



PRIVACY

**S**ono numerosi gli enti pubblici e privati che, quando un computer ha superato la fase di utilizzo utile, decidono di eliminarlo dal parco informatico.

Le modalità di eliminazione sono numerose e vanno dalla donazione ad enti benefici, posti in Italia e all'estero, al conferimento ad enti specializzati, in qualità di rifiuti di apparecchiature elettriche ed elettroniche. Questi rifiuti devono essere distrutti in condizioni controllate, in modo da recuperare, per quanto possibile, tut-

BancaMatica

aprile '09

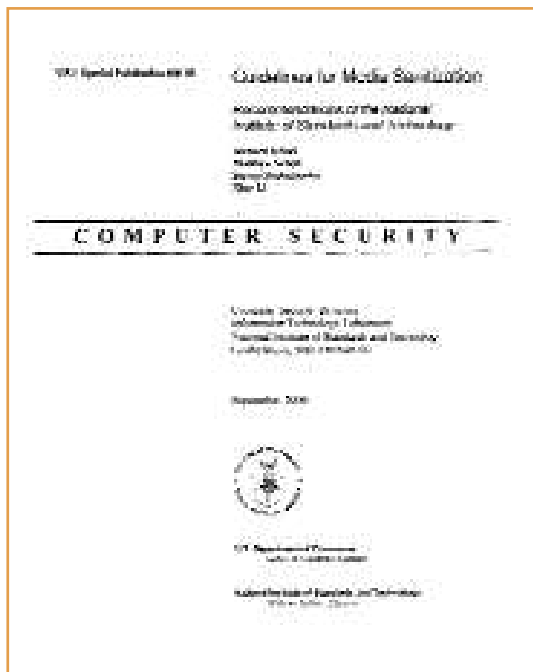
40

# I problemi del vecchio PC regalato alla parrocchia!

Adalberto Biasiotti

**AFFRONTIAMO OGGI  
UN TEMA MOLTO DELICATO,  
SUL QUALE IN PASSATO SONO  
STATE RISCONTRATE  
NUMEROSE VIOLAZIONI.**

ti i componenti riciclabili ivi presenti. Occorre fare attenzione al fatto che molte aziende che ritirano questi apparati non provvedono alla scomposizione in Italia, ma li inviano in grandi container in India, dove la manodopera costa molto meno, e dove giganteschi centri di smaltimento provvedono al recupero di parti in rame, in oro od altro materiale riutilizzabile. Appare evidente che tutte queste modalità di allontanamento di un computer, o più in generale uno strumento informatico, dall'ambito di protezione dell'azienda, debbono comportare la cancellazione dei dati personali ivi presenti. È questo uno specifico obbligo previsto dal disciplinare in materia di misure minime di sicurezza, e non è derogabile. Il fatto che realtà ciò non avvenga è confermato dai numerosissimi casi, citati dalle cronache di tutto il mondo, di computer usati nei quali sono stati ritrovati dati, an-



che estremamente critici, di natura medica, di natura militare e d'altra natura, che non erano stati debitamente cancellati. Ben venga quindi il provvedimento del garante pubblicato in gazzetta ufficiale 9 dicembre 2008, nel quale viene richiamata con incisività all'attenzione di tutti i titolari trattamento dei dati personali, sulle corrette modalità con cui è possibile gestire questa delicata fase di eliminazione di strumenti informatici, contenenti dati personali.

Per la verità, le preoccupazioni del Garante giungono in forte ritardo, rispetto a quanto numerose normative europee ed americane avevano già preso in considerazione.

Ad esempio, risale a molti anni fa una specifica procedura, codificata con apposito documento, che indica le modalità con cui è possibile giungere ad una cancellazione sicura di dati personali su supporto informatico.

Il Garante mette a disposizione, nell'allegato a, alcune alternative, che non necessariamente prevedono la cancellazione dei dati; ad esempio, se i dati sono registrati su supporti informatizzati con procedure crittografiche, la garanzia di non accessibilità dei dati stessi è soddisfacente; con questo accorgimento, ad esempio, l'hard disk può essere riutilizzato, nella porzione libera, senza necessariamente essere distrutto.

La tecnica che molti suggeriscono, vale a dire la formattazione a basso livello o la riscrittura più

volte di serie di zero ed uno sull'hard disk è certamente efficace, ma pone un "piccolo" problema: spesso il tempo necessario per portare a termine queste operazioni, in condizioni tali da garantire un sufficiente livello di cancellazione, richiedono ore ed ore e probabilmente il titolare del trattamento ha altre cose da fare, di natura più pressante!

