Privacy: principi generali e rapporti con le nuove tecnologie

Michele Iaselli

Il nuovo Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003)

Il codice per la protezione dei dati personali è diviso in tre parti:

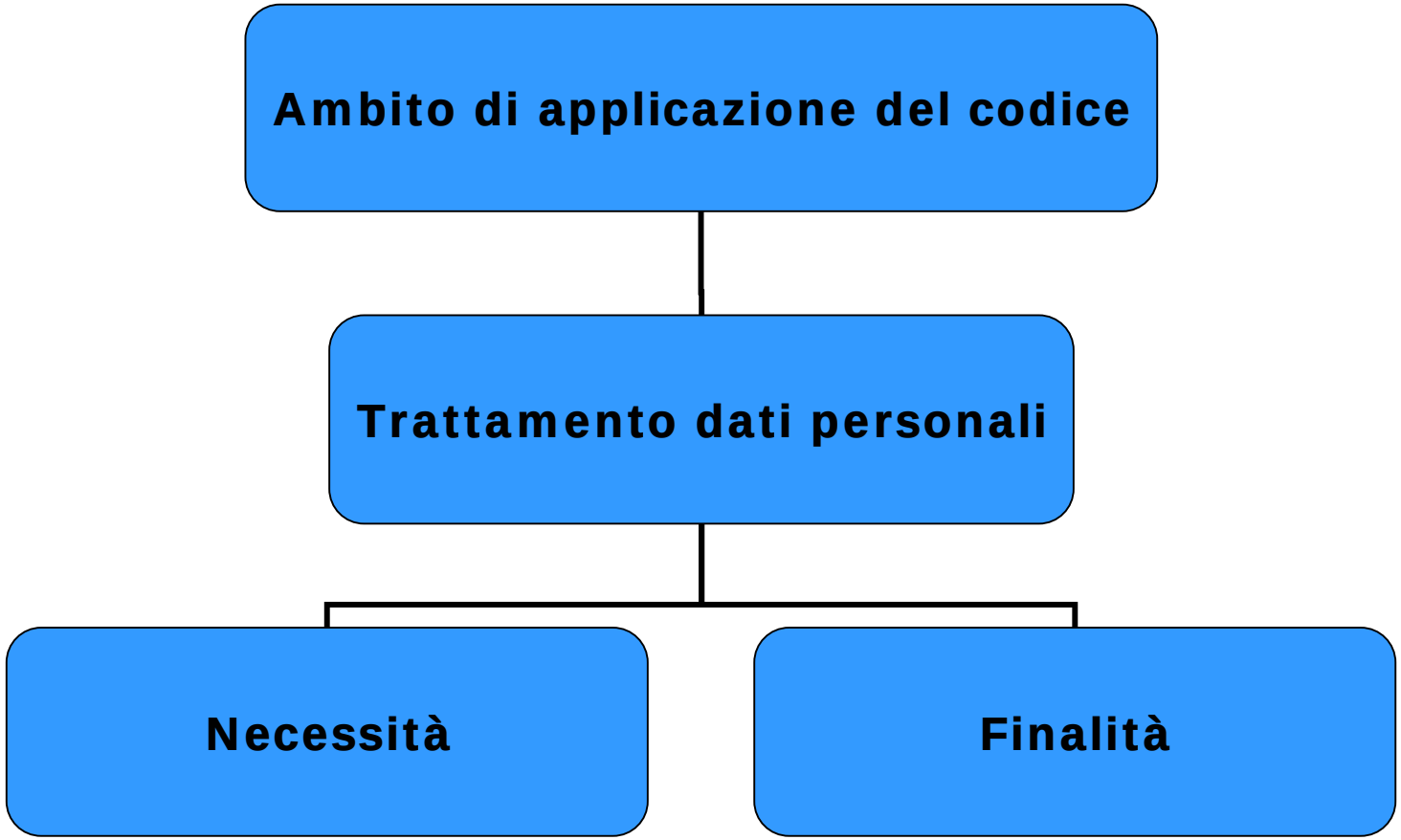
- la prima è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
- la seconda è la parte speciale dedicata a specifici settori: questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori;
- la terza affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

Principi generali in tema di trattamento di dati personali

Il codice si apre con una chiara enunciazione di principio "*Chiunque ha diritto alla protezione dei dati personali che lo riguardano*" la cui portata generale è inequivocabile.

