

## **Indice**

- **Nuova normativa in materia di Privacy;**
- **Pericoli per la privacy digitale;**
- **Tutto quello che devi sapere;**
- **Sentenze;**
- **Informativa e consenso al trattamento;**
- **Sicurezza informatica;**
- **Lettera di incarico;**
- **Sopraluogo;**
- **Adeguamento sicurezza informatica: l'offerta.**

## Nuova normativa in materia di Privacy

Illustrare la nuova legge sulla Privacy significa affrontare il primo indispensabile passo per essere in regola e rendere sicuri i dati personali. Secondo la nuova normativa, infatti, a breve ogni impresa sarà tenuta a dotarsi di adeguati sistemi di sicurezza informatica tesi all'assoluto rigore nel trattamento delle informazioni e dei dati sensibili.

A disposizione le soluzioni tecnologiche per adempiere agli obblighi di legge in modo rapido e indolore. Le ultime versioni dei sistemi operativi Microsoft Windows XP per il sistema client e Small Business Server 2003 per il sistema server, congiuntamente con Microsoft Office 2003, offrono le misure idonee per la sicurezza dei sistemi informatici.

I programmi che fanno bloccare i computer, che non sono aggiornabili e non dispongono dei requisiti per poter usufruire dell'assistenza tecnica sortiscono l'effetto contrario. Provocano un senso di frustrazione nei dipendenti e fanno perdere loro del tempo prezioso.

Il "Codice in materia di protezione dei dati personali" (DL n. 196 del 30/6/2003), in vigore dal 1° Gennaio 2004, riforma interamente la disciplina sulla privacy. Il Codice abroga e sostituisce tutte le precedenti leggi, decreti e regolamenti in materia, riunendo in un unico organico contesto l'intera normativa sulla privacy.

Aziende, imprese, ditte, studi professionali, banche, assicurazioni, e tutte le altre categorie, private e pubbliche, sono tenute ad operare nel rispetto di precise regole che riguardano la sicurezza dei dati e dei sistemi al fine di ridurre al minimo le fonti di rischio e garantire correttezza, integrità e aggiornamento delle informazioni. Tra le misure richieste alcune sono definite minime e altre più ampie, o "idonee". Le prime sono di tipo tecnico, informatico, organizzativo, logistico e procedurale, le seconde sono invece decise in autonomia dal titolare, in relazione alle proprie specificità. La mancata adozione di entrambe comporta delle sanzioni. Il risultato dovrebbe essere la realizzazione di un vero e proprio sistema di sicurezza che protegga i dati custoditi all'interno dell'azienda. Altra novità è l'importanza assunta dal Documento Programmatico annuale per la sicurezza, che dovrà essere allegato al bilancio della società e aggiornato ogni anno.

### Vediamo i punti chiave

- **Finalità della 196:** proteggere i dati personali di chiunque
- **Chi deve applicarla:** tutte le Imprese e i Professionisti
- **Le misure:** ci sono misure obbligatorie per tutti e misure specifiche per chi gestisce dati sensibili e giudiziari (avvocati e commercialisti) o per chi svolge attività particolari (ad esempio) professioni sanitarie
- **La tipologia di misure:** Informatiche, logistiche, procedurali
- **Le sanzioni:** penali per chiunque ometta di adottare o applicare le misure minime previste e civili per chi procuri un danno da inadempienza
- **Documento Programmatico:** entro il 30 giugno 2005 le imprese devono compilare o aggiornare un Documento Programmatico sulla Sicurezza (DPS), cioè un manuale in cui descrivere la situazione attuale e gli interventi che l'impresa intende realizzare per adeguarsi alla nuova normativa.
- **Data di ultima attivazione:** 30 giugno 2005
- **Data ultima di entrata in vigore:** 1° gennaio 2006

## Pericoli per la privacy digitale

Sappiate che esiste la possibilità che qualcuno si sia intromesso nei vostri dati personali. Se l'ha fatto, è probabile che abbia dato un'occhiata al vostro conto bancario in linea.

È emblematico il caso di un "ladro di identità" attualmente in carcere. Per un paio d'anni questo delinquente ha installato di nascosto nei computer pubblici software in grado di registrare le sequenze di tasti digitate dagli utenti. In questo modo, registrava nomi utente e password che quindi rivendeva in Internet o utilizzava per rubare denaro.

È stato scoperto mentre utilizzava il personal computer di una delle vittime che al momento si trovava a casa. Incredula, la donna fu in grado di osservare come il ladro informatico esaminasse metodicamente l'intero contenuto del suo computer utilizzando GoToMyPC, un software che consente di utilizzare il computer in modalità remota quando ci si trova in viaggio. La vittima aveva usato GoToMyPC da una macchina pubblica. Jiang aveva rubato il suo nome utente e la sua password.

Ciò porta alla luce un problema in genere sottovalutato. I software spia possono facilmente essere installati nei computer pubblici, come quelli che si trovano in Internet café, aeroporti, biblioteche e altri luoghi pubblici.

Questo tipo di software consente di impossessarsi di password e nome utente di chi utilizza il computer. Il rischio è quello di essere derubati di denaro o della propria identità digitale. Queste informazioni dovrebbero essere sufficienti per persuadervi ad adottare alcune precauzioni nell'uso di terminal PC pubblici.

### **Il software è invisibile all'utente**

Per questi scopi vengono in genere utilizzati programmi software che sono invisibili all'occhio non esperto. Vi sono anche dispositivi hardware che svolgono essenzialmente la stessa funzione, se vengono posti tra tastiera e computer, ma attirano troppo l'attenzione per essere utilizzati in postazioni pubbliche.

I programmi software invece possono registrare passo per passo e in modo discreto la sequenza dei tasti utilizzati dalla vittima e inviare quindi tramite posta elettronica le informazioni raccolte in un momento prestabilito. In alternativa, il malintenzionato potrà scaricare i dati registrati. Altri programmi software registrano delle istantanee dei siti visitati e inviano i dati tramite posta elettronica.

Come ho detto, i programmi spia agiscono in modo invisibile all'utente. A meno che non si sappia esattamente dove e come cercarli, trovarli è impossibile. Prima di utilizzare il computer, è consigliabile verificare che non contenga software spia (nel modo spiegato in seguito).

Tuttavia, ci sono altri potenziali pericoli, oltre ai programmi spia. Usare un computer pubblico è un'operazione veramente rischiosa!

Ecco cinque cose da ricordare prima di usare un computer sconosciuto:

### **Verificate che non contenga programmi spia**

Scaricate X-Cleaner Spyware Remover da [spywareinfo.com](http://spywareinfo.com) e copiatelo su un disco floppy. Se il computer pubblico che utilizzate dispone di unità floppy, inserite il disco ed eseguite X-Cleaner per controllare il disco rigido. Non è necessario installare X-Cleaner.

## **Cancellate le vostre tracce**

I browser Internet tengono traccia delle pagine visitate. Al termine dell'esplorazione con Microsoft Internet Explorer, fate clic su Strumenti > Opzioni Internet. Nella scheda Generale fate clic su Elimina file e Elimina cookie, quindi scegliete Cancellazione Cronologia. Se utilizzate Netscape Navigator, la procedura è leggermente più complessa.

- Controllate le impostazioni prima di attivare la connessione. Fate clic su Edit e Preferences. Fate clic sulla freccia accanto a Navigator e selezionate History. Sulla destra, in Browsing History, impostate "Remember visited pages" su 0.
- Fate clic sulla freccia accanto a Privacy and Security, quindi su Cookies. Selezionate Disabile Cookies e Disabile Cookies in Mail and Newsgroups.
- Al termine dell'esplorazione, fate clic su Edit e su Preferences. Fate clic sulla freccia accanto a Navigator e quindi su History. Fate clic su Clear History e Clear Location Bar. Sul lato sinistro, in Privacy and Security, fate clic sulla freccia. Selezionate Cookies e fate clic su Manage Stored Cookies. Nella scheda Stored Cookies fate clic su Remove All Cookies.
- In Advanced, nel riquadro di sinistra, fate clic sulla freccia e quindi su Cache. Selezionate Clear Memory Cache e Clear Disk Cache.

## **Protegete le vostre password**

I browser memorizzano anche le password. Prima di attivare la connessione, in Internet Explorer scegliete Strumenti > Opzioni Internet. Nella scheda Contenuto fate clic su Completamento automatico e deselezionate le quattro caselle di controllo presenti.

Al termine dell'esplorazione, scegliete nuovamente Strumenti > Opzioni Internet. Nella scheda contenuto fate clic su Completamento automatico e selezionate Cancella moduli e Cancella password.

In Netscape fate clic su Edit e Preferences. Fate clic sulla freccia accanto a Privacy and Security. Fate clic su Passwords. Deselezionate la casella Remember Passwords. Al termine dell'esplorazione, fate nuovamente clic su Passwords in Privacy and Security. Fate clic su Manage Stored Passwords, selezionate la scheda Passwords Saved e fate clic su Remove All.

Netscape utilizza una funzione simile al completamento automatico di Internet Explorer, che salva i dati immessi nei moduli. Per disattivarla, in Privacy and Security fate clic su Forms. Deselezionate "Save form data from Web pages when completing forms". Al termine dell'esplorazione, tornate alla pagina Forms. Fate clic su Manage Stored Form Data e quindi su Remove All Saved Data.

Eliminando i dati dal browser si può essere certi che nessuno possa risalire ai siti visitati

o alle password con dati salvati. Tuttavia, le password possono comunque essere rilevate da un programma di registrazione delle sequenze di tasti.

Alcuni programmi di registrazione delle sequenze dei tasti, anche se non tutti, possono essere ingannati semplicemente inserendo le lettere e i numeri della password tramite una procedura di copia e incolla. Ad esempio, se la pagina visualizzata sul browser contiene testo e la vostra password è "Dodo", sarà sufficiente individuare le lettere "d" e "o" sulla pagina, copiarle e incollarle nella casella della password.

Probabilmente, il modo migliore per proteggere le password è quello di utilizzare password temporanee durante il viaggio e quindi modificarle.

## **Non fidatevi della crittografia**

Sul mercato sono disponibili numerosi software di crittografia, che possono essere utilizzati per crittografare i messaggi di posta elettronica. Tuttavia, il messaggio viene crittografato quando si preme il pulsante di invio. Se sul computer è installato un programma per la registrazione delle sequenze di tasti, la crittografia è inutile, in quanto password e testo vengono registrati durante la digitazione.

## **Fate affidamento sul buon senso**

I computer pubblici possono essere sicuri, ma non c'è modo di esserne certi. Sul computer di casa o dell'ufficio è possibile implementare tutte le misure di protezione necessarie, ma non si può essere certi della configurazione di una macchina pubblica.

## **Attenzione**

Trattate sempre con cautela queste macchine. Se potete, evitate di utilizzarle per eseguire operazioni bancarie, compravendita di azioni o transazioni con carta di credito. Se dovete controllare la posta elettronica, utilizzate una password temporanea e chiedete all'amministratore di sistema come impostare le pagine in modo che dopo un certo tempo non sia possibile tornare alla visualizzazione precedente.

Se vi limitate a esplorare Internet, non dovrebbero esserci problemi. Evitate però, se possibile, di trattare questioni delicate

### **Tutto quello che devi sapere su pirati, virus informatici e attività dolose:**

Il tempo è prezioso. La vita è troppo breve per preoccuparsi dei computer. Siamo d'accordo. Ma per riconoscere le minacce esistenti e scoprire come affrontarle è necessario avere un minimo di conoscenze tecniche. Non è il caso di preoccuparsi, ci limiteremo allo stretto indispensabile.

### **Reti inter-reti e internet**

Il computer in sé è qualcosa di straordinario, una meraviglia tecnologica. Ma il suo punto di forza sta nel consentire la comunicazione. Basta collegare tra di loro due o più computer mediante schede di rete e cavi (o attraverso una configurazione senza fili) per ottenere una rete locale, o LAN (Local Area Network). Tutti i computer connessi in rete possono condividere dati e sistemi di posta elettronica, nonché accedere a risorse condivise come stampanti, modem o connessioni a Internet a banda larga. Collegando tra di loro due o più LAN si ottiene una rete remota, o WAN (Wide Area Network). Per esempio, attraverso una linea dedicata è possibile collegare tra di loro due uffici ubicati in luoghi diversi.

Collegando tra di loro più reti si ottiene una inter-rete. Le informazioni contenute in un computer connesso a una rete qualsiasi possono essere trasmesse a qualsiasi altro computer connesso a qualsiasi altra rete tramite l'inter-rete, che funge da portante comune. Una inter-rete può essere descritta come una rete autostradale che collega i diversi sistemi in vari locali.

Internet non è altro che una inter-rete a livello mondiale. Tutti i computer connessi a Internet comunicano tramite protocolli standard, cosicché le informazioni trasmesse da qualsiasi computer connesso possono essere ricevute da tutti gli altri. E qui iniziano i problemi: finché non ci si connette a una rete pubblica si è relativamente al sicuro da minacce esterne. Attivare un collegamento a Internet, d'altro canto, equivale a rendere pubblici il proprio nome, indirizzo e numero di telefono e a dichiarare di possedere uno o più computer.

### **Pacchetti**

In genere, le informazioni viaggiano attraverso le reti sotto forma di pacchetti. Per pacchetto si intende un insieme di dati corredati da un indirizzo e da altre informazioni che consentono alle reti di inviarli dove richiesto. Tutto ciò che viaggia su Internet viene suddiviso in pacchetti: pagine Web, messaggi e-mail, file scaricabili, ecc... È un po' come organizzare il trasporto di un circo: è impensabile cercare di trasportare l'intero circo in un unico veicolo. È necessario suddividerlo in veicoli separati, informare ciascuno di essi sulla rispettiva destinazione e, una volta arrivati, provvedere a ricomporre il circo. Così come i veicoli sulle strade, i pacchetti sono fisicamente connessi e si spostano a flussi. I dati più voluminosi sono suddivisi in una serie di pacchetti e ricomposti una volta arrivati a destinazione. Durante la Trasmissione in Internet, i pacchetti sono effettivamente esposti a "orecchie indiscrete".

### **Porte e indirizzi**

A ciascun computer collegato in rete viene assegnato un numero univoco, denominato indirizzo IP. L'indirizzo IP definisce in modo univoco un computer in rete e fornisce ai pacchetti di dati tutte le informazioni necessarie perché giungano a destinazione. Gli indirizzi IP possono essere

considerati alla stregua di indirizzi stradali. Una parte dell'indirizzo indica il segmento di rete del computer di destinazione, mentre l'altra identifica il computer vero e proprio.

Come abbiamo visto, l'indirizzo IP si riferisce al computer e al segmento di rete su cui esso si trova, ma non basta. È necessario che anche le applicazioni installate sul computer in questione possano essere identificate. Si pensi al numero di un appartamento compreso in un indirizzo stradale: l'indirizzo stradale indica l'edificio in cui si trova l'appartamento, mentre il numero indica l'appartamento vero e proprio. Allo stesso modo, l'indirizzo IP indica il computer, mentre il numero della porta indica il programma installato sul computer. A tutti i programmi installati su un computer che devono inviare e ricevere dati in rete viene assegnato un determinato numero di porta. Quando i pacchetti di informazioni vengono ricevuti in corrispondenza di un dato numero di porta, il computer è in grado di identificare l'applicazione che riceve il pacchetto. Ad esempio, la porta 80 è la porta dei server Web (ovvero i server che ospitano i siti Web che si consultano tramite il browser), mentre la porta 25 viene utilizzata per l'invio di messaggi e-mail. I pacchetti vengono dunque indirizzati a una porta specifica presso uno specifico indirizzo IP.

## Firewall

I firewall vengono utilizzati per bloccare il traffico di rete attraverso le porte specificate. In questo modo, il computer dotato di firewall può comunque accedere ai servizi presenti su altri computer, ma non viceversa. Alcuni firewall esaminano i pacchetti in entrata e talvolta quelli in uscita dalla rete per assicurarsi che siano autentici e bloccano quelli sospetti. Inoltre, i firewall nascondono le identità dei computer interni alla rete aziendale per evitare che i pirati informatici possano prendere di mira macchine singole.

## Server

Un server non è altro che un computer collegato alla rete, ma che assolve delle funzioni specifiche, quali condividere una stampante, memorizzare file o rendere disponibili le pagine Web. Anche i notebook o i desktop connessi a Internet in un certo senso possono essere considerati dei server e, in mancanza di firewall, sono esposti alla ricezione di traffico indesiderato dal Web.

## Virus, worm, Trojan Horse, spamming e falsi messaggi

Tramite la posta elettronica ogni anno vengono inviati miliardi di messaggi, molti dei quali, purtroppo in numero sempre maggiore, sono da considerare pericolosi. Nell'agosto 2003, un'azienda produttrice di sistemi di protezione e-mail analizzò 413 milioni di messaggi. Il 3% conteneva un virus, il 52% era posta indesiderata e in gran parte dei casi conteneva un'immagine pornografica. Le principali minacce diffuse attraverso la posta elettronica sono cinque:

- **Virus**, ovvero programmi concepiti per replicarsi e, potenzialmente, arrecare danno. Spesso vengono nascosti all'interno di programmi innocui. All'interno dei messaggi e-mail, i virus spesso si camuffano da giochi o immagini e ricorrono a oggetti ingannevoli (ad esempio: "Foto della mia ragazza nuda") per invogliare gli utenti ad aprirli ed

eseguirli. I virus cercano di replicarsi infettando gli altri programmi installati sul computer.

- **Worm**, simili ai virus ma, anziché infettare i programmi installati su un computer, sono in grado di inviare dei messaggi e-mail al fine di replicarsi.
- **Trojan Horse**, ovvero programmi dannosi che si camuffano da applicazioni innocue. A differenza di virus e worm, non sono in grado di replicarsi ma sono comunque in grado di causare danno. Virus e worm vengono spesso occultati all'interno di un Trojan Horse.
- **Spamming o messaggi di posta elettronica indesiderati**, che utilizzano grandi quantità di larghezza di banda e causano notevoli perdite di tempo. Il volume complessivo dello spamming è spesso impressionante e può costituire un veicolo per la diffusione di virus. Generalmente, si tratta di messaggi sessualmente espliciti, che possono creare un ambiente di lavoro oppressivo e causare potenziali responsabilità legali qualora le aziende non si attivino per arginare il fenomeno.
- **Falsi messaggi di posta elettronica**, quali avvertimenti fasulli sui virus, catene o improbabili offerte gratuite sono solo una perdita di tempo per chi legge. Inoltre, i falsi messaggi di posta elettronica spesso contengono virus o Trojan Horse.

### **Motivi della vulnerabilità del software**

Non è certo nelle intenzioni degli sviluppatori scrivere programmi software non sicuri. Un sistema operativo, ad esempio, è il prodotto di decine di migliaia di ore di lavoro ed è costituito da milioni di righe di codice. Una semplice svista o un bug possono fornire un punto di accesso inatteso ad un sistema altrimenti sicuro. Sviluppare software totalmente privo di bug è impossibile. Certo, ciò non significa che non si debba comunque continuare a tentare.

Ci sono poi i malintenzionati. Willie Sutton, svaligiatore di banche di professione, dichiarò: "Rapino le banche perché è lì che si trova il denaro". Per i programmi software è esattamente lo stesso. Più un programma software è conosciuto e diffuso, più sarà oggetto di attacchi informatici.

Vi è una continua lotta tra hacker, che cercano di sfruttare qualunque punto debole esistente, e sviluppatori, che tentano di eliminarli. È esattamente quanto accade tra fabbricanti di serrature e scassinatori o tra produttori di sistemi di allarme e ladri d'auto. Ecco perché gli sviluppatori di software rilasciano aggiornamenti per l'eliminazione dei punti deboli conosciuti e perché è sempre consigliabile installare tali aggiornamenti.

### **Minacce comuni alla protezione delle reti**

Le motivazioni degli hacker sono di varia natura (profitto, dolo, gloria), ma le loro modalità operative sono simili. Vi sono diversi tipi di minacce, ciascuna delle quali ha infinite varianti:

- **Spoofing**. Lo spoofing si manifesta in modi diversi. Lo spoofing degli IP consiste nella creazione di pacchetti che sembrano provenire da un indirizzo IP diverso da quello effettivo. Si tratta di una tecnica utilizzata principalmente nel caso di attacchi unilaterali (per esempio gli attacchi DoS). Infatti, se i pacchetti sembrano provenire da un

computer presente nella rete locale, possono tranquillamente attraversare la protezione del firewall, concepita per difendere la rete da attacchi esterni. Gli attacchi condotti attraverso lo spoofing degli indirizzi IP sono difficili da individuare e richiedono tutta l'abilità e i mezzi necessari per monitorare e analizzare i pacchetti di dati. Lo spoofing della posta elettronica, invece, consiste nel comporre un messaggio e-mail il cui campo Da non indica l'effettivo indirizzo del mittente. Ad esempio, verso la fine del 2003 circolava su Internet una serie di messaggi e-mail fasulli che sembravano contenere un annuncio ufficiale di aggiornamenti alla protezione da parte di Microsoft e che contenevano un falso indirizzo e-mail Microsoft.

- **Manomissione.** La manomissione consiste nel modificare il contenuto dei pacchetti durante la loro trasmissione in Internet oppure nel modificare i dati memorizzati sui dischi rigidi dei computer dopo che la rete è stata violata. Per esempio, un hacker potrebbe posizionare una presa su una rete per intercettare i pacchetti in uscita e accedere alle informazioni o alterarle quando lasciano la rete aziendale.
- **Disconoscimento.** Il disconoscimento indica la capacità di un utente di negare, mentendo, di avere commesso azioni che è impossibile provare altrimenti. Per esempio, un utente che abbia eliminato un file può facilmente negare di essere il responsabile in mancanza di meccanismi di controllo che possano provare il contrario.
- **Divulgazione di informazioni.** La divulgazione di informazioni consiste nell'espone informazioni a individui che normalmente non vi avrebbero accesso.
- **Attacchi DoS (Denial of Service).** Gli attacchi DoS sono assalti informatici lanciati da un attacker allo scopo di sovraccaricare o interrompere un servizio di rete, ad esempio un server Web o un file server. Ad esempio, a seguito di un attacco DoS un server potrebbe essere così impegnato a rispondervi da ignorare le richieste di connessione legittime. Nel corso del 2003 sono stati organizzati imponenti attacchi DoS contro diverse grandi aziende su Internet, tra cui Yahoo e Microsoft, nel tentativo di intasare i server.
- **Elevazione dei privilegi.** L'elevazione dei privilegi è un procedimento mediante il quale un utente induce un sistema a concedere diritti non autorizzati, generalmente allo scopo di danneggiare o distruggere il sistema. Ad esempio, un hacker potrebbe accedere a una rete attraverso un account guest, quindi individuare un punto debole del software che gli consenta di modificare i suoi privilegi da guest a amministratore.

Gli hacker generalmente sfruttano a loro vantaggio la capacità di elaborazione dei computer, utilizzando un virus per sferrare un attacco DoS a centinaia di migliaia di computer contemporaneamente oppure facendo uso di un programma per l'identificazione delle password per individuare quella corretta tra tutte le parole di senso compiuto. Le prime password che verificano sono ovviamente "password", "accesso" e le password che coincidono con il nome utente. Dispongono di programmi in grado di sondare a caso tutti gli indirizzi IP presenti su Internet per individuare sistemi non protetti. Quando ne trovano uno, grazie ai programmi di scansione delle porte cercano di individuarne una aperta cui sferrare l'attacco. Se ne trovano una, consultano la libreria dei punti deboli più conosciuti per trovare il modo di accedere al sistema. Nel caso di attacchi più mirati (ad esempio nei casi di spionaggio industriale) il metodo più efficace è costituito dal connubio tra tecnologia e ingegneria sociale. Esempi di questo metodo sono: indurre membri del personale a rivelare informazioni di natura confidenziale,

esaminare i cestini della carta straccia alla ricerca di informazioni importanti o semplicemente controllare i bigliettini affissi ai monitor per scoprire le password.

## Sentenze

Nel "trattamento di dati personali" consistente nella diffusione di informazioni a scopo di cronaca giornalistica, soggetto tutelato dalla legge sulla privacy e legittimato alla proposizione del ricorso al garante è soltanto colui di cui l'informazione giornalistica obiettivamente riferisca; colui che, comunque, identificato o identificabile (ancorchè, per avventura, in modo inappropriato e, magari, interferente con altrui diritti) costituisca l'effettivo termine di riferimento della notizia propalata.

### **Trib. Milano, 14/10/1999**

L'interesse conoscitivo dell'esponente sindacale, per quanto attiene alle determinazioni amministrative riguardanti la categoria professionale che egli rappresenta a seguito di mandato ricevuto, deve ritenersi prevalente su quello alla "privacy" dei singoli dipendenti destinatari di detti provvedimenti, il cui diritto alla riservatezza trova peraltro adeguata tutela nel divieto per l'esponente sindacale di dare pubblicità ai dati ricavabili dalla documentazione ottenuta in visione e riflettenti la sfera giuridica e patrimoniale di ciascuno di essi e nella responsabilità personale che egli assume nel caso di violazione di detto divieto.

### **T.A.R. Puglia Bari, Sez.I, 27/11/2002, n.5206**

L'art. 16 comma 2 d.lg. 11 maggio 1999 n. 135, recante disposizioni integrative della l. 31 dicembre 1996 n. 675 sul trattamento di dati sensibili da parte di soggetti pubblici, nello stabilire che il relativo trattamento "è consentito se il diritto da far valere o difendere, di cui alla lett. b) del comma 1, è di rango almeno pari a quello dell'interessato", rimette la soluzione del contrasto tra il diritto di accesso e quello alla riservatezza alla ponderazione comparativa da effettuarsi in concreto, in primo luogo, dall'amministrazione ed eventualmente, in sede di controllo, dal giudice amministrativo adito ai sensi dell'art. 25 l. 7 agosto 1990 n. 241; tale valutazione comparativa può comportare che il diritto posto a base della istanza ostensiva, pur in astratto subvalente rispetto a quello della riservatezza, risulti in concreto prevalente su quest'ultimo, in considerazione del grado minimo di effettivo coinvolgimento della dignità e della privacy dell'interessato.

### **T.A.R. Lazio Latina, 15/11/2002, n.1179**

L'art. 16 comma 2 d.lg. 11 maggio 1999 n. 135, recante disposizioni integrative della l. 31 dicembre 1996 n. 675 sul trattamento di dati sensibili da parte di soggetti pubblici, nello stabilire che il relativo trattamento "è consentito se il diritto da far valere o difendere, di cui alla lett. b) del comma 1, è di rango almeno pari a quello dell'interessato", rimette la soluzione del contrasto tra il diritto di accesso e quello alla riservatezza alla ponderazione comparativa da effettuarsi in concreto, in primo luogo, dall'Amministrazione ed eventualmente, in sede di controllo, dal giudice amministrativo adito ai sensi dell'art. 25, l. 7 agosto 1990 n. 241; tale valutazione comparativa può comportare che il diritto posto a base della istanza ostensiva, pur in astratto subvalente rispetto a quello della riservatezza, risulti in concreto prevalente su quest'ultimo, in considerazione del grado minimo di effettivo coinvolgimento della dignità e della "privacy" dell'interessato.

### **T.A.R. Lazio Latina, 15/11/2002, n.1179**

Alla disvelazione dei dati relativi allo stato di salute è consentito addivenire solo nei casi in cui gli interessi adottati dall'impresa siano tali da giustificare un "vulnus" della

riservatezza del dipendente, il quale ha diritto a che i propri dati sensibili, protetti dalle norme sulla privacy, non siano divulgati per soddisfare esigenze prospettate sulla semplice eventualità di dover apprestare, in presenza di determinati eventi, tutti ancora da verificare, la difesa di diritti neppure posti in discussione, occorrendo invece accertare lo spessore dell'interesse dedotto dall'impresa nel concreto suo atteggiarsi in ordine al procedimento amministrativo "de quo".

**Cons. Stato, Sez. VI, 26/02/2002, n.2542**

L'obbligo di cooperazione gravante sul datore di lavoro a norma dell'art. 21 dello statuto dei lavoratori presuppone che il referendum sia indetto da tutte le rappresentanze sindacali; per conseguenza è inopponibile al datore di lavoro un accordo unitario stipulato fra le organizzazioni sindacali aziendali il quale stabilisca che le decisioni relative ad atti negoziali delle r.s.u. sono assunte a maggioranza dei componenti; da ciò ulteriormente consegue che il datore di lavoro non è tenuto a fornire al sindacato i nominativi dei propri dipendenti al fine dello svolgimento del referendum non indetto ai sensi dell'art. 21. La comunicazione dei dati personali dei dipendenti è, peraltro, vietata dalla normativa sulla "privacy" introdotta dalla l. n. 675 del 1996.

**Trib. Cassino, 12/07/2001**

In materia sanitaria, il giudizio di comparazione fra esigenze di accesso agli atti e tutela della riservatezza personale deve assumere quali parametri di riferimento la rilevanza giuridica dell'interesse rispetto al quale è strumentale l'accesso documentale, e la sua imprescindibile necessità per la difesa di quell'interesse, che rappresenta il limite entro il quale l'accesso è consentito, oltre che la condizione per la prevalenza sulla tutela della "privacy".

T.A.R. Emilia-Romagna Bologna, Sez.I, 17/12/2001, n.1207 In materia sanitaria, il giudizio di comparazione fra esigenze di accesso agli atti e tutela della riservatezza personale deve assumere quali parametri di riferimento la rilevanza giuridica dell'interesse rispetto al quale è strumentale l'accesso documentale, e la sua imprescindibile necessità per la difesa di quell'interesse, che rappresenta il limite entro il quale l'accesso è consentito, oltre che la condizione per la prevalenza sulla tutela della "privacy".

**T.A.R. Emilia-Romagna Bologna, Sez.I, 17/12/2001, n.1207**

Il diritto di accedere alla documentazione amministrativa al fine della tutela di un interesse giuridico non prevale di norma sul diritto alla riservatezza in materia riguardante lo stato di salute del terzo, ma ai sensi dell'art. 16 comma 2, l. 11 maggio 1999 n. 135, è invece rimesso alla prudente comparazione dell'amministrazione il giudizio di prevalenza dell'interesse alla tutela giurisdizionale (mediante previo accesso) rispetto al diritto del terzo alla tutela della "privacy" personale.

**Cons. Stato, Sez. VI, 30/03/2001, n.1882**

I dati relativi alla prestazione di lavoro straordinario sono dati personali rappresentando una informazione relativa ad una persona fisica identificata. Senza il consenso degli interessati non possono essere comunicati alle organizzazioni sindacali poiché la legge sulla privacy - incentrata sul controllo individuale dell'interessato sulla circolazione del dato personale - non conferisce alcun rilievo ai diritti sindacali nascenti dal contratto collettivo.

**App. Torino, 13/03/2001**

Nell'ambito di un unico immobile condominiale le norme che regolano i rapporti di vicinato trovano applicazione solo in quanto compatibili con la struttura dell'edificio e con le caratteristiche dello stato dei luoghi. Pertanto, qualora esse siano invocate in una

controversia tra condomini, spetta al giudice del merito valutare se, nel singolo caso, dette norme debbano essere osservate o meno, in considerazione dell'esigenza di contemperare i diversi interessi di più proprietari conviventi in un unico edificio, al fine dell'ordinato svolgimento di tale convivenza, propria dei rapporti condominiali. (Nella specie la Corte di cassazione, applicando tale principio, ha rigettato il ricorso avverso la pronuncia del giudice di merito che aveva ritenuto legittima la tettoia in lamiera di una tenda parasole (quest'ultima conforme al tipo e colore previsti dal regolamento condominiale) installata da un condomino, ritenendola necessaria - nel caso concreto - per la tutela della sua privacy e per il riparo dagli agenti atmosferici, nonostante fosse di dimensioni maggiori rispetto a quella di analoghi manufatti di altri condomini, provocasse fastidiosi riverberi di luce a causa della copertura metallica, e comprimesse l'esercizio del diritto di veduta in appiombo del condomino dell'appartamento sovrastante).

**Cass. civ., Sez.II, 30/03/2000, n.3891**

Per l'acquisizione dei dati esterni relativi al traffico telefonico - concernenti gli autori, il tempo, il luogo, il volume e la durata della comunicazione, fatta esclusione del contenuto di questa - archiviati dall'ente gestore del servizio di telefonia, è sufficiente, in considerazione della limitata invasività dell'atto, e sulla base dello schema delineato nell'art. 256 c.p.p., eterointegrato dall'art. 15 comma 2 cost., il decreto del p.m. con il quale si dia conto delle ragioni che fanno prevalere sul diritto alla privacy l'interesse pubblico di perseguire i reati. E invero, anche se manca la previsione di un immediato controllo giurisdizionale di detto decreto motivato, tuttavia il recupero di tale controllo, che attiene a un mezzo di ricerca della prova, avviene attraverso la rilevabilità, anche di ufficio, dell'eventuale relativa inutilizzabilità, in ogni stato e grado del procedimento, così nelle indagini preliminari nel contesto incidentale relativo all'applicazione di una misura cautelare, come nell'udienza preliminare, ovvero nel dibattimento o nel giudizio di impugnazione.

Cass. pen., Sez.un., 21/06/2000, n.16 Per l'acquisizione dei dati esterni relativi al traffico telefonico - concernenti gli autori, il tempo, il luogo, il volume e la durata della comunicazione, fatta esclusione del contenuto di questa - archiviati dall'ente gestore del servizio di telefonia, è sufficiente, in considerazione della limitata invasività dell'atto, e sulla base dello schema delineato nell'art. 256 c.p.p., eterointegrato dall'art. 15 comma 2 cost., il decreto del p.m. con il quale si dia conto delle ragioni che fanno prevalere sul diritto alla privacy l'interesse pubblico di perseguire i reati. E invero, anche se manca la previsione di un immediato controllo giurisdizionale di detto decreto motivato, tuttavia il recupero di tale controllo, che attiene a un mezzo di ricerca della prova, avviene attraverso la rilevabilità, anche di ufficio, dell'eventuale relativa inutilizzabilità, in ogni stato e grado del procedimento, così nelle indagini preliminari nel contesto incidentale relativo all'applicazione di una misura cautelare, come nell'udienza preliminare, ovvero nel dibattimento o nel giudizio di impugnazione.

**Cass. pen., Sez.un., 21/06/2000, n.16**

I documenti relativi alle determinazioni dirigenziali riguardanti le quote dei fondi d'istituto percepite dai vari dipendenti di un istituto scolastico in attuazione delle prescrizioni del contratto collettivo di comparto, non rientrano nel novero degli atti sottratti all'accesso nè la loro visione viola la normativa sulla privacy di cui alla l. 31 dicembre 1996 n. 675, trattandosi di dati sulla retribuzione ostensibili secondo le previsioni contrattuali.

**T.A.R. Toscana, Sez.I, 22/06/1999, n.514**

L'art. 43, comma 2, l. 31 dicembre 1996, n. 675, sulla tutela della "privacy", mantiene

ferme la disposizioni della l. 7 agosto 1990, n. 241, in materia di accesso ai documenti amministrativi, che trovano un diretto riferimento costituzionale nell'art. 97, che sancisce il principio di trasparenza dell'amministrazione, nell'art. 21, che riconosce la libertà di informazione. Ciò nonostante, nei casi in cui sia accolta l'istanza di accesso (ovvero di comunicazione di dati personali), il soggetto che acquisisce il dato deve comunque osservare le relative regole, salvo responsabilità civili e penali che la stessa normativa sulla "privacy" prevede.

**T.A.R. Lombardia Milano, Sez.II, 17/05/1999, n.1689**

I test cd. psicologici non sono, in quanto tali, lesivi del diritto alla riservatezza (anche del lavoratore ex art. 8 l. 20 maggio 1970 n. 300) ed alla "privacy" (leggi n. 674 e 675 del 1996) dei candidati di una procedura concorsuale, ben potendo però tale censura riguardare i singoli quesiti specificamente individuati.

**T.A.R. Emilia-Romagna Bologna, Sez.II, 31/03/1999, n.128**

Nel "trattamento di dati personali" consistente nella diffusione di informazioni a scopo di cronaca giornalistica, soggetto tutelato dalla legge sulla privacy e legittimato alla proposizione del ricorso al garante è soltanto colui di cui l'informazione giornalistica obiettivamente riferisca; colui che, comunque, identificato o identificabile (ancorchè, per avventura, in modo inappropriato e, magari, interferente con altrui diritti) costituisca l'effettivo termine di riferimento della notizia propalata.

**Trib. Milano, 14/10/1999**

Dalle nozioni di "trattamento", di "dato personale" e di "interessato" normativamente definite al comma 2 dell'art. 1 l. n. 675 del 1996 e dalla loro correlazione con la previsione dei successivi art. 13 e 29, risulta che soggetto tutelato dalla l. n. 675 del 1996 e, in quanto tale, legittimato ad investire il Garante ai sensi dell'art. 29 della stessa legge è esclusivamente la persona, comunque identificata o identificabile, costituente l'oggettivo termine di riferimento del "dato", e cioè, dell'informazione "trattata" (raccolta, registrata, diffusa ecc.) e che, di conseguenza, nel "trattamento di dati personali" consistente nella diffusione di informazioni a scopo di cronaca giornalistica, soggetto tutelato dalla legge sulla "privacy" e legittimato alla proposizione del ricorso al Garante è solo la persona di cui l'informazione giornalistica obiettivamente riferisce, e cioè colui che, comunque indetificato o identificabile (ancorchè, per avventura, in modo inappropriato e, magari, interferente con altri diritti), costituisce l'effettivo termine di riferimento della notizia propalata.

**Trib. Milano, 14/10/1999**

La l. 31 dicembre 1996 n. 675 (c.d. legge sulla privacy) si applica anche al trattamento di dati effettuato dall'autorità giudiziaria. Per trattamento di dati personali si intende, a norma dell'art. 1

comma 2 della citata legge, qualunque operazione concernente, fra l'altro, l'utilizzo, la comunicazione e la diffusione di informazioni relative alla persona. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'art. 686 comma 1 lett. a) c.p.p. è ammesso soltanto se autorizzato da espressa disposizione di legge o provvedimento del garante che specifichino le rilevanti finalità di interesse pubblico del trattamento (a reg. ex art. 24 l. n. 675 del 1996).

**Uff. indagini preliminari Trib. Milano, 19/01/1999**

E' infondata la pretesa dell'amministrazione di esibire il documento richiesto con "omissis" in asserito adempimento della disciplina in tema di tutela dei dati personali, considerato che la l. 31 dicembre 1996 n. 675 ha fatto espressamente salve le vigenti leggi in materia

di accesso ai documenti amministrativi e che, in generale, l'applicazione della legge sulla "privacy" non comporta un regime di assoluta riservatezza dei dati, dovendosi verificare caso per caso se sussistano altri interessi meritevoli di pari o superiore tutela.

**Cons. Stato, Sez.IV, 27/08/1998, n.1137**

La tutela della "riservatezza" delle persone presupposta dalle norme in tema di accesso agli atti amministrativi va intesa sia come estensione degli standard di protezione tradizionalmente enucleati dalla giurisprudenza civile e che ricalcano il valore - ben noto nell'esperienza giudiziaria anglosassone - della "privacy" e del "to stay alone" - sia, entro i termini ragionevolmente necessari alla formazione di un convincimento da parte della competente p.a., come salvaguardia degli interessi di coloro che hanno concorso in via determinante alla promozione di un procedimento sanzionatorio nei confronti di un datore di lavoro da essi ritenuto non in regola con le vigenti disposizioni previdenziali ed assistenziali.

**T.A.R. Veneto, Sez.I, 28/12/1995, n.1599**

La divulgazione dell'immagine di una persona nota è consentita contro il consenso di questa quando non sia pregiudicata la sua dignità, la divulgazione resti nell'ambito territoriale della persona nota, la divulgazione non sia fatta a prevalente fine di lucro, la notorietà della persona giustifichi un effettivo pubblico interesse a una completa informazione e l'immagine sia ripresa in un luogo e in condizioni di sicura mancanza di privacy.

**Trib. Napoli, 19/05/1989**

Una veranda è da considerarsi, in senso tecnico-giuridico, una vera e propria costruzione assoggettata al requisito della concessione, poiché difetta normalmente del carattere di precarietà, trattandosi di opera destinata non a sopperire ad esigenze temporanee e contingenti con la sua successiva rimozione, ma a durare nel tempo, ampliando così il godimento dell'immobile; la definizione di tale sua natura non è da ritenersi modificata dalla disciplina normativa introdotta con la l. 28 febbraio 1985, n. 47, la quale anzi precisa, tra l'altro, che sono da giudicarsi opere in assenza di concessione anche quelle rivolte all'esecuzione di volumi edilizi oltre i limiti indicati nel progetto e tali da costituire un organismo edilizio o parte di esso con specifica rilevanza o autonomamente utilizzabile (nella specie, relativa a rigetto di ricorso, l'imputato aveva sostenuto che per la veranda, in quanto destinata alla protezione dagli agenti atmosferici, non fosse necessaria la concessione edilizia; la suprema corte ha invece affermato la necessità della concessione prospettando che la salvaguardia dalle intemperie si realizza con la semplice apposizione alle aperture dei cosiddetti doppi infissi in alluminio anodizzato, mentre la veranda non solo non rappresenta un'opera precaria, ma, realizzando anche la difesa dagli agenti atmosferici, pone in essere un rilevante aumento della volumetria abitativa, comunque utilizzabile, assicurando, infine, spazio e privacy al corpo immobiliare).

**Cass. pen., 06/04/1988**

Lede la privacy di un soggetto la divulgazione della notizia del suo mutamento di sesso in assenza di prova che tale notizia risultasse da documenti pubblici, e in considerazione delle cautele adottate per celare il fatto e della insussistenza di un valore informativo della notizia.

Corte d'Appello degli Stati Uniti d'America, 18/01/1983 Nel caso in cui il contratto integrativo aziendale regoli l'attribuzione del premio di rendimento subordinandolo ad un certo tipo di qualifica di merito, la discrezionalità dell'attribuzione della medesima non può essere assoluta, ma è sindacabile da parte del giudice, che può verificare la valutazione

del datore di lavoro in base ai principi di correttezza e buona fede (art. 1175 e 1375 c. c.); nella fattispecie, trattandosi di lavoratore che riveste la carica di dirigente della rappresentanza sindacale aziendale, il datore di lavoro ha altresì posto in essere un atto discriminatorio nell'attribuzione della qualifica di <sufficiente>: tale pregiudizio finale, infatti, non appare adeguato alle valutazioni parziali riferibili al rendimento alla conoscenza del lavoro, all'iniziativa ed alla capacità di apprendere, al comportamento ed alla disciplina che sono sostanzialmente positive ed è stato espresso sulla base di un giudizio sul carattere (<indulge alla polemica specie in relazione a richieste di lavoro straordinario>) che appare violatore della <privacy> del dipendente e, comunque non rilevante ai fini della valutazione della sua attitudine professionale.

**Pret. Città di Castello, 02/02/1980**

Nel caso in cui il contratto integrativo aziendale regoli l'attribuzione del premio di rendimento subordinandolo ad un certo tipo di qualifica di merito, la discrezionalità dell'attribuzione della medesima non può essere assoluta, ma è sindacabile da parte del giudice, che può verificare la valutazione del datore di lavoro in base ai principi di correttezza e buona fede (art. 1175 e 1375 c. c.); nella fattispecie, trattandosi di lavoratore che riveste la carica di dirigente della rappresentanza sindacale aziendale, il datore di lavoro ha altresì posto in essere un atto discriminatorio nell'attribuzione della qualifica di <sufficiente>: tale pregiudizio finale, infatti, non appare adeguato alle valutazioni parziali riferibili al rendimento alla conoscenza del lavoro, all'iniziativa ed alla capacità di apprendere, al comportamento ed alla disciplina che sono sostanzialmente positive ed è stato espresso sulla base di un giudizio sul carattere (<indulge alla polemica specie in relazione a richieste di lavoro straordinario>) che appare violatore della <privacy> del dipendente e, comunque non rilevante ai fini della valutazione della sua attitudine professionale.

**Pret. Città di Castello, 02/02/1980**

## Sicurezza Informatica

Senza un piano aziendale per la protezione dei PC, l'intero parco file dei computer aziendali può essere accessibile a tutti i dipendenti. Il rischio riguarda ovviamente documenti strategici, resoconti finanziari e informazioni sui dipendenti.

Sicuramente non è quello che volete. Eppure molti proprietari di piccole aziende non stabiliscono alcun piano a questo riguardo, e finiscono per pagarne le conseguenze. Non solo mettono a rischio le informazioni aziendali, ma anche gli accordi di riservatezza sottoscritti con dipendenti e clienti.

Ciò di cui avete bisogno è un piano di protezione formale per PC che sia facile da comprendere e che i dipendenti siano in grado di appoggiare e implementare.

Ecco cinque punti essenziali per un piano di protezione.

- 1) **Utilizzate una password di protezione.** I file protetti tramite password possono essere aperti solo dagli utenti autorizzati. In genere i sistemi operativi includono un sistema di protezione tramite password e la maggior parte delle applicazioni software, fra cui Microsoft Office, consente di utilizzare le password per proteggere file e cartelle.
- 2) **Scegliete password fantasiose.** Non usate il nome del vostro cane, di vostro figlio o del vostro compagno; dati che si possono rivelare facilmente individuabili. Lo stesso vale per date di nascita, indirizzi, cantanti o gruppi preferiti o altre parole che facilmente possono essere associate a voi. Inoltre, occorre ricordare che è più difficile individuare

una password composta da un insieme di lettere e numeri in un'alternanza di caratteri minuscoli e maiuscoli, così come una password che viene cambiata spesso. Fornite a tutti i collaboratori istruzioni su come definire una password, quando sostituirla e come proteggere file e cartelle.

- 3) **Utilizzate la crittografia.** Per proteggere le informazioni importanti memorizzate sui PC aziendali è inoltre possibile crittografare i dati. I software di crittografia trasformano i dati in una serie di elementi incomprensibili che possono essere decodificati solo utilizzando la chiave software appropriata. In genere, i software di crittografia sono utilizzati per limitare l'accesso a dati estremamente riservati, quali elenchi di clienti o informazioni finanziarie, per proteggere i dati dei computer portatili utilizzati fuori dall'ufficio e messaggi di posta elettronica particolarmente importanti.
- 4) **Non lasciate mai i dati senza sorveglianza.** Incoraggiare il personale a chiudere sempre i file prima di allontanarsi dalla scrivania può limitare i rischi di protezione per i PC. In caso contrario, ad esempio, durante la pausa pranzo i file potranno essere letti da chiunque si trovi a passare dall'ufficio. È consigliabile redigere regole precise che indichino chiaramente che tutti gli utenti devono sempre chiudere i documenti non in uso.
- 5) **Riducete i rischi relativi all'uso dei computer portatili.** L'uso dei computer portatili consente di ottimizzare la produttività, ma può anche mettere a rischio la sicurezza dell'azienda, se non si adottano misure di protezione appropriate. Ricordate a tutti i lavoratori mobili l'importanza della sicurezza al di fuori dall'ufficio. Ad esempio, quando si utilizzano documenti riservati in luoghi pubblici come bar o aerei è opportuno utilizzare caratteri di dimensioni ridotte. Se il personale utilizza risorse tecnologiche pubbliche dovrà essere in grado di assicurarsi che i documenti restino sempre sul disco rigido del proprio computer portatile e non vengano copiati sul computer della risorsa utilizzata. La crittografia è un ottimo strumento per proteggere i computer portatili utilizzati al di fuori dell'ufficio. Se si utilizza un software di crittografia, nessuno sarà in grado di carpire informazioni memorizzate sul computer rubato.

## Sopraluogo

Il sopraluogo sarà diretto al controllo della struttura informatica aziendale, per poter adeguare la stessa alle misure minime prevista dalla legge sulla privacy. In particolare saranno analizzati tutti i componenti fisici e logici che riguardano la normativa contenuta nel testo unico 196 del 2003 che troverà adempimento inderogabile in data 30/06/2005.

In particolare il nostro staff provvederà al controllo dei computer non in rete, con verifica del sistema operativo, della connettività esterna, accesso ad internet, utilizzatori, programmi Firewall antivirus, account, ed accessi eventuali.

Sui computer in rete si effettueranno controlli sulla connettività in rete interna Lan aziendale, sui sistemi operativi, sugli utilizzatori, sui sistemi antivirus ed anti-intrusione. Sulla rete aziendale i nostri tecnici provvederanno al controllo dei cablaggi, degli apparati attivi e passivi, sulla presenza ed efficienza dei software applicativi di protezione e sistemi hardware come ad esempio eventuali Router.

Lo staff che provvederà a tali controlli, sarà composto da professionisti che coniugano e fanno della legge e dell'informatica il proprio lavoro. I controlli saranno effettuati con apparecchiature certificate. La nostra azienda si avvale di collaboratori che hanno già operato in questo settore, con esperienze pluriennali nella gestione di macro-reti Lan,

aziendali.

## Adeguamento sicurezza informatica

- Ultimo Aggiornamento (Tuesday, 01 December 2005)

Al fine di adempiere in modo corretto a quanto richiesto dall'Allegato B del Decreto legislativo 196/2003, si devono adottare alcune misure minime di sicurezza dei sistemi informatici ed informativi quali:- Sistemi antivirus- Sistemi firewall- Back-up costante dei dati su supporti rimovibili. Autenticazione informatica di accesso (es. password), redazione delle lettere d'incarico e assegnazione di credenziali d'accesso per i locali dove risiedono i materiali cartacei contenenti i dati da tutelare secondo quanto stabilito dalla legge.

La nostra offerta garantisce il rispetto della suddetta legge ed il sensibile miglioramento della sicurezza indispensabili ad ogni ufficio informatizzato.

### L'offerta comprende:

- Indagine cognitiva per il riconoscimento e identificazione di tutti i dati che necessitano dell'adeguamento
- Antivirus (uno per postazione PC);
- Antispam, per bloccare la posta indesiderata (uno per postazione PC);
- Firewall (uno per postazione PC);
- Unità di back-up esterna rimovibile (se necessaria);
- Software per back-up automatico e programmabile;
- Configurazione delle politiche di sicurezza per i sistemi operativi (gestione utenti e password);
- Unità di riconoscimento biometrico, in caso di dati sensibili;
- Fornitura di tutta la modulistica richiesta;
- Formazione del personale di 2 ore, con relativa certificazione riconosciuta in materia di privacy e rilasciata dalla regione toscana a seguito di un esame on-line;
- Installazione e configurazione inclusi;
- Redazione delle lettere delle d'incarico per le seguenti figure :titolare, responsabile, incaricati.
- Redazione delle lettere per l'informativa ed il consenso alla trattazione dei dati da parte degli interessati.
- Rilascio di un registro per gli accessi non autorizzati effettuati nei locali contenenti dati sensibili
- Rilascio al termine di tutte le operazioni di del DPS da mostrare in caso di controllo alle autorità competenti.

### I PREZZI:

*Per la visione dei prezzi vi invitiamo a visionare il nostro shop*

<http://www.konsulting.us/shop/index1.html>