LA PRIVACY PER IL CONSULENTE DEL LAVORO

BELLUNO – 2012

AVV. ELENA BASSOLI – Past President Aiga Genova
Presidente CSIG (Centro Studi Informatica Giuridica) Genova
PRESIDENTE ANGIF
PROF. A C. "DIRITTO DELL'INFORMATICA" UNIVERSITÀ DI GENOVA, MILANO, ALESSANDRIA

studiolegalebassoli@gmail.com

Nascita ed evoluzione del concetto di privacy

Il Codice della privacy, d.lgs. 196/2003, non è il primo atto normativo che riconosce il diritto alla tutela dei dati personali.
Prima di lui il legislatore aveva provveduto a disciplinare la materia con la L. 675/96 che alcuni di voi ricorderanno.
Tale legge, di attuazione della direttiva del 1995 n. 46, era tuttavia il frutto di un percorso articolato, nato già negli anni 80 con diverse proposte e disegni di legge (Mirabelli, Martelli, Martinazzoli) che erano tuttavia rimasti lettera morta.
La legge 675 disciplinò per la prima volta in Italia la materia per 7 anni, durante i quali si succedettero una decina di decreti legislativi che emendarono la materia a piccole fasi, fino ad approdare alla necessità di un testo unico nel 2003, appunto il Codice della Privacy che oggi analizzeremo.

È importante, prima di affrontare le questioni che maggiormente ci premono, iniziare, come fa il d. lgs. 196/2003 (cd. Codice Privacy) all'art. 4, dalle definizioni dei diversi termini che si incontrano.

Definizioni

GLI OGGETTI

Trattamento
Sostanzialmente qualunque cosa che venga fatta con o sui dati: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione. Ricordiamo che la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati, integrano comunque trattamento.
Nel trattamento, come visto, sono ricomprese anche due operazioni particolari su cui è il caso di soffermarsi un attimo, perché oggetto di precisazioni ad opera del nuovo codice deontologico: la conservazione e la cancellazione:

Dato personale comune
Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (es. codice fiscale, targa auto, numero di telefono)

Dato sensibile
Quel particolare tipo di dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale

Dato giudiziario
Quel particolare tipo di dato personale idoneo a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di

casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. Non vi rientrano i dati relativi a processi civili, né quelli relativi a processi penali per cui non sia prevista l'iscrizione al casellario (reati puniti con sola ammenda).

I SOGGETTI

Interessato
Il soggetto al quale si riferiscono i dati. Può essere una persona fisica o giuridica (enti pubblici o società private).

Titolare
Colui che gestisce ed amministra il trattamento dei dati che riguardano un qualsiasi interessato. Può essere la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile

È figura facoltativa che può essere nominata dal titolare per coadiuvarlo nei compiti e adempimenti imposti dalla privacy. Può essere una persona fisica, giuridica, un ente o un'associazione. Necessita di una lettera di assunzione dell'incarico di responsabile.

Incaricato
È la persona fisica autorizzata a compiere operazioni di trattamento dal titolare: qualsiasi livello operativo o esecutivo di lavoratore autonomo, subordinato o parasubordinato o di altra natura, che debba semplicemente eseguire un compito o una funzione su o con un dato. Deve assumere la qualifica di incaricato (con una apposita lettera di incarico).

Istruzioni agli incaricati: *I professionisti, in particolare, devono fornire anche concrete istruzioni al personale di studio affinché si pongano speciali cautele in caso di utilizzo di registrazioni audio/video, di tabulati telefonici, di perizie ecc. e devono vigilare affinché si eviti l'uso ingiustificato di informazioni che potrebbero comportare gravi rischi per il cliente. Atti e documenti, una volta estinto il procedimento o il mandato, possono essere conservati in originale o in copia, solo se risultino necessari per altre esigenze imposte dalla legge.*

OBBLIGHI DEL TITOLARE

Informativa

Il titolare ha il dovere ex art. 13 di far sapere praticamente sempre all'interessato tutto ciò che ha diritto di sapere. Si tratta di uno dei diritti fondamentali, la cui violazione genera responsabilità amministrativa (3.000 euro di sanzione minima ex art. 161).
L'informativa può essere resa anche oralmente o in forma semplificata, vale a dire mediante affissione di cartelli nei luoghi di passaggio. È sufficiente una sola informativa all'inizio del trattamento.

I professionisti potranno informare la clientela una tantum*, anche oralmente in modo semplice e colloquiale sull'uso che verrà fatto dei loro dati personali. L'informativa scritta potrà anche essere affissa nello studio o pubblicata sul sito web.*
L'informativa agli interessati, che può non comprendere gli elementi già noti alla persona che fornisce i dati e può essere caratterizzata da uno stile colloquiale e da formule sintetiche adatte al rapporto fiduciario con la persona assistita o, comunque, alla prestazione professionale; essa può essere fornita, anche solo oralmente e, comunque, una tantum *rispetto al complesso dei dati raccolti sia presso l'interessato, sia presso terzi. Ciò, con possibilità di omettere l'informativa stessa per i dati raccolti presso terzi, qualora gli stessi siano trattati solo per il periodo strettamente necessario per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive.*

Consenso:

connesso all'obbligo di informativa è il consenso dell'interessato. L'informativa è infatti finalizzata ad esprimere un consenso informato che è sempre richiesto quando si trattino dati sensibili o inerenti lo stato di salute o la vita sessuale.
Esistono tuttavia almeno 3 casi in cui il consenso non deve essere richiesto all'interessato, come disciplinato dall'art. 24

- quando si tratti di far valere o difendere un diritto in giudizio o nell'ambito di investigazioni difensive
- quando il trattamento sia necessario epr dare esecuzione a un contratto di cui l'interessato è parte (è lui che chiede la prestazione quindi è logico che intenda fornire tutti i dati necessari)
- quando il trattamento è imposto da norme di legge, di regolamento o imposto dalla normativa comunitaria

Il consenso dell'interessato, quindi, non va richiesto per adempiere a obblighi di legge e non occorre, altresì, per i dati, anche di natura sensibile, utilizzati per perseguire finalità di difesa di un diritto anche mediante investigazioni difensive. Ciò, sia per i dati trattati nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, anche al fine di verificare con le parti se vi sia un diritto da tutelare utilmente in sede giudiziaria, sia nella fase successiva alla risoluzione, giudiziale o stragiudiziale della lite. Occorre peraltro avere cura di rispettare, se si tratta di dati idonei a rivelare lo stato di salute e la vita sessuale, il principio del "pari rango", il quale giustifica il loro trattamento quando il diritto che si intende tutelare, anche derivante da atto o fatto illecito, è "di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile" (artt. 24, comma 1, lett. f) e 26, comma 4, lett. c) del Codice; aut. gen. nn. 2/2007, 4/2007 e 6/2007; Provv. del Garante del 9 luglio 2003);

Diritti di conoscenza e diritti applicativi dell'interessato ex art. 7

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, (…);
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità (..) di responsabili o incaricati.
Si tratta dei cd. diritti conoscitivi, che sono esercitabili anche nei confronti di chi non è ancora titolare.
Cosa significa ?
L'interessato ha diritto ad accedere in particolare alle informazioni su tre aspetti principali:
Il primo è l' **Origine**: diritto a ricostruire il flusso informativo mediante conoscenza specifica (nominativa) delle fonti di acquisizione e non solo una generica indicazioni di categoria o tipologia.
Il secondo aspetto riguarda la **Finalità**: comunicazioni commerciali o indagini statistiche hanno finalità diverse e ciò produce effetti in relazione all'art. 11 e per i cd. diritti di opposizione.
Infine l'interessato può esigere informazioni circa la **Logica**: ossia l'insieme di principi che governano i software automatici che valutano aspetti come il rendimento professionale, il credito, l'affidabilità o il comportamento.
A questi diritti conoscitivi sono connessi "diritti applicativi", sempre disciplinati dall'art. 7, che prevedono la possibilità per l'interessato di ottenere
- L'aggiornamento la rettifica o l'integrazione di dati che siano obsoleti, errati o incompleti
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge
- l'attestazione che le operazioni sopra dette siano portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi
- l'interessato ha inoltre il diritto di opporsi in tutto o in parte per motivi legittimi al trattamento dei dati personali che lo riguardano o di opporsi al trattamento ai fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Per questi diritti è previsto, per legge, un possibile differimento nel periodo durante il quale, dal loro esercizio, può derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria (art. 8, comma 2, lett. e) del Codice);

Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, al quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'articolo 7 non possono essere esercitati se i trattamenti sono effettuati per ragioni connesse a: Antiriciclaggio, Sostegno vittime estorsione, Indagini difensive o

esercizio di un diritto in sede giudiziaria, per ragioni di giustizia, presso uffici giudiziari CSM o Ministero della Giustizia
Nei casi in cui il diritto non possa essere esercitato, l'interessato ha diritto ha inoltrale una segnalazione al Garante che provvede ad controllo ai sensi degli artt. 157-160.

Modalità di esercizio
La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche.
Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
È possibile conferire per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia

Identità e tempi
L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.
La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

Principio del doppio binario_ Azione civile davanti alla Magistratura Ordinaria o ricorso al Garante?
Il codice prevede che tutti i diritti possano essere esercitati davanti al Garante ma anche davanti al Tribunale Ordinario del luogo in cui ha sede il titolare. Ciò conferma la natura di diritto soggettivo perfetto di cui all'art. 1 del codice e consente all'interessato di poter usufruire di tutti gli strumenti processuali disponibili per la tutela di qualsiasi altro diritto. Non c'è alcuna giurisdizione "domestica", pertanto, neanche nell'ipotesi in cui il titolare sia una pubblica amministrazione. Anzi l'art. 152, comma 12, prevede che "il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento".

Misure di sicurezza minime e idonee e preventive

Nell'ambito del codice privacy è previsto l'obbligo per il titolare di adottare determinate misure di sicurezza al fine di prevenire l'accesso abusivo o la perdita o la distruzione, anche accidentale, dei dati trattati

I soggetti che trattano dati personali devono adottare un adeguato sistema di sicurezza in grado di proteggere i dati oggetto di trattamento; il legislatore opera una distinzione fra misure di sicurezza "minime" ed "idonee e preventive".
Le misure di sicurezza minime, previste dagli artt. 33 e ss. del Codice della Privacy ed individuate dettagliatamente nel Disciplinare Tecnico di cui all'Allegato B del Codice della Privacy[1], sono volte ad assicurare un livello minimo di protezione dei dati personali e devono essere adottate da tutti i titolari prima di qualsiasi operazione di trattamento di dati personali.

Il codice specifica che tutti i professionisti devono adottare adeguate misure di sicurezza dei sistemi informatici per evitare accessi abusivi o furti di dati e custodire con cura fascicoli e documentazione, in modo da evitare che personale non autorizzato o estranei possano prenderne visione.

Misure di sicurezza fisiche, logiche e organizzative

Le misure di sicurezza possono essere ancora suddivise in misure di sicurezza,
- fisiche (es. sistemi di allarme, porte blindate, ecc) logiche
- logiche (antivirus aggiornati almeno semestralmente, password di accesso, ecc)
- organizzative (credenziali di autenticazione per l'accesso differenziate in base alle mansioni svolte. Ad esempio l'addetto al personale non dovrà poter accedere agli archivi della clientela. Viceversa chi si occupa di rilevazione del grado di soddisfazione della clientela non dovrà poter accedere alle buste paga dei colleghi, ecc).

Se queste misure di sicurezza vengono adottate a livello base (es. aggiornare l'antivirus ogni 6 mesi) allora saranno misure di sicurezza minime, alla cui mancata adozione è riconnessa una sanzione penale, se invece vengono adottate al livello più elevato esistente, vale a dire secondo la migliore scienza e tecnica del momento (aggiornare l'antivirus quotidianamente), allora si configureranno come misure di sicurezza idonee e preventive, e la loro mancata adozione determinerà un illecito civile.

[1] Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici.

Seconda parte

(facoltativa)

4. Responsabilità

Principi

L' Art. 11 (Modalità del trattamento e requisiti dei dati) prevede che " I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati."

Si tratta di una delle norme cardine di tutto il codice. La violazione di una delle citate disposizioni può essere fonte di responsabilità amministrativa, civile e anche penale.

Responsabilità civile

Ai sensi dell'art. 15 del codice, l'attività di trattamento dei dati personali è definita dalla legge come "attività pericolosa" ai sensi dell'art. 2050 c.c. Tale norma del codice prevede, sostanzialmente un'inversione dell'onere della prova giacché nell'eventuale giudizio non dovrà essere il danneggiato a fornire la prova della colpevolezza del danneggiante (il titolare del trattamento) ma piuttosto questi a fornire la prova di aver adottato ogni cautela, ma che nonostante questo il danno si è verificato ugualmente. Tutto ciò, risolvendosi di fatto nell'impossibilità di aver adottate tutte le migliori misure di sicurezza che la scienza e la tecnica mettono a disposizione, viene definita "*probatio diabolica*", perché in realtà è impossibile da dare.

Ad esempio se il titolare del trattamento prova di aver adottato un antivirus, come prescritto dalle misure di sicurezza minime, ciò non basta. Perché qualcuno potrà sempre contestare il fatto che quell'antivirus non era sufficiente.

Lo stesso articolo prevede, poi, che è risarcibile il danno non patrimoniale laddove risultino violate le disposizioni dell'art. 11 sopra citato. Ciò significa che l'interessato può ottenere il riconoscimento di tale voce di danno indipendentemente dai danni materiali e per il solo fatto che è stato effettuato un trattamento illegittimo.

Le cautele da adottare

1) Effettuare il trattamento solo se risulta che sussistono le condizioni di legge. Ricorda che il trattamento in ambito pubblico è possibile solo se sussistono 4 requisiti fondamentali:

a) esiste una legge che autorizza quel trattamento che - da solo o con l'intervento precedente, contemporaneo o successivo di altri - stai compiendo

b) esiste un legge che individua le finalità di "rilevante interesse pubblico" del trattamento che - da solo o con l'intervento precedente, contemporaneo o successivo di altri - stai compiendo

c) esiste un regolamento anche interno che individua i tipi di dati che possono essere trattati per raggiungere quelle finalità
d) esiste un regolamento anche interno che individua le operazioni che possono essere compiute su quei dati.
3) Se ricevi una richiesta da parte dell'interessato, fai sottoscrivere un'istanza con l'indicazione delle informazione che vuole ricevere ed accertati della sua identità allegando alla richiesta scritta la fotocopia di un suo documento di identità.
5) Conservare supporti di memoria e stampe in luoghi sicuri. Alla conservazione dei supporti di memoria (DVD, CD, dischetti, memorie flash o penne usb etc.) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Come ogni incaricato, responsabile o titolare ha l'accortezza di non lasciare importanti documenti alla portata di sguardi indiscreti, così deve comportarsi con dischetti e stampe contenenti dati riservati quindi, a meno che non si sia sicuri che contengano solo informazioni non rilevanti si deve riporre tali supporti sotto chiave non appena terminato il loro utilizzo.
6) Account di accesso. L'accesso alla rete, come quello di ogni programma critico, richiede di identificarsi a mezzo di un nome utente ed una password. Le operazioni vengono registrate tenendo traccia dell'utente che le ha eseguite e quindi in base al suo userrname e password. Ogni utente deve avere l'accortezza di non permettere ad altri di utilizzare le proprie chiavi di accesso, anche per non rendersi responsabile di operazioni non eseguite personalmente.
Nel caso si stia utilizzando una stazione di lavoro e si intenda passare a lavorare su una differente, l'utente è tenuto a chiudere le applicazioni e le sessioni di lavoro aperte sul suo computer ed autenticarsi sull'altro sempre con le proprie credenziali. A tal fine è stata disabilitata ove possibile, la funzionalità che permetta di utilizzare le stesse chiavi di accesso da più di un computer alla volta.
7) Cambio delle password e loro scelta. Cambiare periodicamente, al minimo oltre tre mesi, le proprie password di accesso, anche nelle applicazioni (software applicativi: Word, Excel, Outlook etc..) dove non si viene obbligati periodicamente a farlo. Tutte le password devono essere scelte in modo tale da essere difficili da indovinare, evitare le solite date di nascita, numeri di telefono, nomi di familiari o del cane, etc.. E' sconsigliabile anche l'utilizzo di parole che sono contenute nei dizionari (italiano, inglese, etc.) in quanto con alcuni programmi è possibile "provare" tutte le password e quelle contenute in dizionari, sono le prime ad essere tentate. In generale è preferibile una password non "debole", composta da una sigla non banale di almeno 8 caratteri che comprenda lettere, numeri e simboli di interpunzione. (Per evitare di scrivere la password in giro e per evitare di essere troppo banali; è possibile ad esempio scegliere una frase, anche complessa ma che sicuramente non si dimentica e che contenga anche numeri e poi utilizzare solo alcuni caratteri come, ad esempio, le lettere iniziali delle parole)
Non utilizzare la stessa password per sistemi o programmi differenti, o password già utilizzate in precedenza in quanto, se viene scoperta una password di un'area, è facile che venga tentato il suo utilizzo per accedere anche ad altre aree e a distanza di tempo.
8) Cosa fare in caso di furto. Il "furto d'identità" avviene quando persone non autorizzate entrano in possesso del numero della tua carta di identità, del bancomat, della carta di credito, della tessera telefonica o di altre informazioni personali. Non è facile difendersi dai furti di identità ma se noti qualcosa di sospetto puoi prendere le seguenti precauzioni:
Cambia le tue password.
Avvisa la tua banca e gli altri istituti finanziari, compresa la società della carta di credito.

Contatta i creditori se ti accorgi che un conto è stato falsificato o aperto in modo fraudolento. Contatta il dipartimento frodi o sicurezza di ogni creditore e fai seguire una lettera.
Presenta una denuncia presso il dipartimento di polizia locale o del distretto in cui è avvenuto il furto dell'identità. Conserva una copia della denuncia in caso la banca, la società della carta di credito o altri creditori abbiano bisogno di un documento che attesti il furto.
Conserva tutti i documenti che hanno a che fare con il caso, compreso copia della corrispondenza e delle conversazioni telefoniche.
9) Come mantenere il controllo della tua privacy on-line. Per proteggere le tue informazioni personali, devi fare acquisti soltanto su siti Web attendibili, mantenere segrete le informazioni personali e controllare che i siti utilizzino e condividano i tuoi dati in modo corretto e protetto (controlla che nella barra degli indirizzi, dopo “http” compaia una “s” cosicché l'inizio del nome del sito sia “https.www.pincopallino.com”; ciò implica l'utilizzo di un protocollo di comunicazione sicuro.). Inoltre è consigliato posizionare le informazioni personali in un'area protetta da password e non fornire a nessun altro utente il permesso di accesso.
10) Virus informatici. Su ogni personal computer deve essere presente e tenuto aggiornato un programma antivirus. E' compito dell'utente accertarsi che tale programma venga eseguito correttamente, che non siano prodotti messaggi di mal funzionamenti o di presenze di virus informatici, oltre ad accertarsi che avvengano realmente gli aggiornamenti e che il programma sia "attivo" per il controllo del sistema. Gli utenti sono invitati a lanciare periodicamente dei controlli su tutto il disco locale del proprio computer. Nel caso si riscontrino delle anomalie o dei virus, deve essere contattato il titolare. Si ricordi che la prevenzione dalle infezioni
da virus su un computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non si hanno adeguate misure anti-virus, si potrebbe incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della postazione di lavoro. Si raccomanda di proteggere, quando possibile, i dischetti da scrittura prima di leggerli da altri computer (a mezzo dell'apposita linguetta del dischetto); è uno dei mezzi di prevenzione e si riducono i rischi di danneggiare i documenti, infatti i virus non possono rimuovere la protezione meccanica.

I comportamenti da evitare

1) Installazioni di nuovi programmi. Non installare software, in particolar modo di giochi e di programmi che permettano condivisioni di file (tipo Napster, Kazaa, eMule etc.): tutte le installazioni di programmi devono essere effettuate esclusivamente a cura, o con l'ausilio, del personale tecnico e comunque richieste all'Amministratore di Sistema, in quanto le licenze di utilizzo dei programmi devono essere conteggiate e, se necessario, acquistate. Come già ricordato, è meglio diffidare di dischetti e programmi anche se provenienti da fonti apparentemente attendibili. La maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale, ed esiste la possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", anche a mezzo di programmi che sembrano banali o innocui.
3) Condivisioni. Al fine di limitare la diffusione di virus, furti e danneggiamenti di documenti, problemi di funzionamento delle stazioni di lavoro, è vivamente sconsigliato condividere il disco fisso del proprio computer o anche solo parte di esso.
4) Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali. Se si trattano dati di particolare riservatezza, si consideri la possibilità di dotarsi di una macchina distruggi-documenti (shredder) per l'eliminazione di stampe non

più necessarie. In particolare è possibile che l'utente effettui varie copie di stampe prima di ottenerne una che lo soddisfi: soprattutto se il documento contiene dati riservati, distruggere personalmente le copie non utilizzate quando non più necessarie. In ogni caso non gettare mai documenti cartacei senza averli prima fatti a pezzi.
5) Non lasciare lavori incompiuti sullo schermo. Si deve avere l'accortezza di non lasciare lavori incompiuti sullo schermo e chiudere le applicazioni quando si lascia il posto di lavoro; l'assenza potrebbe essere maggiore del previsto e bisogna considerare che un documento presente sullo schermo ha la caratteristica di attirare la curiosità delle persone.
6) Non riutilizzare dischetti per affidare dati a terzi. L'utente deve avere l'accortezza di non far circolare dischetti che siano stati precedentemente utilizzati per contenere dati o documenti importanti, o anche solo delle loro copie di sicurezza, in quanto i vecchi dati, anche se i file sono stati cancellati dal dischetto o dalla chiavetta, spesso possono essere letti a mezzo di appositi programmi di utilità. Neanche la formattazione assicura l'eliminazione dei dati dai dischi é, nel dubbio, è sempre meglio usare un dischetto nuovo.
7) Posta elettronica, diffidare di dati, programmi, messaggi. Gli utenti non devono aderire, con la posta elettronica, a "catene di Sant'Antonio" nelle loro varie forme e versioni; solitamente dietro a messaggi di protesta, commoventi o contenenti promesse di premi, si nascondono società specializzate nella raccolta di indirizzi e-mail che poi provvedono a distribuirli per scopi pubblicitari. Iniziano quindi ad arrivare migliaia di messaggi di posta elettronica da fonti spesso non rintracciabili, che possono mettere in crisi i server e comunque generano inutile traffico di dati che abbassa le prestazioni della rete interna.
I virus informatici più diffusi negli ultimi tempi, si diffondono a mezzo della posta elettronica; una volta che un virus ha infettato un computer, spesso si diffonde automaticamente verso tutti gli indirizzi contenuti nella rubrica: è pertanto necessario prestare attenzione ai messaggi ricevuti anche se sembrano provenire da persone conosciute. Non aprire gli allegati se non attesi, soprattutto se si tratta di programmi eseguibili e, in ogni caso, controllarli con antivirus aggiornati.
8) Non violare le leggi in materia di sicurezza informatica. Ricordarsi che anche solo un esperimento di ingresso non autorizzato in un sistema protetto costituisce un tentativo di reato. Se si è interessati a studiare la sicurezza della propria postazione di lavoro o della rete di cui fate parte, chiedere preventivamente l'autorizzazione al titolare ed eseguire tutte le operazioni con l'Amministratore di sistema. Non utilizzate senza autorizzazione software che possa danneggiare la rete, creare problemi o allarmi di sicurezza, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.
9) Non lasciare acceso il computer se ci si assenta per un periodo di tempo lungo. Lasciare un computer acceso non crea problemi al suo funzionamento e velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che nel frattempo avvenga un'interruzione dell'energia elettrica che possa portare un danno all'elaboratore o alla sua configurazione.
10) Avvio dei computer, impostazioni di BIOS. Non far partire il computer da dischetto o CD e, se possibile, impostare il BIOS in modo da avere come "primari boot device" il disco rigido di avvio e proteggere l'accesso al BIOS tramite password. Infatti se il dischetto, la chiavetta o il CD fossero infetti, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file.

7. Luoghi comuni & miti da sfatare

Documenti amministrativi relativi a terzi non possono essere comunicati perchè “c'è la privacy”.

Con una certa frequenza, a chi chiede di esercitare il proprio diritto d'accesso a documenti amministrativi, viene risposto che non è possibile accettare la richiesta, giacchè esisterebbe una onnipresente esigenza di riservatezza o tutela dei dati.
In realtà, non esiste nessuna prevalenza della disciplina sulla privacy, tranne che si tratti di voler accedere a dati sensibili. Quindi non dovrebbero sussistere problemi ad ottenere accesso ai sensi della normativa in materia. Anzi. L'art. 59 del codice della privacy espressamente prevede che "i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni".
Dunque il rifiuto basato sulla supposta prevalenza della tutela dei dati personali è illegittimo.
Solo per quanto concerne i dati sensibili il successivo art. 60 prevede che il trattamento (cioè l'accesso) "è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, vale a dire che deve consistere in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile". In tal caso la pubblica amministrazione dovrà effettuare il relativo "bilanciamento" nell'ambito della propria discrezionalità amministrativa, consentendo l'accesso solo ove il richiedente intenda tutelare attraverso l'accesso, un diritto di "rango" pari o superiore a quello tutelato dalla privacy.

Il trattamento effettuato senza l'uso di computer non deve rispettare il codice della privacy.

La tutela accordata dalle legge è di natura "oggettiva" e, pertanto, prescinde – in linea di principio e per quanto riguarda le norme applicabili a tutti i trattamenti - dalle concrete modalità con cui sono effettuate le diverse operazione sui dati. Di conseguenza anche un semplice archivio cartaceo deve adeguarsi alla normativa contenuta nel codice (diritti, informativa, responsabilità e sanzioni, misure di sicurezza, tutela).
L'art 35 del codice e l'allegato "B" (disciplinare tecnico), punti 27-29, prevedono, inoltre, espresse misure di sicurezza proprio per il trattamento effettuato "senza l'ausilio di strumenti elettronici".

Le sanzioni previste nel codice della privacy sono solo di natura amministrativa e civile.

Gli artt. da 167 a 172 prevedono diverse ipotesi di reato, con conseguente responsabilità penale. Sono previste ipotesi di reato a titolo di dolo (intenzione di trarre profitto con altrui danno nel caso di "trattamento illecito"), ma anche a titolo di reato omissivo: l'art. 169 punisce, infatti, la mancata adozione di misure minime di sicurezza.

Per eventuali danni o omissioni è responsabile il dirigente o capo dell'ufficio e non il singolo operatore.

Gli adempimenti previsti dal codice riguardano tanto i livelli "alti" (dirigenti, amministratori) che quelli intermedi (quadri, funzionari) o semplicemente esecutivi (operatori o collaboratori). I primi risponderanno per eventuali carenze in fasi di progettazione o attuazione dei sistemi di sicurezza e degli opportuni flussi di dati.
Gli altri potranno essere chiamati a rispondere per il mancato rispetto delle direttive impartite o per la mancata segnalazione di anomalie o incongruenze riscontrabili usando l'ordinaria diligenza (in armonia con il principio che la legge non ammette ignoranza).

Se i dati sono pubblici possono essere utilizzati da chiunque.

Specie con riferimento all'ambito pubblico (in cui non è richiesto il preventivo consenso dell'interessato) il fatto che un dato sia pubblico non è sufficiente a legittimare il trattamento. Per i dati sensibili, infatti, ai sensi degli artt. 19, 20 e 21, devono in ogni caso sussistere i seguenti requisiti:

(1) una espressa previsione di legge che individui la finalità di rilevante interesse pubblico perseguita;
(2) l'autorizzazione (con la stessa legge o con provedimento del Garante) ad effettuare il trattamento;
(3) l'adozione di un atto di natura regolamentare, da parte della stessa amministrazione che effettuerà il trattamento, che specifici i tipi di dati che possono essere trattati e
(4) le operazioni che possono essere eseguite sui dati.

Chi può essere interessato ad accedere al mio computer?

Il fatto che non ci rappresentiamo alcun motivo per cui qualcun altro dovrebbe accedere al nostro sistema, non è una riflessione troppo ponderata. Esistono, infatti, diversi validi motivi, a partire da quello che...non ce ne sia nessuno (dal nostro punto di vista)! In altre parole sarebbe limitativo pensare ad un motivo specifico che spinga un potenziale delinquente informatico ad accedere proprio al nostro pc. I reati informatici vengono commessi perchè ad esempio si cercano - con una azione “a tappeto” - computer non adeguatamente protetti (ci sono sistemi software creati proprio per questi scopi) di cui “prendere possesso” (facendoli diventare veri e propri “zombie”) per realizzare altre azioni criminose (per mettere in atto un attacco ad esempio che sia in grado di bloccare un sito web, si prende il controllo di diverse centinaia o migliaia di computer e si fa in modo che tutti si connettano simultaneamente al sito e mandandolo in “tilt” per il numero eccessivo di connessioni) o per cercare numeri di carte di credito o, in definitiva, per “soldi”. Esiste un vero e proprio mercato degli indirizzi email e qualsiasi modo per procurarsene è buono se si parte dal presupposto di voler fare spamming.
Il mercato del cd. “malware”, cioè del “software cattivo” genera un giro d'affari illegale multi-miliardario e le motivazioni possono essere le più disparate e spaziare da motivi “politici” (attacco al computer della NASA) a quelli commerciali (bloccare il sito di un concorrente) o per dimostrare la propria abilità informatica o semplicemente “per provarci” (considerata la relativa facilità con cui è possibile fare tutto ciò).