La finalità di tale disposizione appare evidente: i dati personali vanno tutelati sempre indipendentemente dalla loro comunicazione e diffusione, dalla possibilità stessa della lesione del valore sociale dell'individuo. Bisogna, quindi, fare riferimento a qualsiasi attività che abbia per oggetto i dati personali posta in essere nel territorio dello Stato con o senza l'ausilio di mezzi elettronici o automatizzati.

Ma al fine di comprendere tale enunciazione e la reale portata del Codice è necessario innanzitutto fare alcune premesse.


Ambito di applicazione del codice
Trattamento dati personali
Necessità
Finalità

Ambito di applicazione

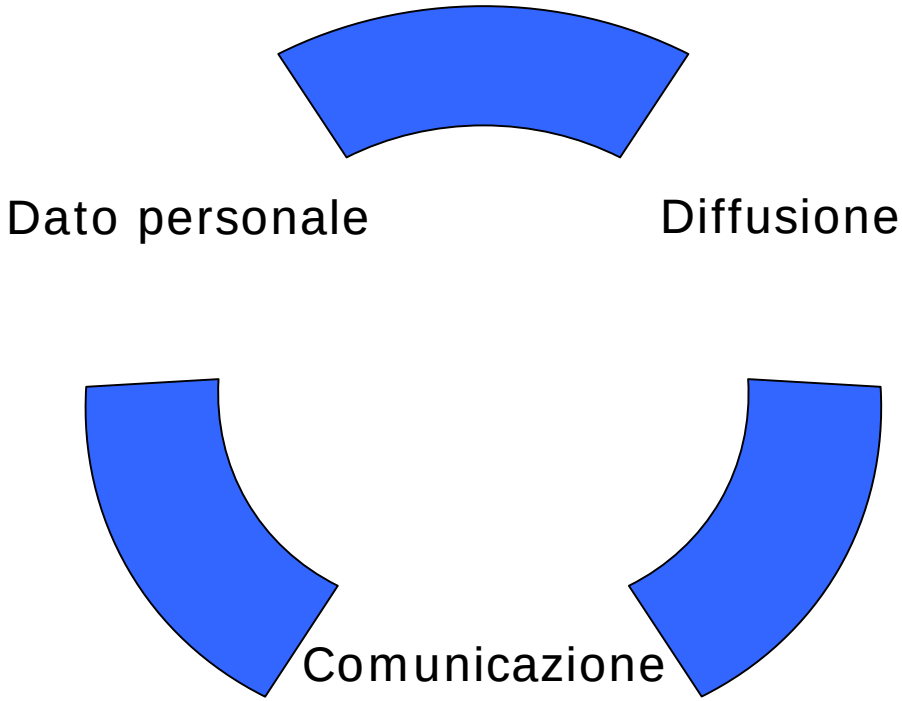
Il legislatore delegato all'art. 5 ha ripristinato quale criterio principale di collegamento della fattispecie alla legge applicabile, **lo stabilimento del territorio dello Stato** o in un luogo sottoposto alla sua sovranità, del soggetto che effettua il trattamento di dati, ancorché gli stessi siano detenuti all'estero.

Nel caso i cui il soggetto che effettua il trattamento sia stabilito in un altro Paese dell'Unione Europea, troverà invece applicazione la legge del Paese di stabilimento.

Trattamento dati personali

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Concetti fondamentali



Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione. Dato personale è, pertanto, un indirizzo, un numero di telefono, un codice di identificazione, una fotografia, un'impronta digitale, una nota valutativa. Insomma un lungo elenco continuamente suscettibile di integrazioni.

Diffusione

Si verifica la diffusione quando le informazioni personali vengono portate a conoscenza, anche attraverso la loro messa a disposizione o consultazione, di soggetti indeterminati.

Comunicazione

Si verifica una comunicazione quando i dati personali vengono portati a conoscenza, anche mediante la loro messa a disposizione o consultazione, di soggetti determinati. Per effettuare una comunicazione deve esserci il consenso dell'interessato (la pubblica amministrazione ha, però, regole particolari).

Principio di necessità nel trattamento dei dati

I sistemi informativi e i software devono essere configurati in modo da minimizzare il ricorso a dati personali e identificativi, sostituendone il trattamento con l'utilizzo di dati anonimi o pseudonimi quando le rispettive finalità non ne risentano, prevedendo l'identificazione dell'interessato solo in caso di necessità.