Di seguito illustriamo quali sono le attuali normative in vigore, alle quali si può fare riferimento in fase di cessione di questi beni a soggetti terzi, che devono formalmente ed esplicitamente impegnarsi a portare a termine le operazioni di cancellazione dei dati, adottando una delle procedure appresso illustrate.

### LE NORMATIVE ESISTENTI IN TEMA DI DISTRUZIONE SICURA DI SUPPORTI INFORMATIZZATI

Le normative esistenti in questo settore sono state per la prima volta elaborate negli Stati Uniti nel 1990, su indicazione di strutture militari.

I militari infatti per primi si erano resi conto della necessità di mettere a punto procedure sicure di distruzione di supporti informatizzati di vario tipo, che potevano contenere dati di estrema criticità.

Il documento elaborato dalla marina degli Stati Uniti nel 1993 ha per lungo tempo rappresentato il riferimento primario per tutti coloro che erano interessati a queste problematiche. Tuttavia il trascorrere degli anni, e soprattutto all'apparizione sul mercato di strumentazioni informatiche ed informatizzate sempre più versatili e complesse, dopo poco ha messo in evidenza la inadeguatezza di questa normativa e la necessità di mettere a punto una normativa più aggiornata.

L'incarico di elaborare questa normativa che è stato affidato al National Institute for Science and Technology - NIST, che da lungo tempo era specializzato nel settore delle normative per i sistemi informatizzati.

Il documento è stato pubblicato nel settembre 2006 ed ancora oggi rappresenta lo standard di riferimento per tutti coloro che debbono attuare procedure di pulizia di supporti informatizzati.

Il pregio di questo documento, oltre ad essere assai aggiornato dal punto di vista tecnico, risiede anche nel fatto che prende in considerazione praticamente l'universo dei supporti, che

tendono a diversificarsi con estrema rapidità. Si pensi ad esempio alle schede che vengono utilizzate nelle macchine fotografiche digitali, alle chiavi USB che oggi sempre più spesso vengono utilizzate per l'archiviazione al trasporto di dati personali, e via dicendo.

Ecco il motivo per cui questo documento prende in esame le modalità di cancellazione di dati presenti sui supporti di tipo magnetico, ottico, elettrico ed altri supporti ancora.

Anche questo documento normativo prende in considerazione vari livelli di cancellazione, proprio in funzione della criticità dei dati.

Giova sottolineare, anche in questo caso, che il responsabile della classificazione del dato è quindi della scelta del livello di cancellazione è sempre il titolare del trattamento di dati personali, oppure il responsabile, cui egli ha affidato la mansione.

La normativa individua diverse modalità di cancellazione dei dati, che sono applicabili a uno o più tipi di supporto.

La norma individua quattro sistemi di cancellazione dei dati, di seguito illustrate:

- l'eliminazione del supporto,
- la cancellazione del dato,
- la cancellazione profonda e
- la distruzione.

Nei paragrafi seguenti esponiamo brevemente il significato e la importanza di queste diverse modalità di cancellazione.

## ELIMINAZIONE

L'eliminazione è l'atto fisico di eliminare puramente e semplicemente il supporto, senza alcun intervento specifico di cancellazione.

Questa operazione viene talvolta effettuata quando ad esempio un articolo di giornale o da altro documento viene gettato nel cestino della carta straccia, senza essere precedentemente distrutto.

## CANCELLAZIONE

La cancellazione è un'operazione assai più impegnativa e, soprattutto per i supporti informatici registrabili, consiste nell'eliminare tutte le informazioni presenti sul supporto, ma rendendo il supporto ancora utilizzabile per future applicazioni.

Giova ricordare al proposito che la cancellazione di un file da un supporto magnetico non necessariamente comporta la cancellazione fisica del file; molto spesso viene semplicemente eliminato nella FAT - file allocation table, il riferimento al nome del file che però continua a essere presente sul supporto magnetico. In pratica, è come se si cancellasse nel catalogo di una biblioteca il titolo di un volume, che però resta disponibile sugli scaffali!

Ecco perché una cancellazione ben fatta prevede come minimo la sovrascrittura di dati sopra i dati esistenti sull'hard disk, in modo da renderli più difficilmente recuperabili.

