1.5 ICT nella vita di ogni giorno

Il mondo elettronico

Tecnologie delle Comunicazione e dell'Informazione (ICT)

Gli ultimi decenni sono stati caratterizzati da grandi trasformazioni tecnologiche che hanno portato a una diffusione sempre maggiore dei computer, sia nell'ambito della vita quotidiana che in quello lavorativo. I primi computer sono comparsi, con il nome cervelli elettronici, nella seconda metà degli anni Quaranta. Col tempo questa definizione si è persa perché è risultato sempre più chiaro che una macchina, per quanto sofisticata ed intelligente, non può eguagliare il cervello umano laddove viene richiesta creatività, fantasia, valutazioni di strategia o considerazioni tipicamente umane.

Per quanto una persona possa essere veloce nel trovare informazioni o nell'eseguire calcoli, però, non potrà mai competere con i tempi con cui un computer riesce a svolgere le stesse operazioni. Anche per quanto riguarda la precisione, una macchina può compiere la medesima operazione infinite volte con una bassissima probabilità di commettere errori.

Possono essere elencati molti casi in cui la velocità e la precisione del computer superano di gran lunga quelle dell'uomo: si pensi per esempio ai calcoli in ambito scientifico o finanziario, oppure ai settori dove devono essere gestite grandi quantità di dati, come i censimenti o le anagrafi.

Il computer, quindi, è capace di portare notevoli miglioramenti in moltissimi campi ed è importante conoscerlo e saper sfruttare appieno le possibilità che offre.

L'**Information Technology** (IT) nasce come conseguenza di tutte queste considerazioni, per capire come rispondere a determinate esigenze, studiando il modo di affiancare il computer al lavoro umano.

I servizi Internet dedicati ai consumatori

È importante conoscere bene il computer e saperne sfruttare le potenzialità perché usandolo possono essere raggiunti notevoli miglioramenti in tutti i campi. La larga

diffusione di Internet ha infatti aperto nuovi scenari nello sviluppo dei servizi rivolti al pubblico: si sente infatti sempre più spesso parlare di *e-commerce*, *e-banking*, *e-government*.

E-commerce

Il termine e-commerce indica la possibilità di acquistare e vendere beni e servizi su Internet. Chi opera in questo settore realizza punti vendita virtuali, cioè siti attraverso cui si possono comprare prodotti di vario genere, come software, viaggi, libri, giocattoli ecc.

Ovviamente il commercio elettronico ha aperto nuovi e interessanti scenari offrendo molti vantaggi al consumatore, per esempio:

- disponibilità 24 ore al giorno dei negozi e dei servizi;
- possibilità di analizzare e confrontare i prezzi e la qualità dei prodotti rimanendo comodamente davanti al computer;
- possibilità di visitare negozi virtuali anche dall'altra parte del mondo, potendo così acquistare beni difficilmente reperibili nei negozi fisicamente raggiungibili;
- i costi dei prodotti sono più bassi, grazie al risparmio sulle spese di gestione dei negozi e sul personale.

E-banking

Anche i servizi e i prodotti bancari hanno subito notevoli cambiamenti. Grazie all'informatizzazione delle banche è stata attivata una vasta gamma di servizi personalizzati per i clienti, come la consultazione delle informazioni sul proprio conto, la possibilità di effettuare bonifici, pagamenti, direttamente effettuabili dal PC di casa connesso a Internet. L'insieme di questi servizi prende generalmente il nome di **e-banking**.

E-government

L'avvento del computer ha aperto nuovi scenari anche nello sviluppo dei servizi rivolti ai cittadini da parte delle Pubbliche Amministrazioni, il cosiddetto **e-government**. Moltissimi servizi pubblici (registrazioni, censimenti ecc.) sono ormai disponibili online e affidati ai computer: dal sito di molti comuni possono essere scaricati i moduli per le varie autocertificazioni, come lo stato di famiglia, il certificato di nascita, il certificato di residenza ecc.; dal sito del PRA (*Pubblico Registro Automobilistico*) si possono ottenere documenti relativi ai dati di un determinato veicolo (visure); può essere trasmessa telematicamente la dichiarazione dei redditi alla Pubblica Amministrazione, che le controlla con appositi software e molto altro.

Impiego nelle attività didattiche

Il termine **e-learning** si riferisce ad un metodo di auto-apprendimento e formazione che sfrutta le potenzialità rese disponibili da Internet. È un modo diverso di apprendere, alternativo all'insegnamento in aula. Con una normale connessione lo studente può accedere ai contenuti dei corsi in qualsiasi momento, scegliendo tempi, ritmi e luoghi di utilizzo del servizio.

Oltre all'e-learning, nel campo delle metodologie didattiche si parla sempre più spesso di **CBT**: un sistema didattico il cui principale vantaggio è quello di permettere all'utente di apprendere, in completa autonomia (in assenza di un docente). Due esempi di CBT sono rappresentati dal **software didattico** e dalla **formazione a distanza** (FAD).

Software didattico

I software didattici sono programmi che hanno un'ampia diffusione nelle scuole e sono in genere dedicati all'apprendimento di specifiche materie come le lingue straniere, la matematica, la musica, l'informatica. I più recenti hanno contenuti multimediali e utilizzano validi strumenti per verificare il livello di apprendimento.

Formazione a distanza

Secondo tempi e modalità specifiche del corso FAD possiamo scaricare sul nostro PC i contenuti delle lezioni per studiarli in un secondo momento. Talvolta si possono eseguire online test e compiti per valutare il livello dell'apprendimento. Per stimolare la collaborazione tra le persone coinvolte è prevista la comunicazione tra insegnante e studente e tra studente e studente, tipicamente tramite posta elettronica o videoconferenza. La formazione a distanza viene molto spesso adottata dalle imprese perché consente al lavoratore di usufruire delle lezioni rimanendo sul posto di lavoro e al tempo stesso consente all'azienda di contenere i costi per l'aggiornamento e la formazione del personale.

Il telelavoro

Una nuova modalità di operare

Il **telelavoro** è la modalità organizzativa più flessibile, resa più efficiente dai moderni mezzi di comunicazione. Esso rappresenta una pratica alternativa al modo tradizionale di progettare, organizzare e svolgere il lavoro, ed è incentrata sulla possibilità di ribaltare i vincoli della distanza, traducendoli in opportunità imprenditoriali, organizzative, di miglioramento della qualità della vita.

Gli elementi che caratterizzano il telelavoro sono:

- la *distanza* tra i soggetti implicati, che agiscono in uno spazio non fisicamente ravvicinato;
- l'*interdipendenza* funzionale tra i soggetti coinvolti;
- l'*interconnessione* operativa, resa possibile dall'impiego delle tecnologie;
- la *flessibilità* nell'erogazione, nell'impiego e nelle pratiche di lavoro.

Queste caratteristiche fanno sì che il telelavoro rappresenti una nuova modalità di prestare la propria opera, non vincolata al tempo e allo spazio, ma dipendente dai risultati e adeguata al proprio ritmo di vita.

Vantaggi e svantaggi del telelavoro

Il telelavoro comporta vantaggi diretti e opportunità per tutti, fra cui i principali possono tradursi:

- per le *aziende*, in termini di efficienza (maggiore produttività e flessibilità) e coordinamento di attività lavorative svolte all'esterno al pari di quelle svolte all'interno;
- per i *lavoratori*, in termini di migliore qualità della vita;
- per la *società* in generale, in termini di benefici ambientali, integrazione di gruppi svantaggiati, diffusione delle nuove tecnologie e delle competenze per utilizzarle, contributo allo sviluppo economico di regioni lontane, sviluppo locale di zone geografiche che altrimenti avrebbero scarsa rilevanza.

I principali svantaggi del telelavoro – o, per meglio dire, le problematiche principalmente individuate, che occorre considerare e tenere sotto controllo – possono essere così riassunti:

- per i *lavoratori*, minore visibilità e carriera, isolamento, riduzione della vita relazionale esterna, minore guida e aiuto nel lavoro;

➢ per *l'azienda*, difficoltà nella gestione dei lavoratori distanti, riorganizzazione dei processi aziendali, conflittualità con i capi intermedi.

Comunicazione

La posta elettronica

La **posta elettronica** (**e-mail**, *electronic-mail*) è uno degli strumenti più usati da chi ha la possibilità di accedere a Internet o a un'altra rete, e può essere immaginata come un normale servizio di posta con tempi di consegna imbattibili e dai costi molto bassi.

In questo paragrafo verranno analizzati i principi di funzionamento della posta elettronica introdotti gli strumenti di base che possono essere usati per velocizzarne l'impiego.

Un messaggio e-mail può contenere normale testo, ma anche altri oggetti. Anzi, lo strumento "posta elettronica" è ormai diventato il principale mezzo di scambio di file di ogni genere tra utenti. Possono venire spediti insieme a un messaggio testuale immagini, documenti di testo, programmi ecc. Il file che si invia insieme al messaggio viene definito **allegato** o **attachment**. Per esempio, se l'utente è in cerca di lavoro, invece di portare il proprio curriculum al datore di lavoro può allegarlo a una e-mail. Il datore riceverà, insieme al messaggio, il curriculum in formato elettronico, che potrà salvare, stampare e archiviare.

Un messaggio può avere più file allegati, purché la dimensione totale non superi quella consentita dal limite imposto al momento della stipula del contratto con il provider.

Un'osservazione pratica riguarda la situazione in cui l'utente riceve la posta al suo computer di casa, e non è dotato di una connessione particolare. Se il messaggio contiene un file molto esteso, il tempo necessario per scaricarlo aumenta e conseguentemente il destinatario deve rimanere connesso per tanto tempo prima che possa essere visualizzato. È consigliabile quindi non spedire file allegati troppo "pesanti", per evitare che il destinatario faccia connessioni, e quindi telefonate, troppo lunghe.

Chat

La **chat** è un servizio messo a disposizione da numerosi siti e permette agli utenti registrati di entrare in apposite "stanze virtuali" (**chatroom** o **canali**) per scambiare messaggi in tempo reale su svariati argomenti. Tutte le persone presenti in quella "stanza" possono leggere i messaggi scritti e intervenire nelle discussioni.

Instant Messaging

Un sistema di **instant messaging** (IM), messaggistica istantanea, è un sistema di comunicazione tra computer connessi in rete, che consente a due utenti di scambiare frasi e brevi testi. È differente dalla e-mail perché lo scambio è immediato: le frasi compaiono istantaneamente all'invio del messaggio. Le conversazioni non avvengono in stanze aperte a tutti, come nelle chat, ma tramite una comunicazione diretta tra i programmi utilizzati.

VoIP

La tecnologia **VoIP** (Voice over IP - in italiano voce tramite protocollo Internet) consente di effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata. Quando uno degli utenti parla, le informazioni vocali vengono trasformate in dati digitali e inviate sulla rete.

RSS L'**RSS** (acronimo di Really Simple Syndication - in italiano pubblicazione davvero semplice) è uno dei più popolari formati per la distribuzione di notizie. È un formato che definisce la struttura con cui devono essere presentate le notizie. Grazie a ciò, un qualunque lettore RSS potrà presentare sempre nello stesso modo notizie provenienti anche da fonti diverse. Attualmente RSS è lo standard per l'esportazione di contenuti Web, usato dai principali siti di informazione, quotidiani online, fornitori di contenuti ecc.

Blog Un **blog** (contrazione di *web-log*, in italiano traccia su rete) è una sorta di diario personale pubblicato in rete. In pratica si tratta di un sito web di facile utilizzo, dove pubblicare storie, informazioni e opinioni oltre a immagini e file; ciascun lettore può scrivere, in tempo reale, le proprie idee e riflessioni e lasciare messaggi all'autore.

Podcast Un **podcast** è un file (generalmente audio o video) messo a disposizione su Internet. Si può usufruire di tale file solo se siamo abbonati.

Comunità virtuali

Gli attuali mezzi di comunicazione hanno permesso la nascita di diverse **comunità online**: comunità di carattere "virtuale" i cui partecipanti non si incontrano praticamente mai nella vita reale (a parte durante i raduni), ma interagiscono tra loro quasi esclusivamente tramite i canali multimediali. Questo permette alle comunità di non essere vincolate a un particolare luogo o paese di provenienza; può farne parte chiunque abbia accesso ad Internet.

La maggior parte delle comunità virtuali nasce intorno a siti web, che diventano quindi luoghi di incontro, di comunicazione e informazione tra persone che condividono gli stessi interessi, aspirazioni o hobby.

Questi siti mettono a disposizione dei propri iscritti chat, forum, servizi di messaggistica ecc. In alcuni casi le comunità virtuali si occupano anche di giochi online per computer. In questo caso prendono il nome di *clan* o *gilde* e diventano quindi punti di riferimento e coordinamento per i giocatori che condividono la stessa passione.

Possono inoltre essere pubblicati e condivisi contenuti come documenti, foto, video ecc.

Gli strumenti da usare in genere sono molto semplici; questo permette di poter usufruire dei vari servizi anche a chi non è un esperto informatico. Un esempio di questo tipo di siti è YouTube, in cui possono essere pubblicati in modo molto semplice file audio e video.

In genere, al momento dell'iscrizione al sito per usufruire di tali servizi vengono richieste alcune informazioni personali. Prima di inserirle è opportuno prendere precauzioni per garantire un minimo di sicurezza:

- al momento dell'iscrizione è opportuno fornire solo i dati personali obbligatori;
- è preferibile fornire sempre il proprio profilo privato;
- visto che chiunque può leggere un blog o un forum, in una discussione devono essere limitate al minimo le informazioni personali;
- è bene far attenzione con chi si ha a che fare, soprattutto se sono estranei.

1.6 Salute e ambiente

Ergonomia

Con il termine ergonomia viene indicata la scienza che studia il rapporto uomo-macchina-ambiente per ottenere la loro migliore interazione. Di seguito vengono riportati i principali accorgimenti da tenere durante il lavoro al computer, volti a evitare danni alla salute.

La tastiera deve essere inclinabile e dissociata dallo schermo per consentire al lavoratore di assumere una posizione confortevole, tale da non provocare l'affaticamento delle braccia e delle mani. La posizione ideale prevede che i gomiti formino un angolo superiore ai 90° e inferiore ai 150°. Il piano di lavoro deve avere una superficie poco riflettente, essere di dimensioni sufficienti da permettere una disposizione flessibile dello schermo, della tastiera e del materiale accessorio. La sedia deve essere stabile, con altezza regolabile, in modo da consentire all'utente una certa libertà di movimento, una posizione comoda e tale che la distanza tra il monitor e gli occhi sia non inferiore a 50 centimetri (Figura 1.12).

L'illuminazione della stanza deve essere sufficiente ma non eccessiva: la luce naturale può essere filtrata con delle persiane e combinata con quella artificiale. Se la postazione di lavoro è vicino a una finestra è necessario orientarla in modo da non avere riflessi né sullo schermo né sulla tastiera. La temperatura e l'umidità, che giocano un ruolo importante, devono essere mantenute costanti e non eccessive magari sfruttando un'adeguata ventilazione.

Sono stati creati dei supporti ai dispositivi del computer per migliorare ulteriormente le condizioni lavorative. Per esempio, sono in commercio molti modelli di tastiera che

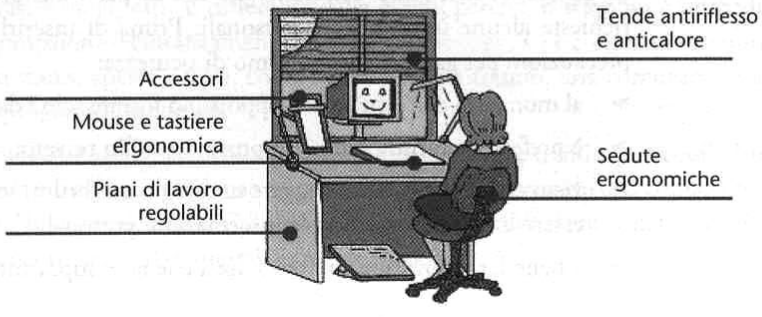

Figura 1.12: Principali elementi di una postazione economica

prevedono la presenza di poggiapolsi per alleviare le tensioni ai polsi, oppure degli schermi antiriflesso per riposare la vista.

Salute

I disturbi fisici associabili all'uso dei videoterminali sono principalmente quelli visivi, denunciati da bruciori, lacrimazione o secchezza, "sabbia" negli occhi, tic nervosi, fotofobia, visione disturbata, pesantezza, mal di testa. La causa risiede principalmente nel riflesso emanato dallo schermo, che si verifica in caso di luce eccessiva o di mancanza di illuminazione adeguata; riflessi provenienti da altre superfici vicine; luce diretta da finestre o fonti artificiali non schermate; scarsa definizione dello schermo; impegno visivo statico, senza interruzioni e troppo ravvicinato. Anche una luce diretta da finestre o fonti artificiali non schermate, una posizione troppo vicina al monitor provocano l'affaticamento della vista. Esistono comunque dei sistemi per ridurre questi rischi, come la regolazione della direzione della fonte luminosa diretta sul video, una migliore regolazione dei colori e delle sfumature del video, una periodica pulizia del monitor e l'uso di schermi antiriflesso.

È necessario cambiare spesso posizione, onde evitare intorpidimenti e tensioni muscolari dolorose, nonché tendiniti, artrosi cervicale ecc. La corretta postura , e alcune accortezze possono aiutare; per esempio:

- eseguire allungamenti del collo, spingendo dalla nuca verso il basso;
- appoggiarsi con il palmo delle mani sulla sedia e fare forza come per sollevarsi da seduti;
- stirare le spalle prendendo il gomito sulla testa con la mano opposta e tirandolo verso la stessa;
- allungare la schiena in avanti, come per abbandonarsi sulle proprie ginocchia.

Infine, è opportuno alzarsi almeno per un quarto d'ora ogni due ore, un po' per interrompere la monotonia e un po' per sgranchire le gambe, respirare a pieni polmoni, fare due chiacchiere e riposare gli occhi. Chi ne ha la possibilità cerchi di non fare una vita sedentaria fuori dal lavoro per compensare l'eccessiva sedentarietà quotidiana.

Ambiente

Devono essere osservati certi accorgimenti per non provocare danni all'ambiente: per esempio l'eccessivo consumo di corrente elettrica, oppure l'impatto dovuto allo smaltimento non corretto di alcuni materiali, come toner e cartucce di inchiostro, l'uso di componenti (in particolare i monitor) a basso consumo e non lasciare il computer acceso inutilmente. Il computer può essere impostato in modo che il monitor e il PC entrino in modalità *stand-by* quando non vengono usati dopo un certo periodo di tempo.

I rifiuti hi-tech hanno il tasso di crescita più rapido in Italia e in Europa, raggiungendo il 4 per cento di tutti i rifiuti urbani, e continuano ad aumentare a un ritmo compreso fra il 16 e il 28 per cento ogni cinque anni, ovvero tre volte in più rispetto alla media dei rifiuti ordinari. I dati europei dello scorso anno parlano di 6 milioni

di tonnellate di spazzatura tecnologica, di cui almeno la metà finisce nelle discariche e solo il 5 per cento viene avviato a un trattamento compatibile con l'ambiente. Per ovviare a questo problema è necessario l'impegno congiunto delle aziende produttrici e dei consumatori.

Dal punto di vista dei produttori si sta cercando di adottare tutti quegli accorgimenti che rispettano l'ambiente sia nella fase di creazione materiale dei prodotti, sia nel momento della commercializzazione. Ciò comporta: sviluppare sistemi che consentono un risparmio energetico o riducono gli scarti; facilitare la selezione dei rifiuti e il recupero dei componenti; utilizzare elementi che riducono al minimo le esalazioni atmosferiche; studiare leghe di saldatura per microcircuiti senza piombo; concepire imballaggi che non invadano l'ambiente.

Per quanto riguarda la gestione del "fine vita", cioè del recupero e riciclaggio dei materiali da ufficio, esistono ditte specializzate che ritirano, recuperano e smaltiscono tutto ciò che non serve più: cartucce e toner, computer obsoleti, ma anche carta e lampade al neon.

Per evitare lo spreco di carta e di inchiostro è necessario tenere quanto più materiale possibile in formato elettronico. Inoltre, quando possibile, è opportuno stampare su carta riciclata; la carta parzialmente stampata non deve essere buttata ma conservata per fare stampe di prova o non ufficiali.

1.7 Sicurezza

Identità e autenticazione

L'ID utente e la password

Nella maggior parte delle aziende in cui il lavoro è basato sull'applicazione dell'informatica, viene definito un insieme di regole, detto **diritto di accesso**, che governano l'uso delle varie strutture informatiche. Il rispetto di tali regole assicura il corretto utilizzo delle apparecchiature elettroniche e delle informazioni memorizzate. Per regolare l'accesso alle macchine viene in genere definito un ID utente, spesso associato a una password. Così come nella vita di tutti i giorni veniamo identificati dal nostro nome e cognome, nel PC l'**ID utente** (o **username** o **userid**) costituisce la nostra identità informatica; essa è una parola che permette al sistema di identificarci e di accettare la nostra richiesta di accesso.

Normalmente, oltre alla userid, è necessaria anche una **password**, o parola d'ordine, cioè un codice alfanumerico di lunghezza variabile, composto da cifre e/o lettere. La password può essere richiesta in diversi momenti durante una sessione di lavoro. Per esempio, può venire richiesta all'inizio della sessione di lavoro per fare in modo che al computer possano accedere solo utenti autorizzati. Se viene digitata una password errata, ovvero non corrispondente a quella registrata nel computer, il sistema operativo non permette di accedere ai dati memorizzati sull'hard disk o su una parte di essi. Molti programmi danno la possibilità di associare una password a singoli documenti, come quelli elaborati con un foglio elettronico o con un word processor.

La password può essere scritta anche su un foglio di carta, purché si abbia l'accortezza di conservarla in un posto sicuro. Dovrebbe essere superfluo osservare che la password di sistema non va memorizzata all'interno del computer, perché come potrebbe essere letta se è proprio lei a fare accedere alle risorse? Analogamente, è bene che le altre password (per esempio quelle per l'accesso alla posta) non siano conservate in qualche file sul PC che chiunque può leggere.

Il backup

Per limitare il rischio di perdita di dati è importante ricorrere alla **copia di backup** (ossia di sicurezza) dei dati. Se per qualsiasi motivo il computer si blocca o si danneggia il disco rigido, la copia di backup può essere trasferita su un altro PC o sullo stesso (dopo averlo riparato) in modo che l'elaborazione non venga interrotta dal malfunzionamento del sistema.

La copia può essere di un singolo documento, di una cartella, finanche dell'intero sistema. Il tipo di supporto di memoria da usare per fare il backup dipende ovviamente dalle dimensioni dei dati da salvare: per esempio se si tratta di un documento di testo (piccole dimensioni), può essere sufficiente un Floppy disk, se si tratta di immagini (grandi dimensioni) è necessario un supporto più capace, come un CD o il pendrive.

Per il backup di sistema sono necessari supporti di memoria capienti, come DVD, nastri magnetici, hard disk esterni.

Frequenza di backup

Non c'è una regola fissa sulla frequenza con cui deve essere effettuato il backup del sistema; in genere è importante farlo quando, dall'ultima volta in cui è stato eseguito, sono stati memorizzati molti dati.

Per esempio, nei grossi enti è necessario effettuare un backup una o più volte al giorno, mentre in una piccola impresa è in genere sufficiente effettuarlo su base settimanale.

Essendo l'operazione di backup lunga e ripetitiva, esistono dei programmi specializzati che svolgono questo compito, spesso integrati nel sistema operativo.

Il supporto su cui deve essere effettuato il backup può essere di vario tipo e differisce a seconda della quantità di dati da memorizzare. Indipendentemente dal tipo di supporto usato è fondamentale che esso sia esterno e, soprattutto, che venga conservato in un luogo diverso da quello in cui risiede il PC contenente i dati di cui è stato fatto il backup. Pensando infatti a un evento che distrugge il PC, per esempio un incendio, se il supporto di backup viene posizionato in un luogo diverso da quello in cui risiede il PC, si è più sicuri del possibile recupero dei dati salvati.

Sicurezza dei dati

Internet viene spesso usata per funzioni che trattano dati personali, in particolare operazioni bancarie e finanziarie; per questo motivo sono stati studiati diversi sistemi per evitare che persone non autorizzate possano leggere e addirittura modificare informazioni.

Firewall

Uno di tali sistemi è il **firewall:** un calcolatore o un software progettato per proteggere i computer di una rete (ma anche una singola macchina) dagli accessi da parte di utenti non autorizzati. Il suo compito è di filtrare i pacchetti di dati, lasciando che giungano a destinazione solo quelli la cui finalità sia chiara e che abbiano la relativa autorizzazione.

Il firewall viene posto tra la rete che deve essere protetta e le linee di comunicazione con l'esterno.

Il problema della sicurezza e della privacy

Uno dei problemi crescenti all'interno delle aziende moderne che si avvalgono di sistemi informatizzati per la gestione del proprio lavoro è quello della protezione e sicurezza dei dati. Per questo motivo esistono aziende specializzate che forniscono consulenze e software atti a trovare soluzioni finalizzate alla sicurezza IT e fisica e che siano in grado di proteggere le aziende da potenziali attacchi informatici, furti, spionaggio industriale e violazioni delle *policies*. Tali software riescono a fornire una sofisticata visualizzazione degli eventi, siano essi informatici o fisici, per consentire ai responsabili aziendali di rilevare i più sottili segnali di una possibile trasgressione delle regole negli ambienti di lavoro, anche quelli più complessi.

Grazie a funzionalità dette di *play back*, viene offerta inoltre una capacità di analisi e documentazione indispensabili per rilevare, prevenire, contrastare e perseguire eventuali comportamenti anomali e dolosi.

I responsabili della sicurezza aziendale non solo richiedono un maggior numero di dati, ma hanno anche la necessità di estrarre in modo più efficiente da enormi quantità di informazioni quelli che possono essere gli indicatori di potenziali o reali problemi; per questo le aziende si avvalgono di sistemi che forniscono esattamente questa capacità di analisi dei dati relativi all'ambiente di lavoro sia fisico che virtuale, garantendo la massima protezione delle risorse aziendali da qualsiasi tipo di minaccia.

Ovviamente, tali sistemi devono essere in grado di assolvere alla loro funzione senza creare problemi di violazione delle leggi sulla privacy.

Il fattore umano

La sicurezza totale di un sistema informativo può essere considerata un limite difficilmente raggiungibile, soprattutto se si tiene conto di variabili non controllabili e non prevedibili, tra le quali il "fattore umano" gioca indubbiamente un ruolo di primaria importanza.

Basta fare un giro nelle aule universitarie o negli uffici pubblici: foglietti dimenticati di fianco a una postazione con riportati a caratteri cubitali nomi utenti e password; comunicazioni di password ad alta voce tra amici o colleghi; postazioni abbandonate in fretta senza effettuare il *logout* dalla rete e nemmeno dalla posta elettronica web, computer portatili lasciati in giro con all'interno cookies, password o documenti aperti e non protetti. E ancora: l'apertura di e-mail provenienti da sconosciuti e recanti allegati "sospetti" (i classici file `.exe`, ma non solo...); il computer lasciato acceso e incustodito; la scelta di password banali (per esempio il nome proprio come username e il cognome come password) o troppo corte; l'installazione di programmi contenenti algoritmi in grado di violare la privacy (i cosiddetti *spyware*) inviando a insaputa dell'utente suoi dati personali ad altri computer collegati alla Rete; la navigazione nel Web senza particolari precauzioni e senza preoccuparsi di verificare la provenienza di eventuali software richiesti dal browser, e via dicendo.

Tutti questi atteggiamenti a rischio sono ricollegabili per lo più a situazioni di distrazione, imprevedibilità, eccesso di **self-confidence** e di buona fede negli atteggiamenti corretti degli altri, oppure semplicemente a una generale sottovalutazione delle conseguenze di determinate azioni.

In ambito aziendale si può cercare di ovviare a molti di questi comportamenti mediante l'adozione di una *policy* relativa alla sicurezza, al cui rispetto siano tenuti tutti gli utenti del sistema informativo: l'utilizzo programmato di firewall; la realizzazione di frequenti copie di backup dei dati; l'aggiornamento dei sistemi tramite i file di correzione resi disponibili dalle software house in seguito alla scoperta di particolari vulnerabilità sul piano della sicurezza. Ma anche regole relative alle password: lunghezza minima, forma (possibilmente un giusto mix di lettere, numeri, simboli) e contenuto (non banale), custodia sicura, data di scadenza (che implica un obbligo di modifica delle password nel tempo).

È opportuno sottolineare l'importanza della frequenza con cui devono essere cambiate le password. Modificando spesso la password di accesso a dati, documenti o al sistema, si incorre più difficilmente a intrusioni da parte di utenti non desiderati.

A livello aziendale la definizione di una politica relativa alla sicurezza non può tuttavia prescindere dalla diffusione di una *cultura* della sicurezza, tramite processi di comunicazione interna e trasparenza supportati da adeguate campagne di sensibilizzazione e formazione.

Implicazioni in caso di furto di un laptop, di un PDA o di un telefono cellulare

Il salvataggio di qualsiasi dato acquisito – che si tratti di file, di dati anagrafici, indirizzi, numeri di telefono o altro – su altre unità di supporto è una buona abitudine che tutti gli utenti dovrebbero acquisire. Tale buona abitudine si rende ancora più necessaria soprattutto se si sta utilizzando un laptop, un PDA o un telefono cellulare. Infatti tali dispositivi, viste le loro dimensioni e per il fatto stesso di essere apparecchiature portatili, sono maggiormente esposti al rischio di furto. Ovviamente, nel caso in cui non si sia provveduto a salvare altrove i dati contenuti all'interno delle memorie, tali dati possono essere considerati definitivamente perduti.

A scopo cautelativo è sempre consigliabile proteggere i dati tramite l'utilizzo di password, nel caso di laptop o PDA, o di codici PIN (*Personal Identification Number*), nel caso in cui si vogliano proteggere i dati contenuti nella memoria SIM del cellulare. In questo modo ci si assicura che gli eventuali ladri non possano usufruire delle informazioni personali, anche se ciò non aiuta a rientrare in possesso del proprio apparecchio.

Per quanto riguarda i cellulari, è possibile bloccarli, in caso di furto, grazie al codice IMEI che li contraddistingue; in questo modo i cellulari segnalati verranno inibiti dalle reti dei gestori telefonici. Per quanto riguarda la SIM card, invece, sarà possibile richiedere una sostituzione che permetta di mantenere lo stesso numero telefonico.

Soprattutto negli ambiti in cui la protezione dei dati e dei dispositivi risulta di primaria importanza vengono usati anche altri accorgimenti, come cavi di sicurezza, che fissano le apparecchiature a tavoli e scrivanie in modo da prevenirne il furto.

Virus

I problemi legati ai virus

Parlando di sicurezza deve essere fatto cenno anche ai virus che costituiscono una delle principali cause di perdita dei dati o danneggiamento dei componenti del nostro PC.

I virus sono programmi appositamente scritti per danneggiare in vario modo i PC: per esempio possono rendere inutilizzabile l'hard disk, cancellare file, rallentare il funzionamento del PC, ridurre lo spazio disponibile nella memoria principale.

In genere un virus si diffonde tramite Internet o posta elettronica oppure attraverso lo scambio fisico dei supporti di memorizzazione (floppy disk, CD-ROM, pen drive).

Per prevenire l'attacco e il contagio da virus informatici deve essere installato un **programma antivirus**, che riesce ad individuare ed eliminare i virus che stanno tentando di infettare o che hanno già infettato il computer.

Vista l'alta frequenza con cui vengono messi in circolazione nuovi virus l'antivirus deve essere sempre aggiornato.

1.8 Diritto d'autore e aspetti giuridici

Copyright

Il copyright del software

Dal primo gennaio 1993 anche l'Italia ha una definitiva e chiara legge a tutela del software (DPR 518 del 29/12/92). Questa legge ha di fatto recepito una direttiva dell'Unione Europea (91/250), che riconosce il software come opera dell'ingegno umano, quindi lo protegge nell'ambito del diritto d'autore, o **copyright**. Copiare software è un reato perseguibile sia civilmente che penalmente e si rischiano multe da 500 a 5000 euro e pene reclusive da 3 mesi a 3 anni!

Di recente, è stata definitivamente approvata la nuova legge sul diritto d'autore – la controversa Legge 248 del 2000 –, che è ormai entrata in vigore a tutti gli effetti. Tra i vari punti affrontati vi sono quelli relativi alla copia di software, film, CD musicali: un vero e proprio business, che nel 2000 ha superato i 500 milioni di euro (soltanto le copie dei software hanno raggiunto i 335 milioni, pari al 44 per cento del mercato).

La legge diventa più dura, e mira a colpire tutti in modo molto severo. Infatti, in base al testo dell'articolo 171-bis, copiare un programma, un file musicale o video è reato anche senza scopo di lucro: al termine "lucro" è stato sostituito il più generico termine "profitto". Profitto come quello di un utente che si fa copiare un software da un amico per installarlo nel computer di casa, o che compra una copia e la installa in due computer, magari il suo e quello del figlio: si tratterebbe di profitto, perché risparmia i soldi che avrebbe speso comprando il programma originale (o il CD musicale, o la videocassetta). Il discorso, giusto in termini generali, si fa un po' pesante se rapportato ai singoli casi personali. Le pene previste sono la reclusione da sei mesi a tre anni, e multe da circa 2500 euro a 15.000 euro. Questo, in teoria, significa che anche la copia di un software che costa 5 euro, magari acquistato via Internet per sé, quindi senza scopi di business, e messo in uso nel computer del figlio, oppure prestato alla scuola, può far condannare chiunque alle pene previste, per niente leggere.

Cosa significa copiare software?

Prima di tutto va precisato che, se si parla di copie non autorizzate, il termine "software" indica esclusivamente i programmi e non i documenti (file) realizzati mediante i primi, che possono essere liberamente copiati.

È già stato detto che, al momento dell'acquisto del programma, viene rilasciata la **licenza d'uso**: un contratto, diretto o indiretto, stipulato tra il proprietario del software e l'utente. Il titolare della licenza può installare il programma sul proprio computer e farne eventualmente una copia di backup per sicurezza. Non può invece, secondo la legge, installare il programma su un altro computer, copiarlo per ragioni diverse dal creare una copia di sicurezza, come per regalarlo, prestarlo o addirittura venderlo ad altre persone, oppure metterlo a disposizione tramite Internet o reti di computer.

La licenza è strettamente legata a un numero di serie del prodotto software. In ogni programma è presente una sezione contenente le informazioni generali sul rilascio della licenza in cui è possibile anche verificare questo numero, di solito utilizzato per identificare prodotti distribuiti senza autorizzazione.

È possibile stipulare anche **licenze d'uso multiple**, che prevedono un uso più ampio del software, permettendo di installare il programma su più di un computer, purché ciò rientri nel limite superiore previsto dal contratto.

È importante precisare che chi acquista o riceve software copiato (in gergo si dice "piratato") da un rivenditore o da un altro soggetto può essere perseguibile legalmente per ricettazione. Per evitare di imbattersi in grane giudiziarie, prima di utilizzare o copiare un programma è dunque bene assicurarsi di essere in possesso della licenza d'uso. Chiaramente quest'ultima ha quasi sempre un prezzo, che è più o meno alto a seconda del programma cui si riferisce.

Software freeware e shareware

Alcuni programmi, per esempio quelli che vengono allegati a riviste specializzate, presso rivenditori di software o su Internet, possono essere utilizzati liberamente perché sono sprovvisti di licenza d'uso o ne prevedono una gratuita. I software che non hanno licenza d'uso sono definiti di **dominio pubblico**, mentre quelli a licenza gratuita possono essere di due tipi: i **freeware** che hanno licenza illimitata e gli **shareware**, la cui licenza è gratuita per un periodo di tempo, al termine del quale il programma deve essere disinstallato dal proprio PC, a meno che non venga acquistata la licenza.

Un'attenzione particolare meritano i programmi che si possono copiare da Internet: alcuni siti offrono programmi shareware, freeware o addirittura commerciali; è compito di chi scarica il programma assicurarsi che il sito sia di comprovata serietà.

I software con restrizioni con restrizioni sull'utilizzo, modifica, riproduzione o distribuzione vengono definiti software proprietari. Per software di questo tipo la licenza è chiamata EULA e tipicamente non permette di modificare il programma, di installarlo su altri computer, di metterlo a disposizione tramite Internet o reti di computer oppure di copiarlo per ragioni diverse dal backup (per esempio regalarlo, prestarlo o venderlo ad altre persone).

Protezione dei dati personali

La protezione dei dati personali

Uno degli usi più frequenti del computer consiste nel trattamento e nell'archiviazione dei dati, i quali in molti casi sono di carattere personale. Per *dato personale* si intende qualunque informazione relativa a persona fisica o giuridica identificabile a partire dai dati stessi. Sono per esempio dati personali quelli anagrafici, come il nome e il cognome, l'età o il sesso, ma lo sono anche lo stato di salute, i dati razziali, le opinioni religiose, politiche o sindacali.

I dati personali sono raccolti in genere da enti pubblici e privati, come banche, ospedali, forze di polizia, uffici del lavoro, che li utilizzano per specifiche finalità riguardanti la propria attività. Ulteriori esempi di sistemi informativi della Pubblica Amministrazione che possono contenere dati personali sono la motorizzazione civile, l'anagrafe centrale, i registri elettorali, la previdenza sociale, i registri delle biblioteche, il casellario giudiziario e la campagna di censimento da parte dello Stato.

L'uso con fini diversi da quelli per cui sono stati raccolti può provocare danni non marginali al cittadino o all'organizzazione alla quale si riferiscono i dati. Si pensi per esempio alle cartelle cliniche ospedaliere, le quali potrebbero contenere delle informazioni sensibili, utilizzabili in modo discriminatorio da un possibile datore di lavoro. È evidente quindi che un'informazione utile dal punto di vista clinico deve essere usata soltanto per lo scopo per il quale è stata raccolta; ogni altro utilizzo è improprio e, come tale, un grave abuso e un attentato alla *privacy* (riservatezza) dell'individuo. Per questo motivo è responsabilità dell'organismo che tratta dati personali, con o senza l'ausilio dell'informatica, custodirli e controllarli in modo da ridurre al minimo i rischi di distruzione o perdita, di accesso non autorizzato o di trattamenti non consentiti o non conformi alle finalità della raccolta.

È opportuno sottolineare che le informazioni personali memorizzate in banche dati informatiche sono spesso consultabili da vari utenti, talvolta non autorizzati. Per questo motivo è necessario aumentare la salvaguardia e la tutela dei dati personali.

Decreto legislativo 196/03

In Italia questa materia è regolata dal **decreto legislativo 30/06/2006 n. 196**, in G.U. 29/07/03, Serie gen. n. 174, Suppl. ord. n. 123/L, in vigore dal 1/01/2004. Esso sostituisce la Legge n. 675/1996 e successive disposizioni modificative ed integrative.

Di seguito vengono riportati i primi tre articoli del decreto.

Diritto alla protezione dei dati personali (Art. 1)

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Finalità (Art. 2)

- Il "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
- Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Principio di necessità nel trattamento dei dati (Art. 3)

Il decreto riconosce il diritto assoluto sui dati personali e di conseguenza ne regola le diverse operazioni di trattamento, riguardanti la raccolta, l'elaborazione, la cancellazione o la diffusione. Tale normativa si applica al trattamento dei dati nel territorio dello Stato Italiano con o senza l'aiuto di mezzi elettronici o automatizzati. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

L'organizzazione che intende trattare dati personali, deve rispettare numerosi obblighi, tra cui:

- comunicare al Garante della privacy le sue intenzioni ed in alcuni casi attenderne un'autorizzazione;
- nominare un responsabile per il trattamento delle informazioni;
- richiedere un consenso scritto alla persona a cui si riferiscono i dati ed informarla sullo scopo di tale raccolta e sulle modalità di gestione;
- adottare misure preventive di sicurezza idonee a garantire la custodia ed il controllo dei dati.

Si rimanda al sito del Garante della Privacy (`http://www.garanteprivacy.it`) per ulteriori approfondimenti.