Comune di Assago

Provincia di MI

Documento Programmatico sulla Sicurezza

ALLEGATO I

"Disciplinare in materia di utilizzo del Sistema Informatico"

Il presente documento è stato emesso il giorno 31 marzo 2011, è stato redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g del D.Lgs 196/2003 e del Disciplinare Tecnico allegato al medesimo decreto sub b.

Data di stampa: 31 marzo 2011

Indice

Art. 1 Oggetto e ambito di applicazione

La progressiva diffusione delle nuove tecnologie informatiche espone l'Ente ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Ente ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Art. 2 Utilizzo dei Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e pertanto è vietato.

In particolare:

(a) L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall' Amministratore di Sistema con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema;

(b) L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno;

(c) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screen saver e la relativa password;

(d) L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato;

(e) È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

(f) È vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita dell'Amministratore di Sistema;

(g) È vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'Amministratore di Sistema;

(h) È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Art. 3 Utilizzo della Rete Informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

Si parte quindi dal presupposto che i files relativi alla produttività individuale vengono salvati sul server e i limiti di accesso sono regolarizzati da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

L'amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei files con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema. Sarà compito dell'Amministratore di Sistema provvedere alla creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica è fatto divieto di:

(a) Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;

(b) Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete dell'Ente;

(c) Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

(d) Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);

(e) Installare componenti hardware non compatibili con l'attività istituzionale;

(f) Rimuovere, danneggiare o asportare componenti hardware;

(g) Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;

(h) Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;

(i) Usare l'anonimato o servirsi di risorse che consentano di restare anonimi;

Art. 4 Utilizzo delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Incaricato della custodia delle Password.

È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, D.lgs. n.196/2003) con contestuale comunicazione all'Incaricato della custodia delle Password.

La comunicazione di variazione delle password dovrà avvenire secondo la modulistica prevista dal Custode e dovrà essere consegnata in busta chiusa, con data e firma dell'incaricato apposte sul lembo di chiusura.

Qualora la password non venga autonomamente variata dall'incaricato entro i termini massimi, l'utente verrà automaticamente disabilitato.

Sarà quindi necessario rivolgersi all'Amministratore di Sistema dell'Ente, il quale provvederà a riabilitare l'utente ed assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

La password deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle Password, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, all'Amministratore di Sistema dell'Ente.

Art. 5 Utilizzo dei Supporti Magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.

Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 6 Utilizzo di PC Portatili (notebook)

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, seminari, ecc...), in caso di allontanamento devono essere custoditi in un luogo protetto.

Art. 7 Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Art. 8 Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.lgs. n. 196/2003.

Art. 9 Amministrazione delle risorse informatiche

L'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle Risorse Informatiche dell'Ente e a cui sono consentite in maniera esclusiva le seguenti attività:

(a) Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Ente collegate in rete o meno;

(b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica dell'Ente secondo quanto stabilito da ogni Capo Area;

(c) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

(d) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

(e) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

(f) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

(g) Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Capo Area dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Art. 10 Reato di omessa custodia del personal computer da parte di un dipendente pubblico

Il tema della criminalità c.d. informatica si è andato sempre più manifestando e imponendo agli occhi di tutti a partire dagli anni '80, favorito dalla diffusione degli elaboratori elettronici non solo in ambiente di lavoro ma anche domestico e, successivamente, da una serie di strumenti in grado di permettere di elaborare dati (telefonini, palmari, i.pod, ecc.) anche in ambienti domestici.

In Italia, il legislatore ha affrontato in maniera organica tale problematica attraverso la Legge n. 547 del 1993. Tale legge ha introdotto una serie di condotte illecite poste in essere su elaboratori elettronici.

Art. 10.1 La responsabilità amministrativa del pubblico dipendente

La norma fondamentale in materia di responsabilità amministrativa del personale degli enti pubblici, resta il r.d. n. 2440 del 18.11.1923, secondo cui "L'impiegato che per azione od omissione, anche solo colposa, nell'esercizio delle sue funzioni, cagioni danno allo Stato, è tenuto a risarcirlo".

La nozione di colpa consiste in un comportamento cosciente dell'agente, che, sia pure senza volontà di recare danno ad altri, causa un evento lesivo per negligenza, imprudenza, imperizia, ovvero per inosservanza delle regole o norme di condotta.

La colpa può consistere oltre che nella violazione di leggi e di regolamenti, in negligenza o violazione di particolari discipline.