In altri termini avuto riferimento al trattamento informatico dei dati personali, l'art. 3 del codice sancisce il principio della necessità di identificare l'interessato solo in casi eccezionali laddove non sia possibile perseguire determinate finalità in altri modi meno invasivi.

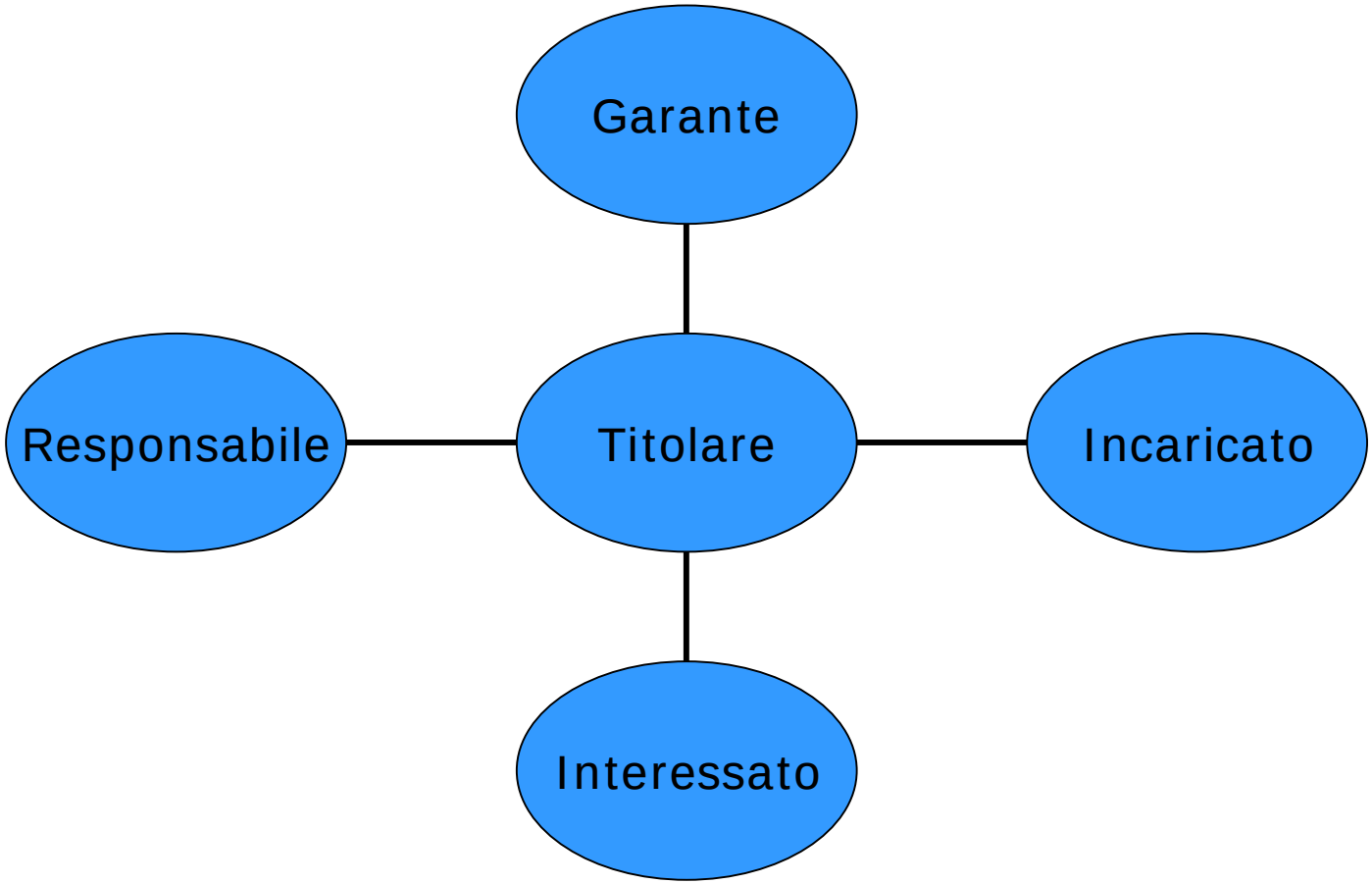
Quest’art. 3 del codice non ha precedenti anche se sin da quando sono stati affrontati i primi problemi di privacy gli studiosi si sono posti il problema della necessità o meno di una specifica tutela avuto riguardo al rapporto tra “riservatezza-computer”; l’impiego dell’elaboratore elettronico, infatti, 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.

