



Come rottamare il pc in tutta tranquillità. Le indicazioni del Garante per la cancellazione sicura dei dati

Non si sa mai chi può sbirciare nella tua spazzatura elettronica. Per questo il Garante ha messo a punto una serie di indicazioni per evitare che, al momento di dismettere apparecchiature elettriche ed elettroniche (anzitutto pc, ma anche cd rom o dvd), rimangano in memoria nomi, indirizzi mail, rubriche telefoniche, foto, filmati, numero di conto bancario, dati personali in generale, anche di tipo sensibile come quelli sanitari, riferiti non solo all'utilizzatore, ma anche a terzi.

Da oggi in poi, privati cittadini, professionisti, ma anche aziende pubbliche che intendono dismettere il proprio "usato" o consegnarlo ai punti di raccolta per lo smaltimento dovranno preoccuparsi di cancellare in maniera definitiva - anche con l'aiuto degli stessi rivenditori o se proprio necessario di tecnici specializzati - i dati personali memorizzati. Questo innanzitutto allo scopo di non esporsi e non esporre altri a rischi anche gravi, come ad esempio la manipolazione di dati e il furto di identità.

Sempre più frequenti sono i casi in cui si segnala il ritrovamento di dati personali all'interno di apparecchi elettronici (compresi i telefonini), non solo nei casi in cui essi siano ceduti ad un rivenditore per la dismissione o la rivendita, ma anche quando siano dati in consegna per riparazioni o sostituzione di componenti.

Le misure suggerite dal Garante per una "rottamazione" sicura di pc e dispositivi elettronici (con un provvedimento di cui è stato relatore Giuseppe Fortunato) hanno dunque l'obiettivo di richiamare tutti gli utilizzatori sulla necessità di assicurare una reale ed effettiva cancellazione dei dati o venga garantita la loro non intelligibilità. Le misure possono essere adottate sia nel momento preliminare della memorizzazione dei dati sia in quello successivo della loro distruzione.

Misure tecniche preventive

È bene proteggere i file usando una password di cifratura, oppure memorizzare i dati su hard disk o su altri supporti magnetici usando sistemi di cifratura automatica al momento della scrittura.

Misure tecniche di cancellazione sicura

La cancellazione sicura delle informazioni su disco fisso o su altri supporti magnetici è ottenibile con programmi informatici di "riscrittura" che provvedono - una volta che l'utente abbia eliminato dei file dall'unità disco con i normali strumenti previsti dai sistemi operativi (ad es., con l'uso del "cestino" o con comandi di cancellazione) - a scrivere ripetutamente nelle aree vuote del disco. Si possono anche utilizzare sistemi di formattazione a basso livello degli hard disk o di "demagnetizzazione", in grado di garantire la cancellazione rapida delle informazioni.

Smaltimento di rifiuti elettrici ed elettronici

Per la distruzione degli hard disk e di supporti magnetici non riscrivibili, come cd rom e dvd, è consigliabile l'utilizzo di sistemi di punzonatura o deformazione meccanica o di demagnetizzazione ad alta intensità o di vera e propria distruzione fisica.

Con questo provvedimento il Garante intende sviluppare una nuova consapevolezza e indicare i modi con i quali rispettare i dati degli altri e tutelarsi rispetto ai propri - commenta Giuseppe Fortunato - La vecchia regola aurea, aggiornata ai nostri tempi vale anche in questo caso: "Non fare ai dati degli altri quello che non vorresti fosse fatto ai tuoi".

Dopo la pubblicazione in Gazzetta Ufficiale il Garante metterà a disposizione sul suo sito www.garanteprivacy.it un documento con le istruzioni per favorire quanto più possibile una cancellazione sicura dei dati.

Roma, 5 dicembre 2008



[doc. web n. 1571514]

Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008

G.U. n. 287 del 9 dicembre 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTI gli atti d'ufficio relativi alla problematica del rinvenimento di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

VISTO il d.lg. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*), con particolare riferimento agli artt. 31 e ss. e 154, comma 1, lett. h), nonché alle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza allegato "B" al Codice;

VISTO il d.lg. 25 luglio 2005, n. 151 (*Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti*), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche ed elettroniche, nonché a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurre la quantità da avviare allo smaltimento (cfr. art. 1, comma 1, lett. a) e b));

CONSIDERATO che l'applicazione della disciplina contenuta nel menzionato d.lg. n. 151/2005, mirando (tra l'altro) a privilegiare il recupero di componenti provenienti da rifiuti di apparecchiature elettriche ed elettroniche (Raee), anche nella forma del loro reimpiego o del riciclaggio in beni oggetto di (nuova) commercializzazione (cfr. in particolare artt. 1 e 3, comma 1, lett. e) ed f), d.lg. n. 151/2005), comporta un rischio elevato di "circolazione" di componenti elettroniche "usate" contenenti dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (quali, ad esempio, coloro che provvedono alle predette operazioni propedeutiche al riutilizzo o che acquistano le apparecchiature sopra indicate);

