Privacy e Sicurezza nelle attività di consultazione telematica

Foggia, 28 ottobre 2011

Michele Iaselli

Al fine di impostare correttamente l'argomento in questione, è opportuno premettere quanto ormai già noto a tutti gli operatori interessati e cioè che con il processo telematico si rientra nell'ambito della informatica giudiziaria gestionale da intendersi come il ramo che investe i procedimenti che si svolgono con l'intervento del giudice e delle parti. Il processo viene gestito con l'ausilio dell'elaboratore, nel quale vengono memorizzati, sotto forma di dati codificabili, tutti gli atti del processo, che corrispondono ad attività strutturate.

Non siamo però più nell'ambito di una prospettiva statica dell'automazione che si limita ad una mera attività di consultazione di dati giuridici e giudiziari eteronomi; ma in tal caso l'avvocato si pone in una prospettiva dinamica che tende ad inserire gli studi legali nel circuito formativo dei dati; in tal caso gli studi legali assumono un ruolo attivo, con un contributo diretto all’automazione di processi gestionali aperti, ove possibile, ad apporti esterni agli uffici giudiziari.

Quindi l’elemento innovativo e decisivo per il nuovo sviluppo dell’automazione dei dati giuridici è quello rappresentato dall’avvento della telematica, che consente la trasmissione dell’informazione a distanza, l’informatica distribuita ed interattiva, la telecomunicazione fra i giudici, le nuove forme di controllo e di partecipazione all’iter processuale sia da parte degli operatori interessati sia da parte degli organi preposti all’Amministrazione Giudiziaria.

Fatta quindi questa dovuta premessa appare chiaro che il problema della privacy e quindi anche della sicurezza informatica assume una rilevanza considerevole sia per il fondamentale utilizzo delle nuove tecnologie sia per la natura sensibile dei dati trattati (giudiziari).

Come è noto 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, 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.

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.

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.

Questi principi di carattere generale naturalmente assumono un rilievo fondamentale quando si opera in un settore così delicato come quello giudiziario.

Ne è ben consapevole lo stesso legislatore che all’art. 6 del Decreto del Ministero della Giustizia del 21 febbraio 2011, n. 44 sancisce che “il portale dei servizi telematici consente l'accesso da parte dell'utente privato alle informazioni, ai dati e ai provvedimenti giudiziari secondo quanto previsto dall'articolo 51 del codice in materia di protezione dei dati personali”.

Per essere più precisi le stesse regole tecniche approvate con provvedimento del Ministero della Giustizia del 18 luglio 2011 all’art. 6 dispongono che “L'identificazione informatica avviene sul portale dei servizi telematici mediante carta d'identita' elettronica o carta nazionale dei servizi e sul punto di accesso mediante token crittografico(smart card, chiavetta USB o altro dispositivo sicuro)……”.

Inoltre anche l’art. 18 delle predette Regole tecniche riprendendo quanto sostenuto dall’art. 16 del Regolamento dispone che “la comunicazione che contiene dati sensibili e' effettuata per estratto: in questo caso al destinatario viene recapitato l'avviso disponibilita' della comunicazione di cancelleria..... il destinatario effettua il prelievo dell'atto integrale accedendo all'indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso”. Tale prelievo avviene attraverso l'apposito servizio proxy del portale dei servizi telematici, su canale sicuro (protocollo SSL).

A questo punto è evidente che in tale settore il rispetto di quanto prescritto dall'art. 33 (le c.d. misure minime di sicurezza) del Codice per la protezione dei dati personali assume un carattere tassativo. Tali misure garantiscono la sicurezza minima al trattamento dei dati.

Si fa riferimento in particolare all’art. 34 del Codice che disciplina ed elenca principalmente le misure minime di sicurezza da adottare nel caso di trattamenti di dati personali effettuati con strumenti elettronici, demandando la determinazione delle modalità di applicazione alle disposizioni contenute nel Disciplinare tecnico allegato al codice (allegato B).

Principali prescrizioni

Per il trattamento con strumenti elettronici si prevede l’obbligo di adottare l’autenticazione informatica dell’utente, anche mediante l’utilizzo di eventuali sistemi biometrici, e adeguate procedure di gestione delle relative credenziali di autenticazione.

Il titolare deve adottare appropriate procedure, con la caratteristica della periodicità, per mantenere aggiornate le utenze ed i relativi profili di accesso sia per gli utenti normali, sia per quelli che sono addetti alla gestione o manutenzione dei sistemi. C'è da osservare, sul punto, che i precedenti ruoli di amministratore di sistema e custode delle password non sono citati dal d.lgs. n. 196/2003, ma di recente (2008) l'Autorità Garante con provvedimento generale ha di nuovo regolamentato la figura del'Ads.

Deve essere definito un sistema di autorizzazione per abilitare gli utenti all'accesso ai dati e/o ai trattamenti.

Gli strumenti elettronici e i dati devono essere protetti da accessi non autorizzati da parte di utenti, programmi informatici e da trattamenti illeciti.

Il titolare deve adottare appropriate procedure per il backup dei dati, il loro recupero, nonché il ripristino della disponibilità dei sistemi e dei dati.

Il titolare deve adottare un Documento Programmatico sulla Sicurezza.

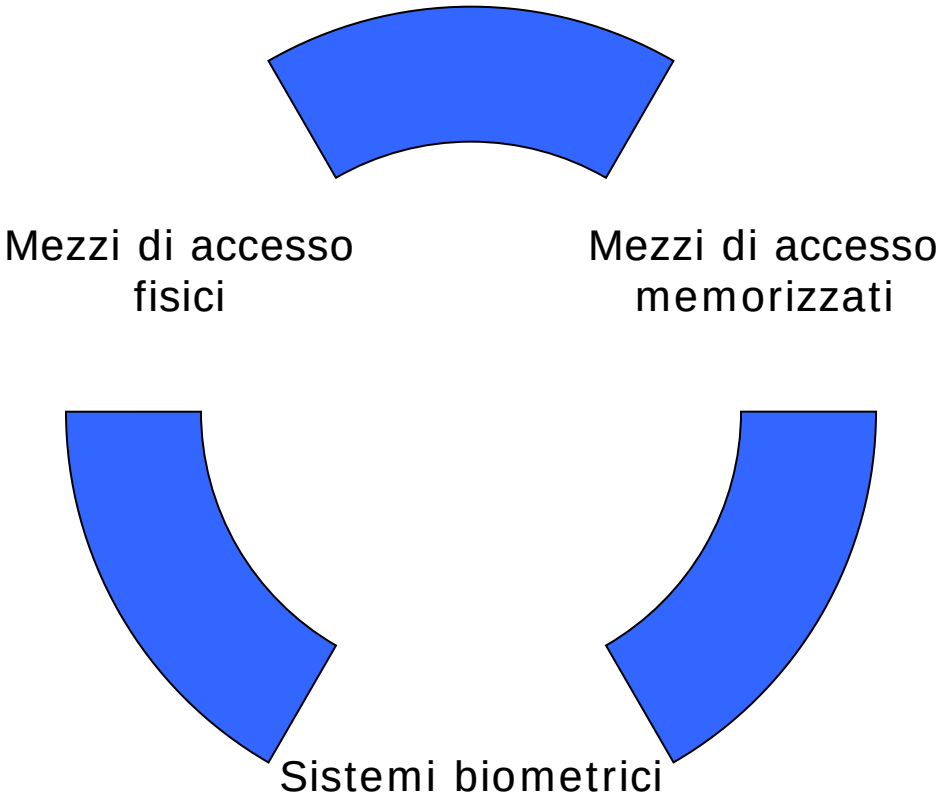
E’ necessario adottare tecniche di cifratura per i trattamenti atti a rivelare lo stato di salute o la vita sessuale rilevati da organismi sanitari.

Non bisogna dimenticare che la *sicurezza* nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.
Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i *data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).*

Riguardo l’aspetto “sicurezza” connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati.

Come può essere garantita la sicurezza?


Mezzi di accesso fisici
Mezzi di accesso memorizzati
Sistemi biometrici

I mezzi di accesso fisici sono consegnati all'utente legittimo ed egli esclusivamente ne viene in possesso e ne è responsabile. Tali mezzi sono costituiti da **documenti di riconoscimento tradizionali**, da **chiavi meccaniche** di varia forma e complessità, da **chiavi elettroniche** (c.d. tesserini magnetici di riconoscimento, carte di credito). Ciascuno di questi strumenti può essere considerato come una forma di legittimazione e di accesso controllato. Detti mezzi non sono, in genere, usati da soli, salvo che in ambienti poco attenti ai problemi della sicurezza. Infatti contraffazione e duplicazione sono abbastanza praticabili con tecnologie di medio livello, e quel che è più pericoloso, i predetti mezzi di identificazione possono essere sottratti o ceduti a soggetti non autorizzati.

I mezzi di accesso memorizzati dall'utente legittimo consistono in una sequenza di elementi (numerici, alfabetici o simbolici) che vengono forniti segretamente e memorizzati dall'utente legittimo e da questo forniti al sistema al momento in cui si vuole accedere allo stesso.

Il P.I.N. (Personal Identification Number): si tratta di un numero di identificazione personale che viene attribuito in maniera segreta esclusivamente all'utente legittimo. Molto noto è quello utilizzato con la carta Bancomat. Tale numero va scritto su un'apposita tastiera numerica al momento in cui si accede al computer.

La Password, ossia la c.d. “parola chiave”: si tratta di una parola, o di una sequenza di lettere e numeri, anche complessa, memorizzata dall’utente legittimo e che deve essere scritta, in genere su una tastiera. Detta combinazione alfanumerica va opportunamente scritta con rapidità per evitare che malintenzionati riescano a seguire la sequenza dei tasti premuti e a ricavare così, la parola chiave.

La combinazione numerica-logica variabile: in alcuni casi la parola chiave non è fissa, ma varia dinamicamente con riferimento ad una parte di elementi fissi ed altri variabili. Per esempio, una combinazione dinamica può essere rappresentata dalla sommatoria di un certo numero conosciuto dall'utente, addizionato, sottratto, diviso o moltiplicato ad un altro numero che potrebbe variare con riferimento al giorno della settimana, alla data completa, ovvero ad un dato variabile.

I mezzi di accesso che confrontano caratteristiche fisiche dell'utente con quelle memorizzate dal sistema (i cd. sistemi biometrici). 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).