Finalità del trattamento dei dati

Il trattamento dei dati personali si deve svolgere nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Figure fondamentali



Garante

Il Garante per la protezione dei dati personali è costituito da quattro componenti, due eletti dalla camera e due dal Senato. L'attuale presidente dell'Autorità è Francesco Pizzetti.

Compito del Garante è vigilare sull'applicazione della legge.

Titolare

E’ il soggetto che esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza. Può essere una persona fisica, una persona giuridica o un ente.

Responsabile

E’ la persona fisica o giuridica che può essere designata da parte del titolare del trattamento. Dovrà sempre essere scelto tra persone che per esperienza o capacità forniscano idonea garanzia sul pieno rispetto delle norme in materia di trattamento dei dati, compreso il profilo della sicurezza.

Incaricato

Chiunque compie operazioni di trattamento. Possono essere individuati come incaricati solo le persone fisiche e non anche le persone giuridiche.

La designazione degli incaricati deve ritenersi valida anche se sussiste la documentata preposizione della persona fisica a una unità per la quale è individuato l'ambito del trattamento consentito agli addetti all'unità medesima.

Interessato

E’ la persona a cui si riferiscono i dati. Non si deve, però, pensare solo alla persona fisica, per quanto nella maggior parte dei casi l’interessato si identifichi con quella. Il concetto, infatti, ricomprende anche la persona giuridica, l’ente o l’associazione a cui si possono riferire dati personali.

Privacy e nuove tecnologie

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.

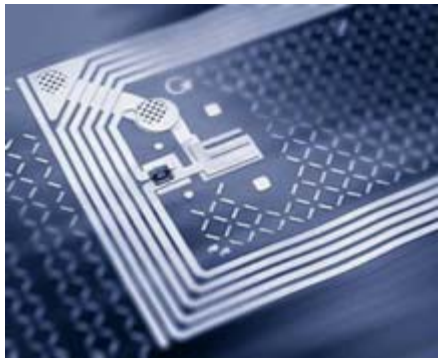
Difatti, nell’attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. *persona elettronica*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

Si deve ricordare innanzitutto che l’obiettivo delle nuove tecnologie è quello di migliorare la qualità della vita dei cittadini nel rispetto della sicurezza e della privacy. Qualsiasi problematica inerente i rapporti tra nuove tecnologie e privacy va sempre risolta inquadrandola nell’ambito di una considerazione globale dei benefici socio-economici che scaturiscono dall’innovazione tecnologica. Ad esempio non possono trascurarsi i grandi vantaggi rappresentati dalle banche dati presenti in Rete oltre che nello svolgimento dell’attività amministrativa, anche nel migliorare in generale la qualità della vita dei cittadini e nel promuovere le attività produttive ed economiche.

Con l’approvazione del decreto legislativo n. 196 del 30 giugno 2003, il quadro delle misure di protezione dei dati personali è stato profondamente modificato. I meccanismi di adeguamento previsti renderanno il Codice meno soggetto all’obsolescenza di fronte all’avanzare delle tecnologie, restando peraltro immune da tecnicismi e mantenendo invece una sufficiente generalità e indipendenza da specifiche tecnologie.

In particolare è necessario che qualsiasi trattamento di dati personali, specie se sensibili, sia rispettoso dell’art. 3 (richiamato dall'art. 81 per le carte elettroniche) del Codice in materia di trattamento di dati personali che sancisce il principio di necessità.

Rfid e Biometria



Tra le tecnologie più innovative degli ultimi tempi che pongono non pochi problemi in tema di privacy rientrano senz'altro sia le RFID che i sistemi biometrici.

Rfid è un acronimo (Radio Frequency ID Devices) con cui si indicano dispositivi microscopici simili a microchip contenenti un identificativo (ad esempio, un numero di serie), che è possibile riconoscere attraverso un lettore compatibile funzionante in radiofrequenza.

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il “tracciamento” di singole unità di prodotto nella catena di distribuzione dell’industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate.