Esistono in commercio dei software, alcuni di tipo open, che permettono di sovrascrivere dati sopra un supporto magnetico, in modo da rendere inaccessibili dati sottostanti.

Alcuni applicativi ripetono questa operazione più volte, per rendere sempre più difficile il recupero dei dati sottostanti.

Occorre infatti sottolineare che il recupero dei dati sottostanti può talvolta essere possibile, sfruttando il principio della magnetizzazione residua del supporto. Si tratta di una operazione relativamente semplice, che diventa tanto più sicura, quante più volte il supporto magnetico viene nuovamente registrato, a esempio con una serie di 0 ed 1.

Queste tecniche di cancellazione non sono però utilizzabili su supporti magnetici che, per una ragione qualsiasi, non siano accessibili con normali tecniche di lettura e scrittura.

## CANCELLAZIONE PROFONDA (PURGING)

La cancellazione profonda consiste in un intervento specifico, particolarmente adatto per gli hard disk, che sono stati fabbricati dopo l'anno 2001, in tecnica ATA.

In questo caso un attacco di laboratorio può consentire di recuperare i dati, utilizzando speciali applicativi e personale particolarmente addestrato.

Ecco la ragione per la quale la operazione di cancellazione profonda non consiste nella sovrascrittura di nuovi dati, ma nell'applicazione di un intenso campo magnetico, tale da smagnetizzare completamente il supporto magnetico in questione.

Questa operazione, chiamata degaussing, dal nome dell'unità di misura dell'intensità di campo magnetico, il Gauss appunto, consiste nel-

l'espone il supporto magnetico ad un campo magnetico estremamente elevato, in modo tale da cancellare qualsiasi diversa forma di magnetizzazione sia presente sulle particelle di ossido di ferro, che costituiscono la superficie del disco registrato o registrabile e il cui cambio di polarità magnetica comporta appunto la memorizzazione dell'informazione.

Esistono dei degausser che sono basati su un potente magnete permanente ed altri basati su elettromagneti, anche essi di grande intensità. Uno dei vantaggi di questa apparecchiatura è che l'apparato è relativamente portatile ed opera in tempi relativamente brevi.

Naturalmente il degausser non è utilizzabile per la cancellazione profonda di supporti non magnetici, come ad esempio i supporti ottici.

## DISTRUZIONE

La distruzione del supporto è evidentemente la soluzione finale alla cancellazione.

Dopo che il supporto è stato distrutto, non può essere più riutilizzato.

La distruzione fisica può essere effettuata utilizzando numerosi sistemi, che prevedono ad esempio la bruciatura, la polverizzazione, la balazione dello strato magnetico e simili.

La distruzione per solito viene utilizzata quando i dati da cancellare sono estremamente critici e si vuole evitare qualsiasi possibile tentativo di recupero. La distruzione può anche essere ragionevolmente compiuta quando il valore del supporto magnetico è estremamente basso e il costo di altri interventi di cancellazione risulterebbero sproporzionati rispetto al valore del supporto da cancellare.

La tecnica della distruzione è evidentemente tanto applicabile a supporti magnetici, quanto a supporti ottici, a condizione che le dimensioni finali dei frammenti del supporto ottico siano relativamente piccoli.

Giova infine sottolineare un altro aspetto, che fa deporre a favore della distruzione, laddove possibile, legato al fatto che oggi sono disponibili servizi di laboratori avanzati, che sono in grado di recuperare dati presenti sui supporti magnetici, apparentemente del tutto irrecuperabili.

Nella **foto 1** presento un supporto magnetico, un hard disk, nel quale un difetto della testina di lettura e scrittura ha profondamente inciso la superficie del disco.

In questo caso l'uso di speciali tecniche permette di recuperare i dati presenti sulla parte non danneggiata.

Parimenti, nella foto allegata viene presentato un personal computer portatile coinvolto in un incendio.

Nel caso della **foto 2**, il supporto magnetico, apparentemente irrecuperabile, può invece essere letto utilizzando speciali applicativi e sfruttando soprattutto il fatto che il supporto magnetico spesso si trova all'interno di un involucro metallico, che in parte lo protegge dagli attacchi dall'esterno.

Ecco la ragione per cui, se si deve procedere alla distruzione di un supporto magnetico, è indispensabile aprirlo ed attaccare direttamente il supporto magnetico, invece che la sua custodia, che è stata progettata appunto per proteggere al meglio il supporto ivi racchiuso.

foto 1



foto 2

