella clonazione di una carta di credito attraverso l'apparecchiatura elettronica utilizzata negli esercizi commerciali per pagare i beni acquistati.
I dati che vengono raccolti, vengono poi trasmessi a organizzazioni criminali.

Rubare l’identità di un deceduto – I malviventi più spietati svolgono le loro attività criminali utilizzando l’identità di persone decedute, ottenendo informazioni sulla loro età, data di nascita ed indirizzo attraverso necrologi e pubblicazioni funebri.

Tramite questionari: spesso ci vengono inviati per posta. Se sono molto lunghi, il compilatore non si accorge che sta fornendo ad estranei delle informazioni private.

Tramite… noi stessi: a volte ci capita, inconsciamente, di raccontare in pubblico fatti che ci riguardano (nell'anticamera del dottore, al supermercato durante la fila alla cassa…), non sapendo che per un ascoltatore interessato possiamo essere una miniera di dati…

GRAZIE!!!

Michele Iaselli

Presidente ANDIP (Associazione Nazionale per la Difesa della Privacy)

www.difesaprivacy.it