Ma attraverso le cd. “etichette intelligenti” si possono trattare, anche senza che l’interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l’aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

In questo settore il problema privacy sta diventando molto delicato perché tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una “lettura” delle etichette a maggiori distanze) nonché – specie in ragione dell’adozione di *standard* tecnici comuni – dalla possibilità che terzi non autorizzati “leggano” i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, “riscrittura”).

Per questi motivi il Garante ha svolto una prima attività di approfondimento della materia (provvedimento generale del 9 marzo 2005) rivolgendo l’attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all’applicazione della normativa sulla tutela dei dati personali.

Del resto è notizia recente che l'obiettivo perseguito dalla Commissione europea attraverso una recente Comunicazione diffusa all'esito di una consultazione pubblica conclusasi nel 2006 è proprio una politica europea per i sistemi Rfid che coniughi l'esigenza di sfruttare le potenzialità di questa tecnologia con l'attenzione alla tutela della privacy ed ai possibili rischi per la salute e l'ambiente.

I sistemi biometrici

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.

Si tratta della ricerca più avanzata in tema di sicurezza degli accessi informatici. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Tra i sistemi biometrici si ricordano:

1. *le impronte digitali e le impronte palmari*;
2. *il riconoscimento della voce* (difettoso in caso di malattie da raffreddamento);
3. *il reticolo venoso della retina dell'occhio*;
4. *il controllo dinamico della firma* (con riferimento anche alla sua velocità di esecuzione).

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.

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, rischia di assumere aspetti preoccupanti con l'utilizzo della biometria.

L’Autorità Garante già è intervenuta, con un provvedimento del 28 settembre 2001, per stabilire le prime rigorose regole in base alle quali, all’ingresso degli istituti bancari, può essere consentita l’installazione di sistemi di rilevazione cifrata che, in caso di necessità, permettano la lettura delle impronte digitali.

In considerazione della particolare natura delle informazioni biometriche e dell'assenza di norme specifiche, l'Autorità ha valutato entro quali limiti possa considerarsi lecita, nell'ambito della realtà bancaria, l'installazione di sistemi di acquisizione criptata delle impronte digitali e quali debbano essere le imprescindibili garanzie da assicurare per il rispetto dei diritti fondamentali delle persone.

Al di là, quindi, dei principi generali stabiliti dal codice in materia di protezione dei dati personali l’Autorità Garante con i suoi interventi ha previsto una serie di prescrizioni che devono essere attuate nello specifico settore delle nuove tecnologie con particolare riferimento alle Rfid ed ai sistemi biometrici.

Le prescrizioni

Oltre al principio di necessità va rispettato il principio di liceità (art. 11, comma 1, lett. a), del Codice). Il trattamento mediante questi nuovi sistemi è lecito solo se si fonda su uno dei presupposti che il Codice prevede, rispettivamente, per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22) e, dall'altro, per soggetti privati ed enti pubblici economici (ad es., adempimento ad un obbligo di legge, o consenso libero ed espresso: artt. 23-27).

Il titolare *(art. 4, comma 1, lett. f))* può trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi *(art. 11, comma 1, lett. b)*). I dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti; devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi *(art. 11, comma 1, lett. b) e e) del Codice)*.

Il titolare deve verificare il rispetto del principio di proporzionalità in tutte le diverse fasi del trattamento. I dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare.

Il titolare del trattamento, nel fornire agli interessati la prescritta informativa precisando anche le modalità del trattamento *(art. 13 del Codice)*, deve indicare la presenza di etichette *RFID o sistemi biometrici* e specificare che, attraverso gli stessi strumenti è possibile raccogliere dati personali senza che gli interessati si attivino al riguardo.

Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 del Codice, semplificando le modalità e riducendo i tempi per il riscontro al richiedente *(art. 10, comma 1 del Codice)*.

In particolare, poi, per i sistemi biometrici, l’utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali deve essere riferita a situazioni di rischio, valutate anche sulla base di concordanti valutazioni da parte dei locali organi competenti per l’ordine e la sicurezza pubblica.

La rilevazione delle impronte non può dar luogo ad alcuna "schedatura" da parte degli istituti di credito che, quindi, non potranno costituire alcuna banca dati con le informazioni raccolte.