Integra una fattispecie di colpa, sotto il profilo della imperizia o negligenza, l'inosservanza di regole tecniche idonee ad evitare o diminuire un danno che, benché non tradotte in leggi o regolamenti, siano però entrate nell'uso corrente ed abitualmente applicate.

Si ha fatto colposo, non soltanto per l'inosservanza di legge, ma anche quando l'evento dannoso si verifica a causa di negligenza o imprudenza, indipendentemente dalla volontà dell'agente di produrre l'evento stesso. Quando una norma giuridica prescrive l'uso di una determinata cautela al fine di evitare eventi di danno, la prescrizione è usata nella presunzione che quella cautela

sia idonea ad impedire il verificarsi del sinistro. Oltre alla violazione di una regola di condotta, si richiede anche la coscienza e volontà dell'atto illecito.

Art. 10.2 La responsabilità patrimoniale

La Costituzione attraverso il secondo comma dell'art. 103 stabilisce che "la Corte dei Conti ha giurisdizione nelle materie di contabilità pubblica e nelle altre specificate dalla legge".

Si è così fatta luce sulla giurisdizione della Corte dei Conti che risulta, per l'appunto, limitata alla "contabilità pubblica".

Con tale nozione deve intendersi la materia di contabilità pubblica in tutti quei rapporti – di responsabilità per danni nel rapporto interno di impiego o di semplice servizio – connessi alla gestione finanziaria e patrimoniale svolta dall'amministrazione dello Stato o di altro ente pubblico.

Elementi che concorrono ad individuare la nozione di contabilità pubblica sono:

(a) l'elemento oggettivo della "qualificazione pubblica del denaro o del bene"

(b) l'elemento soggettivo, rappresentato dalla natura pubblicistica dell'ente in questione.

Si può quindi affermare che "la responsabilità patrimoniale, individuata dalla disposizione del secondo comma dell'art. 103 Cost., può essere complessivamente definita come la responsabilità in cui incorrono i dipendenti e gli amministratori degli enti pubblici nei confronti della stessa p.a., per fatti da loro commessi in dipendenza o comunque in connessione con il loro rapporto con l'ente pubblico, per violazione specifica o generica dei doveri nei confronti della struttura pubblica, causa di un pregiudizio appunto patrimoniale alla pubblica amministrazione".

Art. 10.3 Il reato di omessa custodia del personal computer da parte di un dipendente pubblico

Prima di passare a trattare del reato oggetto di tale dissertazione riteniamo opportuno fornire la definizione dell'elemento costitutivo della fattispecie: il computer.

Il computer è una macchina elettronica statica programmabile strutturata attorno ad un microprocessore, in grado di eseguire calcoli ad altissima velocità. Le applicazioni dei computer sono infinite ma, da un punto di vista oggettivo, il computer è utile e applicabile in tutte quelle situazioni in cui esistono problemi che possono essere tradotti in formule di tipo matematico.

Il reato di omessa custodia di un personal computer è un reato colposo di tipo omissivo che si verifica allorché un soggetto – pubblico dipendente –assegnatario di un elaboratore elettronico – pc –omette di custodirlo e a seguito di tale condotta negligente si determina la sottrazione dello strumento informatico sic et simpliciter oppure il suo utilizzo per fini non legittimi; comunque, in entrambi i casi si verifica un danno all'Ente.

La omissione, in questo caso, consiste nel mancato compimento di una azione possibile che il soggetto ha il dovere di compiere e che la legge penale comanda di realizzare,. Precisamente, si tratta di un reato omissivo proprio, o di pura omissione, consistente nel mancato compimento dell'azione comandata (=mancata applicazione delle misure minime di sicurezza, così come disposte dal Codice in materia di protezione dei dati personali).

Ciò lo si desume dal punto 9 dell'Allegato B- Disciplinare Tecnico in materia di misure minime di sicurezza, al Decreto Legislativo n. 196/2003. La violazione di tale disposizione comporta la applicazione delle sanzioni penali in quanto rappresenta una violazione delle misure minime di sicurezza, che devono essere adottate da chi tratta dati personali.

A tale riguardo l'art. 33 del D:lgs 196/03, recita "Nel quadro dei più generali obblighi di sicurezza di cui all'art. 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali".

Il Disciplinare tecnico richiede che sia attuata la protezione degli strumenti elettronici e dei dati rispetto ai trattamenti illeciti di dati, agli accessi non consentiti, e a determinati programmi informatici.

Occorre, pertanto, dare attuazione ad una serie di misure minime di sicurezza che, nel caso specifico, saranno di tipo informatico (password, sistema di autenticazione, sistema di autorizzazione, antivirus, ecc); organizzative (formazione del personale) e logistiche (porte allarmate, .telecamere, ecc.).

Tale reato contravviene all'obbligo di impedire il verificarsi di un evento lesivo (= la sottrazione e/o l'utilizzo illegittimo del pc) e deve esserci una connessione tra l'evento stesso (=sottrazione e/o illegittimo uso del pc) e la condotta omissiva (= il soggetto assegnatario).

Art. 10.4 Pronunce Giurisprudenziali

La Corte dei Conti è stata chiamata a pronunciarsi sul caso di furto di due personal computer portatili avvenuto presso un Comando provinciale dei Vigili del fuoco. Il caso ha per oggetto due funzionari - consegnatari dei pc che sono stati sottratti. Ai due dipendenti in questione – è stato inoltrato un "invito alle controdeduzioni", ritenendo l'Amministrazione ricorrere l'ipotesi di illecito amministrativo ex art. 1. L. n. 20/1994.

Mediante tale "invito" si è fatto presente che la perdita del pc portatile è da considerarsi avvenuta a causa dell'incauta condotta del consegnatario, che non si è preoccupato di custodire adeguatamente il computer, lasciandolo in vista in un posto accessibile.

Uno dei due dipendenti ha fatto notare che "il personal, per motivi tecnici legati ad una migliore visione, era collegato ad un monitor a tubo catodico, sempre presente sulla scrivania, e ad una stampante allo stesso modo posta sulla scrivania. In tale situazione le continue connessioni della stampante con il computer in modalità Stand –by, potevano compromettere le funzionalità del PC, ovvero i dati in esso contenuti per mancanza di idonee protezioni hardware contro l'accumulo di cariche elettrostatiche.

Ciò considerato il Pc portatile era pertanto a svolgere le funzioni di un PC da Tavolo".

Il dipendente, a sostegno della sua difesa faceva presente inoltre che "il computer in questione conteneva i software di gestione delle emergenze che dovevano essere disponibili a tutti i colleghi funzionari in servizio presso il Comando, ... e, quindi, il PC doveva rimanere sulla scrivania, nelle condizioni d'uso, accessibile agli altri possibili utilizzatori".

In merito ad eventuali misure di sicurezza da adottare a salvaguardia del computer, il dipendente precisa che "la chiusura a chiave dell'accesso all'ufficio non era possibile, non essendovi, all'epoca dei fatti, dotazione di chiavi, e che non vi erano ordini di servizio in tal senso, anche perché ciò avrebbe impedito l'uso del PC da parte di altri funzionari".

La Procura regionale, non ha ritenuto sufficienti gli elementi addotti dal funzionario in quanto lo stesso "avrebbe dovuto assumere tutte le misure idonee ad evitare rischi di trafugamento del compiuter, quali, in particolare la chiusura a chiave della stanza o il riporre il PC in un cassetto o in un armadio" e lo citava in giudizio ritenendo che sussistesse una ipotesi di responsabilità amministrativa.

In giudizio la difesa del funzionario sosteneva che "sarebbe assente il nesso causale tra il comportamento del ..(funzionario) ed il furto poiché la sottrazione si è verificata a causa della prassi, instauratasi prima della sua presa di servizio, di libero accesso agli uffici, oppure per il comportamento disattento del personale in servizio nei giorni in cui avvenne".

Sempre secondo la difesa dell'imputato, "mancherebbe inoltre l'elemento della colpa grave, atteso che ... (il funzionario) non ha avuto alcun comportamento negligente, considerata l'oggettiva necessità di lasciare collegato il p.c. ad altre periferiche sulla scrivania nelle condizioni d'uso".

Attesa la obsolescenza del computer all'epoca dei fatti per la difesa mancherebbe anche "il danno erariale".

La Corte dei Conti ha così deciso: "L'ipotesi di danno erariale sottoposta al giudizio di questa Corte è collegata al comportamento del convenuto, che in qualità di consegnatario di un computer... avrebbe causato con la propria incauta condotta la sottrazione dello strumento operativo, per non averlo cautamente custodito, lasciandolo in vista in un posto accessibile".

Nel merito della causa, "Il collegio rileva come l'accertamento della sussistenza o meno della colpa grave nel comportamento contestato al convenuto sia assorbente di tutte le altre questioni. La responsabilità per colpa sussiste solo nei limiti in cui sia individuabile un comportamento non conforme al buon andamento... In sostanza , la colpa va valutata in riferimento all'attività di cooperazione richiesta, cioè come comportamento all'evidenza non adeguato a tali fini o a tali criteri".

In buona sostanza, il collegio giudicante, richiamando la legge n. 639/96, ha sancito che la responsabilità contabile a carico del dipendente sussiste solo "allorché l'attività del pubblico operatore si discosti ampiamente da tali indici di adeguatezza".

Il Collegio, pertanto, non ha accolto la richiesta della Procura regionale dovendo ritenersi rilevante "il fatto evocato dalla difesa della necessità di lasciare in disponibilità d'uso il computer anche e soprattutto nei momenti di assenza dal servizio da parte del convenuto, ai fini della gestione di una eventuale emergenza".

Altra pronuncia giurisprudenziale che si porta alla attenzione del lettore riguarda il caso di un dipendente dell'Agenzia delle entrate accusato di avere lasciato incustodito il PC.

Ci riferiamo alla sentenza della Corte dei Conti della Sicilia chiamata a pronunciarsi sul caso di un dipendente della Agenzia delle entrate, assegnato all'uso di una postazione informatica. Lo stesso dopo una ispezione dalla quale era emersa una anomalia nelle procedure di sgravio, aveva negato di essere stato l'autore materiale della irregolare procedura di sgravio, ma aveva al contempo ammesso di avere lasciato incustodita la postazione in modalità tale da consentire l'accesso a terzi estranei.

Ebbene, "Il procuratore regionale della Corte dei conti ha rilevato che il negligente comportamento del dipendente aveva prodotto una grave inosservanza delle disposizioni dettate dall'Agenzia sulle modalità di utilizzo del sistema operativo, inerenti l'utilizzo del sistema operativo nell'ipotesi di temporaneo allontanamento dalla postazione di lavoro nella fase di trattamento di dati sensibili.".

Il Collegio ha fatto propria la tesi esposta dalla procura in merito al "comportamento gravemente colposo del convenuto, dalla cui postazione informatica, lasciata incustodita ed attiva (con la "password" personale assegnata al dipendente inserita) è stato operato illecitamente l'indebito sgravio di imposta in favore di un contribuente".

A parere della Corte "la negligenza del convenuto è consistita nella violazione delle disposizioni di servizio impartite... agli operatori incaricati del trattamento di dati sensibili mediante procedura informatica. Tali disposizioni impongono lo spegnimento del personal computer al termine della giornata di lavoro,... e, nell'ipotesi di un momentaneo allontanamento, l'attivazione della funzione di blocco della postazione oppure, nel caso in cui non sia possibile il blocco, lo spegnimento del computer".

Art. 10.5 Conclusione

La mancata custodia della propria postazione informatica, da parte del dipendente pubblico preposto, assume una particolare rilevanza alla luce sia delle ipotesi criminose riguardanti la sottrazione dell'elaboratore elettronico sia, soprattutto, alla luce delle disposizioni contenute in materia di trattamento dei dati personali.

Tale problematica va, quindi, affrontata previa sensibilizzazione degli utenti pubblici al problema e delle conseguenze ad esso connesse.

Molto si dovrà lavorare sul versante della formazione del personale incaricato a trattare i dati personali con strumenti elettronici; formazione che, peraltro, rientra tra le misure minime di sicurezza che il Titolare del trattamento dei dati deve adottare.

Allorché il settore pubblico si trova a dovere competere con quello privato, la gestione del dato contenuto nel computer, perché è di questo che si tratta, la sua sicurezza, le sue modalità di trattamento diventeranno gli elementi di valutazione di una amministrazione efficace ed efficiente.

Un ente che non sia in grado di proteggere i suoi dati, e, quindi, la strumentazione informatica attraverso i quali vengono trattati, è destinato a scomparire dal mercato!

Art. 11 Non osservanza del regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

Se i lavoratori perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il datore è autorizzato a procedere per step, con controlli prima sul reparto, poi sull'ufficio ed, infine, sul gruppo di lavoro; solo a questo punto, ripetendosi l'anomalia, sarà lecito il controllo su base individuale.

Art. 12 Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Consulente della struttura. Il presente Regolamento è soggetto a revisione con frequenza annuale.

Assago, lì 31 marzo 2011.

il Titolare del trattamento
GRAZIANO MUSELLA