GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVVEDIMENTO 13 ottobre 2008. Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali.(G.U. n.278 del 9-12-2008) .

RAEE E PROTEZIONE DEI DATI PERSONALI

Il provvedimento del Garante per la protezione dei dati personali ha riguardo ai c.d. rischi **di accessi non autorizzati ai dati memorizzati**, che sussistono in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento ai sensi dell'art. 3, comma 1, lettera i), decreto legislativo n. 151/2005 – da parte di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attivita', in particolare quelle industriali, commerciali,professionali o istituzionali (c.d «titolari del trattamento» ex art. 4, comma 1, lettera f) del Codice), dismettono sistemi informatici o, piu' in generale, apparecchiature elettriche ed elettroniche contenenti dati personali(come pure da parte dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature).

Il parere del Garante fornisce, quindi, dei chiarimenti interpretativi sul combinato disposto delle norme contenute nel **decreto legislativo 30 giugno 2003, n. 196** (Codice in materia di protezione dei dati personali), con particolare riferimento agli articoli 31 e seguenti e 154, comma 1, lettera h), nonche' nelle regole 21 e 22 del **disciplinare tecnico** in materia di **misure minime di sicurezza** allegato «B» al Codice e nel **decreto legislativo 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, nonche' allo smaltimento dei rifiuti), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche e elettroniche, nonche' a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantita' da avviare allo smaltimento (cfr. art. 1, comma 1, lettere a) e b).

Com'è noto, infatti, il decreto legislativo 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 articoli 1 e 3, comma 1, lettere e) ed f) 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).

Il decreto n.151 (e le successive norme secondarie di cui al D.M.25 settembre 2007, n. 185, recante «Istituzione e modalita' di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)»; al D.M. del 25 settembre 2007, recante «Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee», nonche' al 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 responsabilita' (penale ai sensi dell'art. 169 del Codice) e, in caso di danni cagionati a terzi, civile ai sensi degli articoli 15 del Codice e 2050 codice civile) .

Per quanto concerne le misure di sicurezza da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali, le stesse

devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, si' da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilita' 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). Come è noto, tali misure risultano allo stato gia' 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.
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 e' comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilita' di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili.
Per quanto attiene, specificatamente il reimpiego ed il riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche (RAEE) 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 intelligibilita'. 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 puo' con queste procedere alla successiva decifratura. Questa modalita' 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 necessita' 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. Puo' effettuarsi su interi volumi di dati registrati su uno o piu' dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalita' 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 verra' 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'unita' 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 probabilita' 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 capacita' (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocita' 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 inutilizzabilita';

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 piu' funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilita' del dispositivo da parte del sistema a cui e' interconnesso).

Da ultimo, il Garante precisa che in caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche puo' 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 intensita'.