Le informazioni relative alle impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro acquisizione. Non saranno quindi immediatamente riconducibili a persone e l'eventuale associazione alle immagini, rilevate con telecamere, potrà avvenire solo dopo la decrittazione.

Soltanto l’autorità giudiziaria o di polizia, e solo nell’ambito di indagini connesse alla commissione di reati, potrà decifrare ed avere accesso alle informazioni.

I dati cifrati relativi alle impronte e alle eventuali immagini devono essere conservati in file giornalieri per un periodo non superiore a una settimana.

La videosorveglianza

In materia di videosorveglianza al di là dei principi generali fissati dal codice in materia di protezione dei dati personali, provvedimento fondamentale è quello generale sulla videosorveglianza datato 29 aprile 2004 dell'Autorità Garante.

Nel provvedimento, difatti, sono inequivocabilmente sanciti dei principi fondamentali da rispettare nel caso di installazione di telecamere. In particolar modo viene precisato che l'installazione di telecamere è lecita solo se è proporzionata agli scopi che si intendono perseguire. Gli impianti di videosorveglianza devono essere attivati solo quando altre misure siano insufficienti o inattuabili. L'eventuale conservazione delle immagini deve essere limitata nel tempo. I cittadini devono sapere sempre e comunque se un'area è sottoposta a videosorveglianza.

Se è vero che il diritto alla protezione dei dati personali non pregiudica l’adozione di misure efficaci per garantire la sicurezza e l’accertamento degli illeciti è anche vero che l’installazione di sistemi di videosorveglianza non deve però violare la privacy dei cittadini e deve essere conforme al codice in materia di protezione dei dati personali.

Il provvedimento del Garante ha dettato dei principi di carattere generale validi sia per i soggetti pubblici che per quelli privati adottati nel rispetto di quelle fondamentali prescrizioni in tema di privacy di liceità, necessità, proporzionalità e finalità.

Quindi i sistemi di videosorveglianza possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi.

La raccolta e l’uso delle immagini sono consentiti solo se fondati su presupposti di liceità: cioè, per i soggetti pubblici, quando siano necessari allo svolgimento di funzioni istituzionali e, per i privati, quando siano necessari per adempiere ad obblighi di legge o effettuate per tutelare un legittimo interesse.

Inoltre, prima di installare un impianto di videosorveglianza occorre valutare se la sua utilizzazione sia realmente proporzionata agli scopi perseguiti o se non sia invece superflua. Gli impianti devono cioè essere attivati solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano realmente insufficienti o inattuabili.

I cittadini che transitano nelle aree sorvegliate devono essere informati della rilevazione dei dati. L’informativa (della quale il Garante ha anche messo a disposizione un modello semplificato: un cartello con un simbolo ad indicare l’area videosorvegliata) deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi.

In caso di registrazione, il periodo di conservazione delle immagini deve essere limitato: a poche ore o al massimo 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini. Per attività particolarmente rischiose (es. banche) è ammesso un tempo più ampio, che non può superare comunque la settimana.

Quando si intende installare sistemi di videosorveglianza che prevedono un intreccio delle immagini con altri particolari (es. dati biometrici, voce) o in caso di digitalizzazione delle immagini o di sorveglianza che valuti percorsi e lineamenti (es. riconoscimento facciale) è obbligatorio sottoporre tali sistemi alla verifica preliminare del Garante.

Va limitata rigorosamente la creazione di banche dati quando è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza la loro registrazione (monitoraggio del traffico, controllo del flusso ad uno sportello ecc.).

Il provvedimento del Garante detta regole riservate anche ai soli soggetti pubblici. Difatti viene precisato che un ente può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali. Anche quando un'amministrazione è titolare di compiti in materia di pubblica sicurezza o prevenzione dei reati, per installare telecamere deve comunque ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti. Non è quindi lecita, senza tale valutazione, una capillare videosorveglianza di intere aree cittadine.

Viene inoltre ribadito dall'Autorità il divieto assoluto di controllo a distanza dei lavoratori nel rispetto delle garanzie previste in materia di lavoro, sia all’interno degli edifici, sia in altri luoghi di prestazione del lavoro.

Si ricorda che anche il codice per la protezione dei dati personali prevede la delicata materia della videosorveglianza prevedendo all'art. 134 la promozione da parte del Garante della sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini.