Congresso della
Federazione degli Avvocati d'Europa
*Sessione Stage*

# *The legal Profession and Data Protection*

*Wroclaw 22 settembre 2011*

Wroclaw Regional
Chambers
of Legal Advisor

Ordine degli Avvocati di Trani

# Le misure di sicurezza e la protezione dei dati personali

*di*

*Francesco Tedeschi*

**INDICE**



*Contributo scientifico redatto in occasione della Sessione Stage del Congresso della Federazione degli Avvocati d'Europa tenutosi a Wroclaw il 22 settembre 2011*

*Organizzazione:*

FBE

*Ordine Partecipante*

Ordine degli Avvocati di Trani

**Le misure di sicurezza e la protezione dei dati personali**
**Wroclaw 22 settembre 2011**
*di Francesco Tedeschi*

## Preambolo e genesi storica della protezione dei dati personali.

Lo sviluppo del pensiero giuridico ha determinato il riconoscimento di cittadinanza ad alcuni aspetti della vita che prima non ne avevano, ovvero ricevevano riconoscimento di mera aspettativa. Si pensi ai alla tutela della salute che ha visto affermarsi nuove forme di responsabilità quali quella per danni da fumo con l'imposizione del divieto di fumare nei luoghi aperti al pubblico; ovvero il riconoscimento del danno c.d. esistenziale, di costruzione giurisprudenziale consistente nel pregiudizio derivante da scelte di vita diverse da quelle che si sarebero adottate se non si fosse verificato un evento dannoso.
Tra le nuove forme di tutela può annoverarsi il diritto alla riservatezza ovvero alla privacy, quale diritto della personalità del cittadino.

Invero, già il 1890 Samuel Warren e Louis Brandeis osservavano che l'individuo deve avere la piena protezione della sua personalità e della sua proprietà in quanto principi così antichi come lo stesso common law[1], operando così un superamento del principio della legge quale " *rimedio soltanto contro l'ingerenza fisica nella vita e nei beni, contro gli atti violenti di trasgressione* "[2]. Warren e Brandeis concentravano la loro attenzione sul diritto alla riservatezza dell'individuo alla luce dell'uso che poteva farsi delle riproduzioni delle fotografie sui mass media. Si trattava di un primo approccio ad una visione dinamica del diritto, il quale deve tutelare le esigenze della vita dell'individuo seguendo il corso delle innovazioni tecnologiche e del costume come una sorta di continuo *work in progress*.

In epoca più recente il diritto alla *Privacy* ha trovato il suo riconoscimento nelle normative statali anche attraverso la sua elevazione a rango costituzionale come espressione di un valore fondamentale connaturato alla personalità dell'uomo.

Il diritto alla riservatezza ha trovato un pieno riconoscimento a livello internazionale con la ***Dichiarazione Universale dei diritti dell'Uomo,*** adottata dall'Assemblea Generale della Nazioni Unite il 10 dicembre 1948, che all'art. 12 riconosce il diritto inviolabile dell'uomo alla esclusione dalle

[1] "**The right to Privacy**" di Warren e Brandeis *in Harvard Law Review – Vol IV December 15, 1890 N. 5*
[2] così nel testo: *Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis*

interferenze nella sua vita privata[3]. In Europa la ***Convenzione Europea per la Protezione dei Diritti del'Uomo e delle Libertà Fondamentali*** del 1950 attribuisce valore al dato personale anche se in embrione. Più recentemente la ***Carta dei diritti fondamentali dell'Unione Europea***, approvata dal Consiglio Europeo in data 11 dicembre 2000 ha espressamente riconosciuto, quale diritto fondamentale dell'individuo, il diritto alla protezione dei dati personali[4]. Tuttavia ogni Stato membro della Comunità, ben prima del riconoscimento nella Carta di Nizza, si è dotato di una normativa a tutela dei dati personali. Possiamo ricordare la Germania che aveva disciplinato la materia con una legge del *Land* dell'*Essen* nel 1970; tuttavia è la Svezia, con la legge denominata *Personal Data Act* del 1973, ad essere riconosciuta come la prima nazione del mondo a dotarsi di una legge *ad hoc* per la tutela dei dati personali. Le altre nazioni d'Europa non sono state insensibili al fenomeno e nel corso del tempo hanno adottato una normativa a tutela dei dati personali: la Repubblica Federale Tedesca nel 1977; l'Austria nel 1978; la Francia con una prima legge del 1978 modificata nel 2004, l'Inghilterra nel 1984 e nel 1998 ; la Svizzera dapprima con la legge cantonale del Canton Ticino nel 1987 e poi con quella federale nel 1992; la Spagna nel 1999 e, per finire l'Italia con una prima normativa nel 1996 seguita da una disciplina più organica nel 2003.

## Dati personali

Preliminarmente appare opportuno affrontare un aspetto di tipo giuridico/ terminologico.
Cosa si intende per dato personale?

Per dato personale qualunque informazione relativa a

- **persona fisica**
- **persona giuridica**
- **ente o associazione**

identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

---

[3] così recita l'art. 12: *Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, nè a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*.

[4] Così recita l'art. 8:

1. *Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
2. *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.*
3. *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*.

In buona sostanza, ogni informazione che possa consentire l'individuazione del soggetto cui l'informazione si riferisce, anche attraverso elementi apparentemente esterni al soggetto quali fotografie, filmati, estremi di documenti di identità – patente; PIN; ID; suoni; impronte digitali; caratteristiche biometriche; caratteri alfanumerici ecc., costituisce un dato personale.

Allorquando il professionista legale tratta un affare affidatogli si trova a gestire una miriade di dati personali non sempre riferiti al cliente; compito del professionista è gestire ed utilizzare i dati dei quali, per ragione del suo ministero, è venuto in possesso ai soli fini della difesa tecnica del suo cliente. Pertanto l'avvocato dovrà limitarsi a trattare i dati in modo pertinente e non eccedente l'effettiva necessità con il caso affidato.

Generalmente si usa il termine trattamento con riferimento alla gestione dei dati personali perché tale termine è più ampio della semplice conservazione o utilizzazione del dato personale in *database* fisici o informatici.
Infatti, nell'attività professionale l'avvocato non si limita ad utilizzare il dato personale a soli fini statistici o di conservazione, ma ne fa un uso più vasto. Il legislatore italiano nella sua disciplina ha individuato alcune forme di trattamento dei dati personali fornendo una elencazione esemplificativa, ma non esaustiva: *raccolta, registrazione, organizzazione, conservazione, consultazione,elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione* [5].

Come è intuibile ogni attività che ponga l'avvocato in relazione con un dato personale è *trattamento*; al fine di prevenire utilizzi dannosi per il soggetto interessato al dato personale, vanno assunti comportamenti a loro tutela. La pericolosità dell'attività di trattamento assume particolari connotazioni allorquando, per ragioni professionali, il professionista viene a conoscenza di dati definiti *sensibili* quali l'origine razziale, la vita sessuale, le convinzioni religiose o politiche, i carichi pendenti, i precedenti giudiziari e penali. Non sfuggirà che spesso il professionsita è a conoscenza di dati non solo dei propri clienti ma di soggetti esterni quali, l'avversario, i propri dipendenti, i testimoni ecc.

## La tutela dei dati personali e i modelli comportamentali.

Pe il valore attribuito al dato personale, si impone una particolare attenzione nei modelli comportamentali degli operatori che interagiscono con essi, e tra questi, in particolare, i professionisti nel settore legale.

[5] Così l'art. 4 D. L.vo 196/2003

Da sempre gli avvocati hanno avuto ben chiaro che l'attività da loro svolta non poteva prescindere dalla necessità di offrire al cliente una sicurezza circa il contenuto degli affari trattati. Infatti, gli avvocati, sia per effetto del contratto di mandato che per regole deontologiche, hanno il dovere di riservatezza e protezione degli affari loro affidati dai clienti. Non sfuggirà che il professionista si espone a responsabilità di natura civilistica e deontologica nel caso in cui venga meno agli obblighi di riservatezza.

Tuttavia, il dovere di mantenere la riservatezza è connaturato con l'obbligo di proteggere tale riservatezza, attraverso l'adozione di misure volte a rendere tale dovere effettivo e non relegato a mera petizione di principio.

Per l'avvocato si impone un onere di cambiamento dell'approccio verso la materia e di ipotizzare gli adempimenti come adempimenti di routine che si adottano al momento della acquisizione del conferimento dell'incarico da parte del cliente. Infatti, quando un cliente affida un incarico si è soliti inserire i documenti ricevuti in una cartellina sulla quale viene indicato il nome del cliente e la controparte; i dati personali del cliente vengono inseriti in una agenda che consenta il suo facile reperimento, e conseguentemente poi si è soliti provvedere a collocare il fascicolo di ufficio in uno schedario, non certo accessibile a chiunque frequenti lo Studio Legale. Conseguentemente il professionista dovrà solo cambiare leggermente il suo modus operandi, provvedendo a seguire alcune regole di prudenza che gli eviteranno di essere esposto al rischio di arrecare danno al cliente e di farsi muovere un rimprovero di scarsa affidabilità.

Purtroppo la sicurezza viene spesso percepita in senso negativo perché tesa a determinare interferenza con le consolidate procedure di gestione dello Studio ed aumentare il lavoro con adempimenti supplementari; tuttavia la sottovalutazione del fattore sicurezza aumenta la vulnerabilità dei sistemi di protezione non solo dei dati, ma dell'intero processo produttivo dello Studio.

In una ottica di strategia a medio-lungo termine una maggiore attenzione al fattore sicurezza dei dati personali costituisce uno strumento di potenziamento e di acquisizione di clientela perché le modalità adottate per garantire la sicurezza dei dati detenuti per conto del cliente costituirà un fattore determinante di scelta del professionista. In questa ottica il professionista deve mutare la propria *Weltanschauung* operativa e proiettarsi verso modelli di gestione dello Studio compatibili con quelli generalmente accettati come virtuosi.

## Le politiche di sicurezza ed il Sistema di gestione dei processi organizzativi.

Va osservato che come nei normali processi produttivi di tipo industriale/commerciale, anche per le professioni legali la scelta di un modello comportamentale potrà essere decisiva ai fini della valutazione in sede disciplinare o civilistica, nel caso di diffusione, smarrimento o cessione dei dati personali detenuti, onde individuare il discrimine tra comportamento colpevole e comportamento incolpevole. Tale scelta si rende ancor più determinante allorquando i dati personali vengano gestiti e trattati attraverso strumenti elettronici connessi ad una rete esterna (*cfr.* con internet ).
Tuttavia, tutte le normative di riferimento, ponendosi come norme in bianco, pur individuando alcuni parametri di riferimento, in genere, non li indicano con precisione rimettendo la valutazione della correttezza dei comportamenti di sicurezza a *standard* comunemente accettati a livello internazionale.

In buona sostanza, come accade per gli IAS in tema di principi contabili, che costituiscono principi ai quali in genere devono attenersi le imprese nella redazione dei bilanci recepiti dalle normative nazionali ed europee, così in materia informatica la sicurezza dei sistemi è demandata a *standard* internazionali.

La necessità di valutare i rischi e di adottare procedure *standard* di verifica e certificazione della sicurezza dei sistemi trova una sua prima disciplina nel 1985 ad opera del Dipartimento di Difesa americana che emanò il definito volgarmente "*Orange Book*" [6]. Successivamente il Dipartimento di Difesa Americano ha elaborato ulteriori guide raccolte nelle denominate *Rainbow Series*, rappresentanti le regole generalemte accettate di *security policies.*

In Europa, nella metà degli anni '90, l'Inghilterra rilevò la necessità di individuare regole di sicurezza e validazione dei processi di sicurezza dei sistemi informatici. Tali regole dettero origine nel 1993 allo *Standard BS 7799*[7], successivamente corretto ed implementato nel 1999 dando origine agli *Standard BS 7799-1* e *BS 7799-2*[8], quest'ultimo, ulteriormente integrato nel 2006 con il *BS 7799-3*. Al fine di renderli più universalmente accettati, gli *British Standards* vennero sottoposti all'approvazione

[6] Il nome ufficiale di tale documento è: *DOD-5200.28-STD DoD Trusted Computer System Evaluation Criteria, 26 December 1985*
[7] Lo *Standard BS 7799* è denominato *Code of practice for information security management*
[8] Mentre lo *Standard BS 7799-1* riproduce il Code indicato alla nota che precede il *BS 7799-2* si occupa della gestione della sicurezza ed è denominato *Specification for security management*

dell'*International Organization for Standardization* che nel 2000 emanò l'*ISO/IEC 17799/2000*[9]*,* integrato nel 2005 dallo Standard ISO/IEC 27001.

In genere quando si pone attenzione al fattore sicurezza non si può disgiungere tale elemento dal fattore rischio inteso come pericolo di perdita o lesione di un bene materiale o immateriale.

Lo sviluppo tecnologico e l'evoluzione del pensiero giuridico volto al riconoscimento di nuovi diritti e di tutela degli stessi in vari ambiti, hanno determinato maggiore attenzione al fattore prevenzione ed hanno impresso maggiore impulso all'individuazione di strumenti volti a prevenire perdite o lesioni dei diritti.

Si pensi all'evoluzione della tecnologia nel campo della motorizzazione. Le automobili di qualche anno fa erano poco attente a strumenti di prevenzione del rischio "*impatto da scontro*"; oggi ogni auto è dotata di air bag ed il rischio di lesioni determinate da uno scontro è limitato.

La maggiore attenzione rivolta alla tutela di riservatezza dei dati personali ed al loro utilizzo solo a precise condizioni, ha determinato la necessità di individuare gli strumenti per prevenire il rischio di loro perdita o loro diffusione e/o uso indiscriminato.

L'insieme degli strumenti rivolti alla protezione dei dati personali sono le misure di sicurezza.

Per l'individuazione delle misure di sicurezza informatiche dirette alla protezione dei dati personali trattati con l'ausilio di strumenti elettronici, i richiamati *Standard* internazionali costituiscono un valido aiuto e l'adozione degli accorgimenti ivi indicati costituisce un valido elemento fortemente attenuante, se non addirittura esimente, della responsabilità per danneggiamento e/o uso improprio dei dati personali trattati.

Tuttavia, la predisposizione delle misure di sicurezza richiede una preventiva attività di analisi e valutazione attraverso due *step*:

- **La politica di sicurezza,** intesa come l'insieme degli obiettivi di sicurezza dei dati personali che si intende adottare in funzione della loro tutela
- **Il sistema di governo della sicurezza dell'informazione**,inteso come l'insieme dei meccanismi di sicurezza adottati ed aggiornati al fine di mantenere il livello di protezione dei dati sempre costante nel tempo.

[9] Invero l'*ISO/IEC 17799/2000* ha recepito solo lo *BS 7799-1.*

Tali step si traducono in modelli dinamici perché hanno una validità connessa con lo lo sviluppo tecnologico e con le continue forme di aggressione informatiche mutanti nel tempo.

Pertanto il professionista dovrà adottare degli schemi organizzativi e di gestione dei dati diretti ad un continuo confronto tra gli obiettivi di sicurezza e gli accorgimenti tecnici necessari in relazione con i rischi cui i dati sono esposti alla luce dei più recenti sviluppi tecnologici.

Tuttavia, va osservato che le attività operative sono tra loro interdipendenti e la modifica di un fattore di rischio comporta la necessità di modificare tutta l'architettura predisposta per la tutela dei dati trattati.

Possiamo immaginare il *processo di sistema di governo della sicurezza* e *la politica di sicurezza* adottata come i tasselli di un puzzle che devono coincidere per forma e spessore, per cui la variazione di forma di uno deve necessariamente comportare la variazione dell'altro onde consentire la conservazione dell'unità del puzzle.

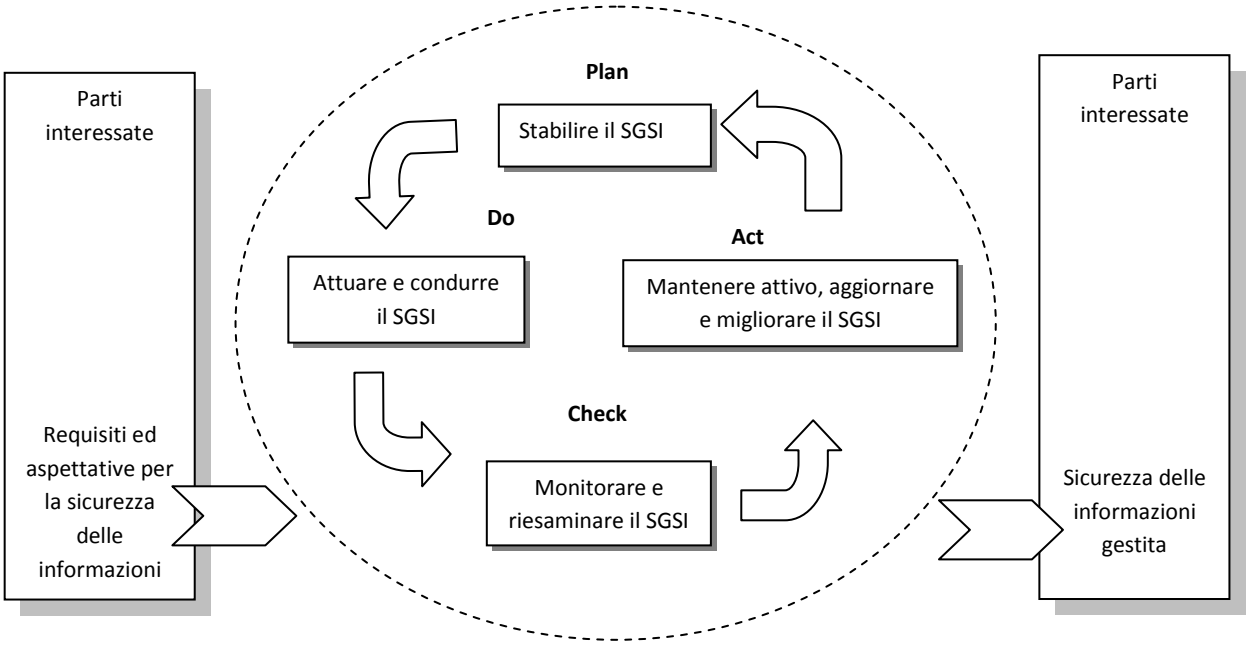
Il modello dinamico di Sistema di gestione di sicurezza informatica adottato dallo *Standard* ISO/IEC 27001 si articola in sei fasi secondo lo schema che segue:


Come è evincibile dallo schema i risultati delle analisi e le misure adottate sono messe continuamente in discussione alla luce dei cambiamenti determinati da fattori esterni ed interni, ed alla luce degli sviluppi tecnologici in tema di variazione dei fattori di rischio.

L'adeguamento del sistema di gestione si basa su un modello chiamato *PDCA*[10] applicato al sistema di gestione della sicurezza informatica

[10] PDCA è l'acronimo dei termini inglesi ***P**lan, **D**o, **C**heck, **A**ct,* di solito rappresentato in questa forma circolare, definita anche come "*ruota di Deming*", per evidenziare l'interazione continua delle operazioni di valutazione e gestione dei processi organizzativi

schematicamente raffigurato nello Standard ISO/IEC 27001 nel modo che segue:




## Misure di sicurezza

Nell'affrontare il tema delle misure di sicurezza è opportuno l'analisi distinta tra

- **il trattamento effettuato con l'uso di strumenti elettronici**
- **il trattamento effettuato senza l'uso di tali strumenti.**

La distinzione è doverosa per le diverse implicazioni determinate dalla scelta di trattamento attraverso l'una o l'altra modalità.

## Trattamento effettuato con l'uso di strumenti elettronici

Per strumenti elettronici si intende qualsiasi oggetto elettronico idoneo a conservare dati personali quale un h*ard disk* una *smart-card*, un telefono cellulare con una scheda di memoria versatile, una macchina fotografica digitale, una *memory stick* e quant'altro sia suscettibile di acquisire e conservare dati personali.

Una prima scelta operativa consigliata per prevenire rischi di dispersione di dati personali è quella di evitare un uso promiscuo dello strumento elettronico usato nello Studio Legale per il trattamento dei dati. Pertanto sarebbe opportuno che il *pc* dedicato al lavoro dello Studio ed al trattamento dei dati non sia utilizzato con una connessione ad internet per usi privati (chat, scaricamento di programmi di diletto, collegamento a server di scambio file, ecc), ovvero per ragioni non direttamente connesse con l'esercizio dell'attività.

L'uso degli strumenti elettronici impone l'adozione di misure dirette ad un uso consapevole dello strumento. Infatti, possiamo immaginare lo strumento elettronico come un immobile al cui ingresso è preposto un soggetto che potrà consentire l'accesso solo a persone qualificate.

In tale ottica possiamo individuare alcuni *step* per l'accesso allo strumento elettronico

### a) Autenticazione informatica

L'autorizzazione di accesso ai dati presuppone l'avvenuta individuazione corretta del soggetto autorizzato ad accedere ai dati.
Il sistema di autenticazione è proteso ad individuare con precisione chi intende accedere ai dati personali contenuti in un sistema informatico.
In buona sostanza, l'autenticazione informatica consiste nella verifica dell'identità dell'utente, che consente da un lato di controllare chi accede ai dati e, dall'altro, di attribuire la responsabilità ad un soggetto specifico per gli eventuali usi impropri dei dati.
L'autenticazione informatica si compone di due elementi:

- **il codice di identificazione**
- **il codice di verifica dell'identità**

#### Codice di identificazione

Il codice di identificazione consiste nell'attribuzione di un nome ad ogni utente.
Nella tecnica informatica tale codice viene chiamato solitamente *User Id*
In genere il codice di identificazione corrisponde al nome del soggetto che opera ovvero al suo numero di matricola.
E' evidente che il codice di identificazione deve essere personale ed univoco onde consentire a posteriori di individuare il soggetto che ha avuto accesso ai dati in un certo momento per le indagini sulle cause del malfunzionamento del sistema.

#### Codice di verifica dell'identità.

Il Codice di verifica dell'identità consiste nel superamento della prova di accertamento della identità del soggetto attraverso il riscontro della corrispondenza del soggetto autorizzato con il codice di identificazione con chi materialmente sta accedendo ai dati personali.
Per riprendere l'esempio dell'immobile dotato di portineria, per l'accesso non è sufficiente che un soggetto si qualifichi come chi dice di essere, ma deve provare di esserlo
Nell'attuale panorama di conoscenze tecniche si possono individuare tre tipi di codice di verifica dell'identità:

- **una parola chiave o *password* che consiste in una informazione nota solo all'operatore;**
- **un oggetto posseduto in via esclusiva dall'operatore;**
- **una caratteristica fisica personale dell'operatore.**

**Parola chiave o Password.**

Il tipo più comune di verifica dell'identità è la ***password***.

Per quanto criticato, perché facilmente eludibile, l'uso di tale sistema di verifica è sufficientemente sicuro. Infatti, il Governo Federale degli Stati Uniti lo ha usato per molti anni

La parola chiave è una composizione alfanumerica la cui lunghezza può essere variabile a seconda di quanto stabiliscano le normative in materia[11], ovvero se il sistema non lo consente, nel numero massimo di caratteri consentito.

Nella scelta della parola chiave è preferibile una composizione alfanumerica. Infatti, il numero di parole che possono comporsi in una stringa di 8 caratteri, utilizzando una composizione mista di parole e numeri, è maggiore di una composizione di soli numeri o lettere della stessa lunghezza. Infatti, la probabilità che si possa individuare un carattere di una *password* di 8 caratteri alfanumerici è 1 su $8^{62}$ e sempre che non si utilizzino caratteri speciali quali i caratteri accentati ovvero i simboli del tipo @; €; $

Nella scelta della parola chiave lo Standard internazionale ISO/IEC 27002 indica i seguenti requisiti di selezione:

- ricordata con facilità;
- non basata su qualcosa che qualcun altro potrebbe facilmente indovinare o ottenere utilizzando le informazioni relative persona, quali le date di nascita dell'utente o di loro familiari, numeri di telefono o nomi di familiari;
- non vulnerabile da termini utilizzati in dizionari;
- non contenente identiche e consecutive lettere o numeri.

A questi requisiti ritengo possano aggiungersi i seguenti utili accorgimenti:

- facilmente individuata dall'utente;
- digitata senza difficoltà.

[11] Lo Standard ISO/IEC 27002 non indica una misura minima di caratteri limitandosi a suggerire, al punto 11.3.1 una sufficiente lunghezza minima. Il legislatore italiano ha stabilito che una lunchezza rassicurante sia una composizione alfanumerica di almeno 8 caratteri

Pertanto la *password* non deve essere così banale da consentire a chiunque di scoprirla; tuttavia la scelta dalla parola chiave deve corrispondere a criteri che consentano all'utente di operare sullo strumento elettronico.
Ogni utente potrà utilizzare la tecnica che ritiene più opportuna per elaborare una *password* difficilmente individuabile.
Ad esempio, una tecnica potrebbe essere quella di usare come *password* le strofe di una canzone ovvero le prime lettere delle parole di una poesia.
Vi sono anche programmi generatori di *password* casuali.

Ma la password non deve essere immutabile nel tempo; essa va cambiata periodicamente ed ogni qualvolta si ritenga compromessa.

Il sistema informatico usato dovrebbe essere strutturato in modo tale da invitare al cambiamento della parola chiave quando si è raggiunto il tempo massimo di utilizzo della stessa. Altresì lo stesso sistema dovrebbe avere la capacità di verificare che la nuova *password* usata non sia quella usata da altro utente ovvero sia stata già usata in precedenza. Il sistema dovrebbe essere impostato in modo tale da consentire il riutilizzo di una *password* ogni *n* utilizzi.

La *password* è strettamente personale e va utilizzata la tecnica della "*one time password*" consistente nell'attribuzione all'utente di una password che questi ha il dovere di cambiare al primo utilizzo del sistema ed il sistema deve essere strutturato in modo tale da invitare l'utente a cambiare la password prima dell'utilizzo del programma di accesso al trattamento dei dati personali.

L'attribuzione di una parola chiave personale risponde a criteri di ragionevolezza. Infatti, solo una *password* personale ed utilizzabile in modo esclusivo da un solo utente consente di individuare il responsabile in caso di uso improprio dei dati personali, così come può consentire di individuare il responsabile di una cessione illecita della *password*. Infine tale criterio rende più facile la disattivazione della *password* nell'ipotesi in cui l'incaricato cessi i rapporti con lo Studio Legale.
Una parola chiave quando non è più utilizzata deve essere archiviata. L'archiviazione richiede che il sistema sia in grado di consentire l'accesso all'archivio delle *password* solo a soggetti qualificati, quali il titolare del trattamento, il responsabile del trattamento, ovvero l'amministratore di sistema.

Altro aspetto fondamentale da tenere presente in tema di *password* è la sua digitazione.

Operativamente l'utente deve poter digitare la *password* in modo da evitare che terzi estranei possano vedere la tastiera. Quanto al video tutti i più moderni sistemi prevedono che durante la digitazione della *password* non si vedano i caratteri immessi ma solo dei simboli anonimi.
Il sistema dovrà prevedere un numero massimo di tentativi di digitazione della *password*, ovvero la disabilitazione di accesso al sistema dopo un certo periodo di inattività.

Nei sistemi più complessi è prevista l'ipotesi di sblocco in caso di dimenticanza della parola chiave.
Lo sblocco potrà avvenire direttamente dall'utente attraverso un meccanismo di domanda e risposta: al momento della immissione la prima volta della *password* il sistema stabilisce con l'utente le modalità per consentirgli di riottenere la *password* dimenticata attraverso una domanda e relativa risposta predeterminata dall'utente.
In ogni caso, il titolare del trattamento deve poter accedere al sistema nell'ipotesi di blocco del sistema attraverso una *password-passepartout*. Infatti, se l'utente incaricato per una ragione qualsiasi non dovesse essere al posto di lavoro, deve essere sempre possibile per il titolare accedere ai dati personali da lui trattati.

Un ulteriore compito del professionista è quello di istruire gli utenti incaricati al trattamento dei dati personali di non lasciare incustodito o accessibile il terminale o il *pc* e che, nell'ipotesi di certo periodo di inattività, deve attivarsi un *screen saver* che impedisca a terzi di poter accedere ai dati ivi contenuti, prevedendo in tale ipotesi che per poter riattivare il sistema sia necessario digitare nuovamente la parola chiave.

### Oggetto posseduto in via esclusiva dall'operatore.

La verifica della identità dell'operatore potrà avvenire anche con un oggetto che possiede in via esclusiva l'utente.
In genere l'oggetto più utilizzato è un badge o scheda magnetica che viene inserita in un apposito lettore ed abilita le procedure.
Altro potrebbe essere un oggetto con apparato radio che il sistema riconosce, consentendo l'abilitazione delle procedure alla presenza del soggetto.
Tali sistemi non sono completamente sicuri perché facilmente duplicabili, dimenticati o persi. In tal caso non si potrebbe accedere al sistema.
Una possibile soluzione potrebbe essere quella di prevedere una scheda per l'accesso al sistema e la digitazione di una password per l'abilitazione delle procedure.

### Una caratteristica fisica personale dell'operatore.

Trattasi dei c.d. dispositivi di riconoscimento biometrico fondati sul riconoscimento di alcune parti del corpo del soggetto quali l'impronta digitale, la retina dell'occhio, la voce, la firma, la mano ovvero l'esame del volto.

In genere non si ritiene che tali meccanismi di verifica del codice di identificazione siano in contrasto con la *privacy* dell'utente perché, tecnicamente, il meccanismo di riconoscimento della caratteristica dell'operatore non si estende a tutta la parte del corpo interessata.

Ad esempio, un meccanismo di verifica che si basasse sulla lettura delle impronte digitali non estenderebbe il suo esame all'intera impronta ma ad alcuni elementi che sarebbero confrontati con quelli precedentemente immessi nel sistema.

L'insieme del codice di identificazione e di quello di verifica costituiscono le **credenziali di autenticazione.**

### b) Adozione di procedure di gestione delle credenziali di autenticazione.

Le credenziali di autenticazioni non utilizzate per almeno sei mesi devono essere disattivate, salvo quelle relative alle necessità di gestione tecnica (c.d. user-id e *password*-passepartout)

Il sistema potrà prevedere l'automatica disattivazione in caso di non utilizzo della *password*

Le credenziali di autenticazione vanno ovviamente disattivate nel momento in cui l'utente incaricato del trattamento non faccia più parte dello Studio.

Rientrano tra le procedure di gestioni anche le istruzioni sulle modalità di uso del pc da parte dell'utente.

### c) Utilizzazione di un sistema di autorizzazione.

Non è sufficiente prevedere un meccanismo di accertamento delle credenziali di autenticazione per rendere sicuro il sistema di trattamento dei dati personali.

E' altresì necessario prevedere un meccanismo di individuazione dei criteri di accesso ai dati personali per il loro trattamento attraverso un sistema di autorizzazione.

Si può definire Sistema di Autorizzazione il complesso degli strumenti elettronici e delle modalità di abilitazione all'accesso e trattamento dei dati in relazione a ciascun Profilo di Autorizzazione previsto per ogni utente.

Per Profilo di Autorizzazione può definirsi il complesso degli elementi abbinati univocamente ad un soggetto che consenta di individuare a quali dati egli può accedere e quali trattamenti può effettuare.
In parole povere con un sistema di autorizzazione si individua "*Chi*" può fare "*Cosa*"
In uno Studio Legale non sempre tutti i componenti hanno gli stessi compiti; né il Titolare del trattamento ha interesse a consentire l'accesso a chiunque su tutti i dati.
Pertanto bisognerà individuare un Profilo di Autorizzazione personalizzato per ogni singolo operatore.

Nella strutturazione di un Profilo di Autorizzazione dovrà predisporsi un mansionario che stabilisca a quali risorse ogni utente avrà accesso e con quali modalità potrà accedervi.
Uno schema di sistema di autorizzazione potrà essere così strutturato:

**Titolare** : accesso a tutti i dati.

**Segreteria :** : l'utente incaricato potrà avere accesso ai dati personali ma non a quelli sensibili; in particolare potrà stabilirsi che tale soggetto, occupandosi della gestione contabile dello Studio, potrà avere accesso ai dati dei clienti e dei terzi in funzione della gestione contabile. Altrettanto dicasi per la gestione degli appuntamenti: la Segreteria potrà avere accesso ai dati personali dei terzi in funzione degli adempimenti di udienza e conseguenti per la gestione degli appuntamenti, degli adempimenti e delle scadenze. L'utente incaricato potrà avere accesso ai dati archiviati solo se strettamente necessario alle funzioni assegnate

**Praticanti:** : accesso alle cartelle e file di elaborazione documenti contenenti anche i dati sensibili purchè per questi ultimi vi sia controllo di uso non ripetuto. All'uopo potrà predisporsi che il Titolare abiliti l'accesso di volta in volta. Il praticante potrà avere accesso ai dati archiviati solo sotto stretto controllo del Titolare.

Il Sistema di Autorizzazione dovrà essere predisposto all'inizio del trattamento per ciascun incaricato; periodicamente ed almeno ogni sei mesi, secondo quanto stabiliscono gli Standards Internazionali, andrà

verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. Pertanto una modifica delle mansioni comporterà la modifica del Profilo di Autorizzazione.
Da un punto di vista tecnico dovranno strutturarsi le *passwords* in modo tale che chi è autorizzato ad accedere e trattare dati personali non possa accedere agli altri dati. Ad esempio, l'addetto alla Segreteria non potrà accedere ai file dei documenti se non è previsto che egli possa utilizzare le procedure di formazione degli atti e dei documenti.

Infine, un Sistema di Autorizzazione potrà prevedere i livelli di accesso temporale in modo da escludere che alcuni soggetti possano accedere e trattare i dati in orari diversi da quelli c.d. d'ufficio

**d) Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.**

Una figura importante, nell'architettura della sicurezza dei sistemi informatici, è l'addetto alla gestione o alla manutenzione degli strumenti elettronici.

L'individuazione di tale soggetto è fondamentale perché le *Best Practices* e gli *Standards* internazionali impongono il ripristino degli strumenti elettronici in tempi brevi.

La scelta deve ricadere su un soggetto esperto poiché l'addetto alla manutenzione deve intervenire senza indugio sia sull'*hardware* che sul *software*.

L'addetto alla manutenzione non solo deve conoscere il funzionamento del programma applicativo ma deve essere in grado di intervenire sul sistema operativo; sui *software* di sicurezza anti intrusione ed antivirus, oltre che sull'*hardware*.

Se all'interno dello Studio non vi è una persona particolarmente esperta che sia in grado di assumere tale ruolo, è opportuno stipulare un contratto di assistenza e manutenzione con un professionista del settore.

Nel contratto di assistenza si dovrà prevedere l'obbligo di intervento immediato, ovvero in modo da garantire il ripristino della funzionalità completa del sistema in tempi ragionevolmente brevi. Altresì il contratto dovrà prevedere che, nell'ipotesi di trasferimento dell'hardware presso la sede dell'esperto, i dati contenuti nella memoria di massa dell'hardware non siano dallo stesso utilizzati, visionati e comunque trattati in alcun modo, fissando una penale nel caso di inosservanza a tale obbligo.

**e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici. I malware.**

Al fine di prevenire intrusioni indesiderate ai sistemi, specie se collegati alla rete internet, vanno installati programmi specifici che prevengano tali rischi che si aggiornino periodicamente.

Analogamente il sistema operativo deve essere in grado di aggiornarsi ogni qualvolta vengano rilasciate nuove *release* dal produttore dirette, attraverso *patch*, alla prevenzione della vulnerabilità del sistema, ovvero alla correzione di eventuali difetti di funzionamento del *software* o dell'*hardware*.

L'utilizzazione del termine intrusione e vulnerabilità del sistema trova la sua giustificazione nell'ampiezza dei pericoli di attacchi informatici che non possono essere prevenuti con un semplice antivirus.

Appare opportuno affrontare in questa sede l'argomento della sicurezza informatica che costituisce l'antecedente logico e pratico alla sicurezza dei dati.

Le tecniche di intrusione ai sistemi informatici, con il passare degli anni, si sono fatte sempre più pericolose e più subdole, perciò il *virus* rientra nella più estesa categoria dei software maligni denominati nella comune accezione ***malware***

I *malware* possono distinguersi in quelli diretti a danneggiare il sistema, compromettendone il regolare funzionamento e provocando il danneggiamento dei dati ivi contenuti ed in quelli che, invadendo il sistema, violano la privacy dell'utente.

Tra i primi si annoverano i ***virus*** intesi come programmi che si moltiplicano attraverso la diffusione in rete ed attraverso i quali i file contenuti nell'*hard disk* vengono cancellati. Il pericolo delle nuove forme di *virus*, come il famoso *I Love You*, è rappresentato dalla rapidità della loro diffusione, perché, in genere, questi nuovi *virus* contengono istruzioni per replicarsi e per trasmettersi a tutti i contatti contenuti nel programma di posta elettronica, con la conseguenza che tutti i contatti ricevono un messaggio di posta elettronica contenente come allegato il file infettato.

Altra forma di *malware* è il ***worm*** ( verme): non solo è autoreplicante ma è in grado di attivarsi anche senza l'intervento umano, sfruttando i bug del sistema. A tal proposito i produttori di sistemi operativi provvedono periodicamente a mettere in rete una *patch* ( pezza) diretta ad eliminare i bug del sistema.

Un altro tipo di *malware* particolarmente pericoloso è il ***trojan***.
Tale tipo di malware che prende il nome dal cavallo di Troia, consiste in un *software* contenuto all'interno di un altro programma o di un altro file che esegue regolarmente la sua funzione, ma che alla sua prima apertura attiva il *trojan*. Una volta attivato, il *trojan* si insedia nel sistema operativo e si attiva ogni volta che il *pc* viene acceso. Attraverso questo programma il *pc* infettato e collegato ad internet si trasforma in un server al quale un altro *pc* ,anch'esso collegato in internet, con un *software* di collegamento con il *trojan*, accede liberamente. In buona sostanza ogni qualvolta ci si collega ad internet con un *pc* infetto da un *trojan*, il *cracker* che ha infettato il *pc*, automaticamente può accedere, controllare, manipolare,cancellare tutto o parte del contenuto dell'hard disk oltre che immettere dati e file nel *pc* infettato e fare attivare altri e nuovi programmi. Si è preferito usare il termine corretto di *cracker* al posto di quello più comunemente conosciuto come *hacker* perché quest'ultimo è un programmatore esperto dei sistemi operativi e delle problematiche connesse alla violazione del sistema, mentre il *cracker* è colui che viola i sistemi informatici in modo e per motivi illeciti. Tuttavia il *cracker* può accedere ad un *pc* ed infettarlo con un *trojan* anche senza l'apertura di un file, sfruttando le vulnerabilità della rete e la vulnerabilità delle porte di accesso ad internet del *pc*. In poche parole il *cracker* con un programma denominato *portscan* verifica se il *pc* interessato abbia una porta di connessione *non sorvegliata* e sferra l'attacco introducendosi nel sistema.

Altra forma di attività illecita è il ***DoS***[12], attacco informatico in cui si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito *web*, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio[13].

Un *malware* altamente insidioso è il ***Rootkit,*** *software* creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore. La particolare insidiosità del malware sta nel fatto che si colloca nella *root* del sistema e si attiva all'accensione del pc prima della partenza del sistema operativo, con la conseguenza che l'antivirus non lo riconosce; infatti, l'antivirus si attiva come primo programma dopo la partenza del sistema operativo.

Infine ci sono i virus c.d. buoni che si preoccupano di individuare il *malware* e di rimuoverlo. Spesso, però, il *cracker* usa mascherare il *malware* da virus buono.

[12] **DoS**, è la sigla di **denial of service**, letteralmente *negazione del servizi.*
[13] Definizione tratta da *Wikipedia*

Tra i secondi possiamo individuare:
gli ***spyware*** che hanno la funzione di spiare i comportamenti dell'utente connesso ad internet ed inviare informazioni relative a comportamenti o al sistema del pc collegato a qualcuno che può utilizzarle per inviare posta indesiderata ( c.d. *spam* ) ovvero per scopi illeciti;
gli ***adware*** che hanno la funzione di aprire fastidiosissime finestre pubblicitarie durante la navigazione in internet;
il ***dialer*** che, promettendo l'accesso a siti per adulti in modo "gratuito", ovvero a siti dai quali è possibile scaricare suonerie o programmi "gratuiti, una volta attivato disconnette il modem dalla linea telefonica cui è connesso e lo collega ad un numero a pagamento.

Una delle forme di diffusione dei *malware* avviene attraverso messaggi di posta elettronica.
Una buona regola è quella di non aprire mai un allegato di posta elettronica se proviene da un mittente sconosciuto.

Tuttavia anche nell'ipotesi in cui un allegato di posta proviene da una persona a noi nota, è sempre meglio accertarsi se il mittente abbia effettivamente spedito il messaggi di posta con l'allegato.
Infatti, l'invio di c.d. ***fake e-mail*** è una tecnica di trasmissione di posta elettronica con allegato infetto. E' abbastanza facile, anche senza la conoscenza di particolari tecniche informatiche, inviare una *fake e mail*, mediante la modifica dell'account di posta elettronica. In sostanza, quando si imposta un indirizzo di posta elettronica nel programma di posta elettronica si forniscono indicazioni nel pannello generale dell'account. La modifica di queste consente di spedire posta elettronica sotto falso nome.
Orbene al momento del ricevimento del messaggio, se l'utente è registrato nei contatti del programma di messaggistica elettronica, il programma indicherà il mittente con il nome indicato nell'account modificato. In questo caso l'utente ritenendo di potersi fidare del messaggio ricevuto aprirà l'allegato e così inconsapevolmente avrà attivato il *malware*.

Pertanto è vivamente consigliato non aprire mai allegati di posta elettronica che siano dei file eseguibili. I file eseguibili sono quelli che contengono programmi; tecnicamente sono quelli che hanno una estensione *.exe*
Tuttavia una tecnica usata dal *cracker* è quella di modificare l'estensione del *file* attribuendogli una estensione più tranquilla ad esempio *.doc* ( file documento di word) ovvero *. jpg* ( file immagine); a volte l'allegato ha una doppia estensione confidando nel fatto che, in genere, nel sistema

operativo Windows nel pannello *Visualizzazione* di *Opzione Cartelle* vi è l'opzione di spunta nel pannello *nascondi estensione per i tipi di file conosciuti*. Pertanto allorquando si riceve un messaggio di posta elettronica la visualizzazione dell'allegato indica che trattasi di *file* innocuo anche se non è così.

Va osservato, invero, che nell'ipotesi di una *fake e-mail* potrebbe essere possibile risalire al mittente originale attraverso la verifica dei dettagli del messaggio dalle proprietà del messaggio. In tale riquadro potrà individuarsi da quale server e con quale *IP*[14] il mittente ha inviato il messaggio. Conseguentemente, attraverso una denuncia all'Autorità Giudiziaria, potranno attivarsi le indagini per l'individuazione del soggetto che ha inviato il messaggio con allegato infetto.

Si è usato il condizionale perché, in realtà, il messaggio potrebbe essere inviato attraverso un indirizzo *IP* diverso con una tecnica chiamata *IP Spoofing*, che consente di camuffare l'*IP* e di inviare e-mail in modo anonimo ovvero attraverso l'uso di un pc infettato che diventa uno "zombie" agli ordini del *cracker* che lo userà per inviare e-mail a terzi che riterranno di ricevere i messaggi di posta dall'ignara vittima.

Tempo fa sono pervenuti messaggi di posta elettronica con il logo Microsoft che invitava l'utente ad aprire un allegato costituente, apparentemente, una *patch* di aggiornamento per prevenire attacchi da virus: si trattava di una *fake e-mail* contenente un *malware.* Infatti, era del tutto impensabile che la Microsoft potesse utilizzare la posta elettronica per inviare gli aggiornamenti del sistema operativo. D'altronde era altrettanto inimmaginabile pensare di essere così noti alla Microsoft da ottenere il privilegio di un aggiornamento personalizzato del proprio sistema operativo.

Infine una ulteriore fonte di intrusione è l'uso di programmi di scambio file comunemente chiamati *file sharing* attraverso una connessione *P2P*. Il *file sharing* è usato per lo scambio di file audiovisivi o musicali. Per poter accedere a tale tipo di scambio è necessario utilizzare un programma di *P2P* che consente ad ogni utente di condividere una cartella per lo scambio, così facendo si consente di tenere aperta una porta che un malintenzionato potrebbe usare per accedere al pc.

Come proteggersi dai malware?

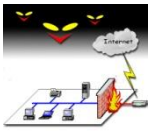
Una forma di protezione è l'antivirus  che ha il compito di scansionare tutti i file ivi compresi quelli ricevuti via *e mail*

[14] Per *IP* si intende l'identificativo personale attribuito dal Server all'utente connesso ad internet.

cancellando quelli infetti.

Il *Sans Institute*[15], cui fanno parte esperti del settore, ha redatto una linee guida[16] per prevenire possibili attacchi informatici.

Al fine di evitare attacchi intrusivi derivanti da programmi quali *portscan*, è bene dotarsi di un *firewall*, programma che frapponendosi tra il modem ed il pc collegato ad internet, blocca tutti i potenziali attacchi che provengono dalla rete.




Un buon *antivirus* e *firewall* dovrebbe avere le seguenti caratteristiche:

- idoneità di effettuare una scansione del pc al momento della sua accensione analizzando i file di *boot* e *system*;
- essere sempre attivo durante il collegamento ad internet;
- scansionare la messaggistica di posta elettronica ed i suoi allegati prima e durante lo scarico sul *pc*;
- bloccare le intrusioni provenienti da programmi, documenti e comunque istruzioni contenute nei *file* ricevuti ovvero nei *file* che tentano di introdursi indebitamente nel *pc* attraverso porte libere;
- cancellare i *file* infetti ovvero, nel caso non sia possibile, riporli in quarantena;
- essere aggiornabile via internet ovvero in altro modo e prevedere un meccanismo di allarme per l'aggiornamento; chiaramente l'aggiornamento dovrà riguardare non solo la definizione dei *virus*, ma anche quello del programma *antivirus* o *firewall*

E' vivamente consigliato aggiornare i programmi (non solo la definizione dei *virus*) con cadenza settimanale o quindicinale.
E' altresì vivamente consigliata la verifica del periodo di validità dell'abbonamento al programma. Infatti, se l'abbonamento è scaduto il programma di solito consente al massimo l'aggiornamento delle definizioni dei virus, ma non la protezione.

In commercio esistono dei programmi integrati che contengono sia un *antivirus* che un *firewall*.

Una nuova minaccia informatica sta rapidamente diffondendosi: *il phishing*.
Il nome trae origine dal termine inglese *fishing* (pescare): il malintenzionato pesca nella rete ignare vittime
Trattasi di una truffa ben architettata, attraverso artifici e raggiri, che inducendo in errore l'utente contattato consente al malintenzionato di

[15] Il *Sans Institute* è una Società americana fondata nel 1989 specializzata in formazione della sicurezza informatica.
[16] Le linee guida sono reperibili al seguente link: *http://www.sans.org/critical-security-controls/*

ottenere informazioni riservate quali lo *user id* (il nome utente) e la *password* per l'accesso a sezioni riservate per l'utente di siti istituzionali, di banche, di banche dati in abbonamento, di commercio elettronico o altro.
In genere, il truffatore invia una *e mail* ad una serie indefinita di utenti nella quale, utilizzando i loghi, per esempio di una banca, paventa la necessità della verifica dei dati personali dell'utente per i più svariati motivi ( manutenzione del server o altro). In calce all'*e-mail* viene indicato un indirizzo *web* al quale connettersi. L'utente, connettendosi all'indirizzo indicato, vedrà aprirsi una finestra con i loghi del sito della sua banca ovvero, addirittura una *home page* del tutto simile a quella originale del sito della banca. L'utente provvederà a *loggarsi* nella sezione riservata, immettendo il proprio *user id* e la propria *password*. L'utente non accederà a nessuna sezione del sito ma si ritroverà di nuovo nella *home page* ( questa volta quella reale) della banca e penserà che per motivi di connessione non è riuscito a connettersi e riproverà verificando la correttezza dei suoi dati. L'utente riterrà di non avere necessità di effettuare cambiamenti e chiuderà la finestra del *browser*. I dati dell'ignaro utente, nel frattempo, sono stati trasmessi al truffatore che potrà utilizzarli accedendo al sito della banca per effettuare operazioni illecite sul conto corrente del malcapitato con le credenziali sottratte fraudolentemente. Ci si può accorgere della truffa verificando il nome dell'indirizzo *web* che di solito è contrassegnato da una serie di numeri (indirizzo *IP*) e che normalmente una banca non indica.

Da ultimo è stata scoperta una più raffinata tecnica denominata *pharming* attraverso la quale il truffatore sfruttando alcune vulnerabilità della rete utilizza il sito ufficiale della banca per effettuare un reindirizzamento ad un altro sito creato appositamente per perpretare la truffa. E' vivamente consigliato di ignorare messaggi che provengano da banche o altre istituzioni private o pubbliche che invitano l'utente a verifiche dei propri dati; se si hanno dubbi è consigliabile contattare direttamente l'ufficio istituzionale del soggetto che ci ha inviato l'*e-mail* per la verifica dell'autenticità del messaggio ricevuto.

Infine è opportuno evidenziare che, sebbene si possa avere adottato la misura di sicurezza informatica più efficace, rimane sempre un anello debole nella catena della sicurezza informatica: l'**uomo**
Uno dei maggiori pericoli per la sicurezza informatica viene dall'attività dei c.d. *ingegneri sociali*, persone che attraverso sistemi di comunicazione, quali il telefono riescono ad ottenere dati ed informazioni per poter violare i sistemi attraverso una tecnica chiamata di *social engineering*. Il c.d. ingegnere sociale è colui che con tecniche di persuasione, riesce ad

ottenere informazioni riservate; ad esempio, qualificandosi come ufficiale di P.G. potrebbe ottenere informazioni riservate su alcuni fascicoli dello Studio, ovvero qualificandosi come tecnico della Telecom ottenere *password* di accesso ai sistemi per una paventata necessità di controllo delle procedure di accesso ad internet.
Buona regola è quella di verificare sempre la provenienza delle richieste di informazioni per via telefonica e fornirle solo se strettamente necessario.

Alla luce delle suestese argomentazioni appare lecito chiedersi cosa bisognerebbe fare per rendere un sistema informatico sicuro al 100%.
Un adagio informatico sostiene che l'elaboratore veramente sicuro è quello guardato a vista, scollegato da una rete sia interna che esterna, blindato ed essenzialmente **spento**. Tuttavia, anche il *pc* spento non è del tutto sicuro. Infatti, per gli addetti ai lavori non è sconosciuto il c.d. attacco *Tempest*[17] consistente nella intercettazione delle informazioni tramite l'analisi delle onde elettromagnetiche emesse dagli apparati elettronici, utilizzando le falle nelle procedure di sicurezza delle emissioni elettromagnetiche che rendono vulnerabili le apparecchiature elettroniche. Infatti, tutti i pc emettono segnali elettromagentici, regolati da orologi interni; l'attività di elaborazione, così come lo spegnimento o l'accensione del *pc*, regolato dall'orologio di sistema, trasforma il monitor in una sorta di radio trasmittente dei flussi informativi visualizzati dallo schermo, intercettabili via etere da apparecchiature scanner specifiche, rendendo così disponibili i contenuti dell'*hard disk* a terzi. Questo tipo di attività di intercettazione è chiamata attacco *Tempest*.

### f) Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Per la sicurezza informatica dei dati personali trattati appare opportuno prevedere modalità organizzative dirette al salvataggio dei dati (c.d. *backup*) con cadenza almento settimanale.
Il *backup* è di intuitiva importanza specie per chi solitamente usa un *pc* con sistema *windows* collegato alla rete internet.
Infatti, molto spesso accade che il *pc* vada in panne anche per un errore prodottosi nel sistema operativo a causa dell'installazione di un programma che va in conflitto con la struttura del sistema operativo usato nel *pc* (il sistema operativo *windows* può avere delle conformazioni diverse a seconda dei programmi che vengono installati che vanno ad incidere su parti di esso: le c.d. librerie).

[17] Il termine dovrebbe essere l'acronimo di *Transient Electromagnetic Pulse Emanation Standard*;tuttavia alcuni ritengono che trattasi solo di un nome in codice

Nella predisporre l'organizzazione delle procedure di *backup* bisognerà tener conto di operazioni da eseguirsi tra le quali possono suggerirsi le seguenti:

- individuazione del soggetto deputato alle operazioni di *backup*;
- individuazione dei dati da archiviare;
- scelta del supporto di archiviazione;
- fissazione della regola del cambiamento periodico dei supporti di archiviazione;
- etichettatura in modo sicuro dei supporti di archiviazione;
- individuazione di un luogo di conservazione dei dati di *backup*;
- individuazione di ogni eventuale procedura per evitare che quanto archiviato nei supporti possa essere smarrito, danneggiato ovvero reso inutilizzabile;
- scelta della modalità di archiviazione;
- verifica della integrità di quanto verrà archiviato prima della sua archiviazione.

E vivamente consigliato avere delle copie di rispetto non solo dei dati ma anche dei programmi e del sistema operativo. E' opportuno evidenziare che ogni contratto di licenza software consente una o più copie del programma ai fini di operazioni di ripristino.

Pertanto è opportuno che tutti i programmi originali e le copie di rispetto, opportunamente contrassegnate, siano conservate in luogo riservato e in modo tale da poter essere recuperate con facilità al bisogno.

Quanto alle operazione di archiviazione appare opportuno prevedere l'archiviazione periodica, non solo dei dati personali che vengono trattati nello Studio Legale ma, di tutti i dati, *file* o documento necessari per l'esercizio dell'attività professionale. Ad esempio per chi dovesse utilizzare un foglio elettronico per la gestione finanziaria dello Studio è consigliabile fare copie di salvataggio dei relativi *file* per non dover procedere alla rielaborazione della contabilità nell'ipotesi di perdita o malfunzionamento del sistema. Per i *file* di documento (foglio di calcolo; documento; *database* ecc.) si consiglia di salvare il documento con un nuovo nome in modo di averne un clone. Infatti, nell'ipotesi di danneggiamento del *file* sarà possibile recuperare il suo contenuto dal clone.

Sarebbe opportuno che il soggetto deputato alle operazioni di backup sia sempre lo stesso per evitare pericolo di dimenticanze e confusioni.

I supporti di archiviazione possono essere diversi; può utilizzarsi una specifica macchina in rete che funga da server su cui archiviare tutti i dati.

Alcune di queste macchine più evolute sono dotate di più dischi fissi ( hard disk) che, collegati tra loro ed utilizzando una particolare procedura, effettuano una copia dei dati su tutti i dischi in modo da consentire una maggiore sicurezza in caso di danneggiamento di uno dei dischi . Se si sceglie tale soluzione è opportuno che tale macchina sia isolata dal collegamento ad una rete internet. Altri supporti di archiviazione possono essere i *floppy disk*; dischi removibili; cd; dvd; cartucce ecc.

I supporti di archiviazione devono essere etichettati preferibilmente in modo chiaro per evitare che possano essere confusi con altri supporti.

Ci sono diversi tipi di modalità di archiviazione:

**copia integrale** è la copia completa di tutti i dati; richiede un maggiore tempo di archiviazione e si estende anche ai dati non modificati

**copia incrementale** è la copia in nuovo file solo di quelli nuovi e/o modificati rispetto alla copia precedente; i tempi di archiviazione si riducono ma potrebbe essere necessario ricostruire gli archivi attraverso la ricostruzione di tutti i file incrementati

**copia differenziale** è la copia in nuovo file dei soli file nuovi e/o modificati rispetto all'ultima copia completa; richiede un minore tempo di archiviazione ed un minor tempo di archiviazione essendo sufficiente per la ricostruzione usare la copia completa e l'ultima copia differenziata.

Sebbene la copia integrale richieda un tempo maggiore di archiviazione è ritenuta più sicura e comoda, perché necessita di un minor numero di supporti di archiviazione e un minor tempo per la ricostruzione.

I supporti di archiviazione vanno conservati in luogo sicuro e vanno tenuti lontano da fonti di calore e da fonti magnetiche per evitare che possano deteriorarsi fisicamente ovvero smagnetizzarsi. Nell'una e nell'altra ipotesi la ricostruzione potrebbe essere impossibile, e potrebbe essere possibile solo attraverso l'invio dei supporti a centri specializzati con tutte le conseguenze circa la diffusione dei dati.

### Trattamento dei dati personali senza l'ausilio di strumenti elettronici.

Oggi è molto difficile che vi sia uno Studio Legale che non si avvalga di strumenti elettronici. Tuttavia anche nel caso di utilizzazione di strumenti elettronici, i dati personali vengono trattati anche in modalità non informatica. Conseguentemente vanno adottate misure di sicurezza per evitare che i dati vengano manipolati o dispersi.

Le misure suggerite per tali trattamenti si possono riassumere nelle seguenti modalità operative:

a) Aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati o alle unità organizzative.
b) Previsione di procedure per una idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.
c) Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzate all'identificazione degli incaricati.

Appare opportuno ed idoneo stabilire l'obbligo di istruzione degli utenti incaricati al trattamento dei dati personali circa il controllo e la custodia dei dati trattati per l'intero ciclo necessario allo svolgimento dei compiti loro affidati.

E' consigliabile la redazione di un mansionario nel quale siano individuati specificatamente per ogni utente incaricato il tipo di dati da trattare e le modalità del trattamento, ciò anche al fine di fissare i livelli di responsabilità al trattamento dei dati personali.

Dovranno essere fissate delle regole per le modalità di utilizzo del materiale cartaceo contenente i dati personali.

In linea generale, si evidenzia che tutti i fascicoli di uno Studio Legale contengono dati personali sottoposti a trattamento e, conseguentemente, necessitano di cautele e protezione da indebito uso delle informazioni ivi contenute.

Appare opportuno che i fascicoli siano riposti in cassettiere con chiusura a chiave ovvero riposti in una stanza separata dai luoghi di frequentazione del pubblico.

Sotto il profilo operativo si suggerisce l'adozione dei seguenti accorgimenti che hanno natura esemplificativa e non esaustiva:

- individuare un luogo al riparo da un facile accesso di terzi estranei che possa contenere in modo sicuro gli archivi ( le cassettiere, o altri sistemi di raccolta e conservazione dei fascicoli di studio);
- stabilire che l'utente incaricato possa prelevare solo un fascicolo per volta dall'archivio e tutti gli altri fascicoli necessari allo svolgimento dell'incarico affidatogli;
- stabilire che il fascicolo preso dall'archivio dovrà essere utilizzato per il tempo strettamente necessario ai compiti affidati all'utente incaricato;

- stabilire che i fascicoli non potranno essere mai lasciati incustoditi sulle scrivanie;
- stabilire che,nell'ipotesi di ricevimento di clienti o terzi, si provveda a chiudere il fascicolo e nasconderlo alla vista del cliente per evitare che questi possa carpire informazioni sui dati personali di soggetti a lui estranei attraverso la lettura del contenuto del fascicolo lasciato involontariamente aperto;
- dare istruzioni di non effettuare copie fotostatiche dei documenti contenenti dati personali se non nella misura strettamente necessaria all'esercizio del mandato di difesa ricevuto;
- controllare che la fotocopiatrice non abbia in memoria delle copie non ancora elaborate;
- stabilire che le fotocopie mal riuscite non siano usate come carta da appunti e siano distrutte;
- stabilire che la spedizione di originali avvenga con una modalità che possa garantire la sicurezza di ricezione del documento e dei dati ivi contenuti;
- stabilire che tutti gli appunti, le copie dei documenti realizzati e collazionati siano distrutti dopo la stesura dell'originale;
- disporre la distruzione dei documenti con appositi tritadocumenti;
- dare istruzioni, nell'ipotesi in cui sia strettamente necessario che il fascicolo d'ufficio o i documenti ivi contenuti siano portato fuori dallo Studio per l'udienza ovvero per altri motivi, che lo stesso non non sia lasciato incustodito;
- stabilire che nell'ipotesi di colloqui telefonici sia vietato trattare dati personali se non per motivi strettamente connessi con l'esercizio del mandato di difesa ricevuto;
- stabilire che i dati personali non siano oggetto di divulgazione neanche a titolo di esempio in corso di colloqui professionali ed extra-professionali;
- stabilire che l'accesso agli archivi avvenga solo negli orari di ufficio e stabilire regole per l'individuazione dei soggetti abilitati ad accedere agli archivi oltre gli orari di lavoro.

Infine, sarebbe opportuno redigere apposite linee guida comunicate a tutti gli utenti incaricati nella forma di una lettera di incarico.

## Adozione delle misure di sicurezza e quantizzazione dei rischi.

L'adozione delle misure di sicurezza è modulare e va parametrato ai rischi cui è esposta la struttura organizzativa dei sistemi informatici, individuati attraverso la c.d. **quantizzazione dei rischi**.

La quantizzazione del rischio è una tecnica usata da molte aziende per misurare e determinare gli investimenti diretti a prevenire i danni. Nello specifico,la quantizzazione sarà necessaria per prevenire il rischio di perdita o distruzione dei dati personali trattati.

Un criterio da utilizzarsi nella quantizzazione dei rischi potrà essere il seguente:

- **Valutazione dell'impatto e la frequenza di ogni tipo di rischio**
- **Attribuzione di un valore ad ogni tipo di rischio**
- **Valutazione delle misure di sicurezza da adottarsi per la prevenzione dei rischi**
- **Individuazione:**
  **delle misure che rallentano l'intrusione**
  **delle misure che segnalano l'intrusione**
  **delle misure che consentano il tempestivo intervento sul posto.**

Per la quantizzazione di quanto da ultimo indicato si è soliti far ricorso alla seguente formula matematica Tp>>Ta+Ti, laddove Tp=tempo penetrazione delle difese, Ta=tempo di rilevazione intrusione e Ti=tempo di intervento.

Solo dopo aver provveduto ad una quantizzazione dei rischi potranno individuarsi le misure che si intendono adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità, nonchè quelle dirette a garantire l'efficienza della strutture e degli strumenti usati per il trattamento dei dati e delle misure di contenimento e riduzione dei danni (c.d. *contingency planning*) e di intervento di ripristino immediato dei dati a seguito del verificarsi di un evento accidentale di perdita degli stessi (c.d. *disaster recovery*).

## Protezione dei dati personali ed attività di comunicazione

Finora sono stati analizzati i comportamenti e le procedure organizzative dirette a prevenire fenomeni di intrusione ed accessi indesiderati ai dati trattati dal professionista.

Tuttavia, l'attività professionale si estrinseca attraverso la trasmissione di dati , fascicoli ed atti dallo Studio verso l'esterno. In tali casi, se trattasi di atti e documenti che vengono spediti in forma cartacea, l'assunzione delle misure di salvaguardia dei contenuti di quanto spedito o trasmesso, si sostanzia in una serie di comportamentri consolidati e costituenti prassi comunemente accettate, per cui si provvede a trasmettere il plico chiuso in buste protette dalla visione contro luce ed affidate ad uno spedizionere affidato. Analoghi accorgimenti devono essere assunti allorquando si

provvede a trasmettere un plico in formato digitale; non appare opportuno affidarsi ai normali canali di comunicazione via internet ovvero affidarsi a canali collettivi come la chat di *Facebook.* Infatti, le trasmissioni via internet possono essere facilmente intercettate da malintenzionati che possono acquisire i contenuti trasmessi[18]. Appare preferibille affidarsi a canali sicuri di comunicazione. Alcuni server di posta elettronica utilizzano per le comunicazioni sicure il protocollo *HTTPS*[19] alla stregua dei siti di *e-commerce*. L'invio attraverso tali canali web sono ritenuti sicuri perché utilizzano porte di comunicazione più controllate e meno vulnerabili rispetto alla comune porta c.d. *know port tcp80*[20]. Tuttavia, laddove ci sia serviti di un protocollo di trasmissione sicura, potremmo avere la necessità di evitare che alcuni contenuti digitali cadano nelle mani sbagliate o che siano visionati da soggetti non qualificati[21]. In tali casi l'invio attraverso un canale di comunicazione sicuro non esclude che, per es. la segretaria dello Studio possa aprire il contenuto digitale e visionarlo con pericoli circa la diffusione dei dati che vorremmo mantenere segreti. Per ovviare a tale pericolo dovremmo utilizzare le stesse modalità di cautela di un plico inviato a mezzo di un vettore qualificato ed affidabile che provvederà alla consegna del plico solo alla persona interessata e non ad altri. In questo caso potremmo avvalerci di programmi di crittografia dei contenuti digitali[22] ovvero ci si può avvalere di programmi di steganografia[23], quali *Puff*.

## Conclusioni.

Gli sviluppi tecnologici determinano la necessità di ripensare il modo tradizionale di gestione dell'attività professionale.

La particolare attenzione delle normative internazionali e nazionali alla protezione dei dati personali impone delle scelte determinanti volte a mutare la cultura della sicurezza.

---

[18] Alcune tecniche di intrusione nei canali di comunicazione quali il *man-in-the-middle* o il *session hijacking* consentono l'intromissione nel flusso veicolare di dati nella rete e permettono di prendere visione dei contenuti digitali trasmessi, eventualmente alterarli e ritrasmetterli senza lasciare tracce.

[19] La sigla è l'acronimo di ***H**yper **T**ext **T**ransport **P**rotocol **S**ecure*

[20] Le c.d. *know ports* sono quelle assegnata dallo IANA ((***I**nternet **A**ssigned **N**umbers **A**uthority*) e costituiscono i protocolli standard di comunicazione

[21] Si pensi all'invio di un contenuto digitale ostensibile di dati genetici delicati perché riferentesi ad indagine difensiva penale e la cui diffusione anche involontaria potrebbe pregiudicare gli interessi del cliente.

[22] La crittografia è una modalità per offuscare un testo in modo da renderlo comprensibile solo a chi possiede la chiave di decifrazione: famoso è il c.d. Cifrario di Cesare che trasponeva di tre lettere il contenuto del testo in modo da renderlo all'apparenza incomprensibile. La crittografia digitale si avvale di chiavi di decifrazione di tipo informatico attraverso algoritmi matematici; la firma digitale è la forma più nota di strumento di crittografia digitale.

[23] L'algoritmo di steganografia, a differenza di quello crittografico, elabora all'interno di una forma comune visibile che non desta sospetti, quale una immagine o un *file* audio, un contenuto nascosto e visibile solo al destinatario in possesso della chiave di decrittazione del documento elaborato.

Il cambiamento di prospettiva deve essere il frutto di una scelta consapevole ed interiorizzata perché, per quanto si possano assumere tutte le cautele e le misure di sicurezza più idonee al passo con gli sviluppi tecnologici, la predisposizione psicologica rappresenta la pietra angolare su cui tutte le scelte operative programmatiche devono essere assunte.

Le politiche di sicurezza e le conseguenti scelte operative non devono essere considerate come inutili oneri; al contrario devono costituire il metro di valutazione di modelli comportamentali virtuosi che si traducono in referenze di qualità nell'esercizio della professione. Non sfugga che molti Studi Legali si propongono per ottenere la Certificazione di Qualità, ed il requisito dell'adozione di misure di sicurezza per la protezione dei dati e dei contenuti affidati dai clienti rappresenta un elemento di valutazione positiva per l'ente certificatore al quale ci si è rivolti per ottenerla.

L'imprenscindibile adozione di una strategia di sicurezza a tutela dei dati personali si pone in sintonia con la elevazione, a livello normativo, del diritto alla *privacy* dell'individuo assurto a valore primario di rango costituzionale.
Richiamo sul punto la comunicazione 251 della Commissione dell'UE del 31 maggio 2006: *A strategy for a Secure Information Society*, seguita dalla Risoluzione del Consiglio in data 22 marzo 2007[24] che, per rimanere nel tema, tra l'altro ha elaborato raccomandazioni dirette: a *sostenere i programmi di formazione e migliorare la sensibilizzazione della pubblica opinione ai temi della sicurezza delle reti e dell'informazione;* a *prestare la dovuta attenzione alla necessità di prevenire e combattere minacce nuove o esistenti alla sicurezza di reti di comunicazione elettronica, comprese l'intercettazione e l'utilizzazione illegale di dati*

Alla luce di quanto esposto, se il dato personale è un valore di libertà dell'individuo, e le misure di sicurezza costituiscono uno strumento di tutela di tale valore, entrambi si pongono tra loro in un rapporto sinergico a corrispondenza biunivoca che esprime così nel suo insieme una scelta di giustizia perché *giustizia non esiste là dove non vi è libertà*[25].

Francesco Tedeschi

[24] Risoluzione 2007/C 68/01 pubblicata sulla Gazzetta Ufficiale dell'UE del 24 marzo 2007
[25] Luigi Einaudi *Il buongoverno: saggi di economia e politica (1897-1954)*, Laterza, 1954

*Per scaricare l'articolo in formato pdf*