CONSIDERATO che il "reimpiego" consiste nelle operazioni che consentono l'utilizzo dei rifiuti elettrici ed elettronici o di loro componenti *"allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l'utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti"* (art. 3, comma 1, lett. e), d.lg. n. 151/2005) e il "riciclaggio" consiste nel *"ritrattamento in un processo produttivo dei materiali di rifiuto per la loro funzione originaria o per altri fini"* (art. 3, comma 1, lett. e), d.lg. n. 151/2005);

CONSIDERATO che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);

RILEVATA la necessità di richiamare l'attenzione su tali rischi di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali (di seguito sinteticamente individuati con la locuzione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice), dismettono sistemi informatici o, più in generale, apparecchiature elettriche ed elettroniche contenenti dati personali (come pure dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature);

RILEVATO che la disciplina di cui al citato d.lg. n. 151/2005 e alla normativa secondaria che ne è derivata (allo stato contenuta nel d.m. 25 settembre 2007, n. 185, recante *"Istituzione e modalità di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)"*, nell'ulteriore d.m. del 25 settembre 2007, recante *"Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee"*, nonché nel d.m. 8 aprile 2008, recante *"Disciplina dei centri di raccolta dei rifiuti"*

urbani raccolti in modo differenziato come previsto dall'art. 183, comma 1, lettera cc) del decreto legislativo 3 aprile 2006, n. 152 e successive modifiche") lascia impregiudicati gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nel trattamento dei dati personali (e la conseguente responsabilità);

RILEVATO che ogni titolare del trattamento deve quindi adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice); ciò, considerato anche che, impregiudicati eventuali accordi che prevedano diversamente, produttori, distributori e centri di assistenza di apparecchiature elettriche ed elettroniche non risultano essere soggetti, in base alla particolare disciplina di settore, a specifici obblighi di distruzione dei dati personali eventualmente memorizzati nelle apparecchiature elettriche ed elettroniche a essi consegnate;

RILEVATO che dall'inosservanza delle misure di sicurezza può derivare in capo al titolare del trattamento una responsabilità penale (art. 169 del Codice) e, in caso di danni cagionati a terzi, civile (artt. 15 del Codice e 2050 cod. civ.);

RILEVATO che analoghi obblighi relativi alla destinazione dei dati gravano sul titolare del trattamento nel caso in cui la dismissione delle apparecchiature coincida con la cessazione del trattamento (art. 16 del Codice);

RILEVATO che le misure da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei *personal computer* o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica);

CONSIDERATO che tali misure risultano allo stato già previste quali misure minime di sicurezza per i trattamenti di dati sensibili o giudiziari, sulla base delle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza che disciplinano la custodia e l'uso dei supporti rimovibili sui quali sono memorizzati i dati, che vincolano il riutilizzo dei supporti alla cancellazione effettiva dei dati o alla loro trasformazione in forma non intelligibile;

RITENUTO che i titolari del trattamento, in occasione della dismissione delle menzionate apparecchiature elettriche ed elettroniche, qualora siano sprovvisti delle necessarie competenze e strumentazioni tecniche per la cancellazione dei dati personali, possono ricorrere all'ausilio o conferendo incarico a soggetti tecnicamente qualificati in grado di porre in essere le misure idonee a cancellare effettivamente o rendere non intelligibili i dati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle;

RITENUTO che chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti debba comunque assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

CONSIDERATO che, ferma restando l'adozione di ulteriori opportune cautele volte a prevenire l'indebita acquisizione di informazioni personali, anche fortuita, da parte di terzi, le predette misure, suscettibili di aggiornamento alla luce dell'evoluzione tecnologica, possono in particolare consistere, a seconda dei casi, anche nelle procedure di cui agli allegati documenti, che costituiscono parte integrante del presente provvedimento;

RITENUTA la necessità di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati (art. 154, comma 1, lett. h), del Codice), con riferimento alla dismissione di apparecchiature elettriche ed elettroniche, anche attraverso la pubblicazione del presente provvedimento sulla *Gazzetta Ufficiale* della Repubblica Italiana;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

a. reimpiegate o riciclate, anche seguendo le procedure di cui all'allegato A);

b. smaltite, anche seguendo le procedure di cui all'allegato B).

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

2. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 13 ottobre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

Allegato A) al provvedimento del Garante del 13 ottobre 2008

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cifratura di singoli *file* o gruppi di *file*, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (*file* o collezioni di *file*), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.

2. Memorizzazione dei dati sui dischi rigidi (*hard-disk*) dei *personal computer* o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, *drive* logici, *file-system*) realizzando le funzionalità di un c.d. *file-system crittografico* (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo *personal computer*, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi *software* con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program* o *file shredder*) che provvedono, una volta che l'utente abbia eliminato dei *file* da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

4. Formattazione "a basso livello" dei dispositivi di tipo *hard disk* (*low-level formatting-LLF*), laddove effettuabile,

attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, *floppy-disk*, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione *software* (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

Allegato B) al provvedimento del Garante del 13 ottobre 2008

Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.