

# Privacy: le nuove regole per l'amministratore di sistema

**C'È TEMPO FINO AL 30 GIUGNO PER ADOTTARE LE NUOVE "REGOLE" RELATIVE ALL'AMMINISTRATORE DI SISTEMA**



**FRANCESCO IPERTI**  
AVVOCATO, SPECIALIZZATO IN DIRITTO  
DELL'INFORMATICA, DOCENTE DELL'UNIVERSITÀ  
LUISS DI ROMA. IDEATORE  
E RESPONSABILE DEL SITO WWW.NEWLAW.IT

Alla vigilia del Natale 2008, è stato pubblicato sulla Gazzetta Ufficiale un provvedimento del Garante per la protezione dei dati personali che ha imposto nuove regole riguardo la figura dell'amministratore di sistema. L'obiettivo della normativa è quello di rendere più trasparente l'operato dell'amministratore di sistema e di adottare regole di designazione e pubblicità verso i terzi simili a quelle previste per i "responsabili" del trattamento. Il provvedimento ha forza vincolante di legge, nonostante sia stato emanato da un organo non tipicamente legislativo. L'entrata in vigore delle regole era stata fissata per metà aprile, di recente è stata prorogata fino al 30 giugno.

## DEFINIZIONE DI AMMINISTRATORE DI SISTEMA

Prima di verificare i nuovi obblighi dettati dal Garante, è opportuno soffermarsi sulle caratteristiche soggettive dell'amministratore di sistema. In realtà, il provvedimento in esame non individua una figura precisa. Anzi, più volte viene evidenziata la necessità di far rientrare nella nozione di "amministratore di sistema" anche figure simili quali gli amministratori di reti, di database eccetera. Il Garante precisa che ai fini del provvedimento non vengono considerate solo le figure professionali finalizzate alla gestione e alla manutenzione di impianti di elaborazione, ma "anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi". Con ciò, evidenziando che dovranno essere assoggettati alle nuove regole anche tutti coloro che svolgono attività tecniche quali il salvataggio

dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware. Peraltro, le attività tipiche degli amministratori di sistema rimangono quelle della custodia delle credenziali e della gestione dei sistemi di autenticazione e di autorizzazione.

## DESIGNAZIONE INDIVIDUALE

L'obbligo di designare un amministratore di sistema e di renderne trasparente detta nomina era previsto nella normativa anteriore rispetto a quella attualmente in vigore. Il Garante sottolinea come nella nuova normativa non vi sia un espresso riferimento a detta figura, ma il ruolo assunto dalla stessa nell'ambito della "società dell'informazione" impone l'obbligo di ripristinarne la designazione individuale. La nomina deve farsi per iscritto con descrizione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. In altre parole, la nomina di amministratore di sistema deve essere fatta senza ricorrere all'istituto della "testa di legno", ma verificando il curriculum (esperienza e capacità) e l'onorabilità (affidabilità) dell'amministratore di sistema il quale dovrà, altresì, godere della piena fiducia del titolare del trattamento.

## PUBBLICITÀ DELLA NOMINA

I dati anagrafici relativi alle persone fisiche nominate "amministratori di sistema", con l'elenco delle funzioni a essi attribuite, devono essere indicati nel Documen-

to Programmatico sulla sicurezza. Qualora il titolare non abbia l'obbligo di redigere il Documento Programmatico sulla sicurezza, è necessario indicare gli stessi dati anagrafici in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

È ovvio che l'obbligo non è valido per il Documento Programmatico che sia stato ultimato entro il 30 marzo di quest'anno (termine ultimo per l'aggiornamento periodico del Dps), ma varrà per la scadenza del prossimo anno.

In caso di attività affidate in outsourcing, il titolare deve conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni.

La pubblicità della nomina deve avvenire attraverso l'informativa rilasciata ai dipendenti al momento dell'assunzione, ovvero attraverso strumenti di comunicazione interna (per esempio, intranet aziendale, ordini di servizio o bollettini). Senza dimenticare la possibilità di inserire detta informazione nell'ambito del "disciplinare tecnico" che, dal 2007, dovrebbe regolamentare l'utilizzo di Internet e posta elettronica a opera dei dipendenti.

### **CONTROLLO DELL'ATTIVITÀ DI AMMINISTRATORE DI SISTEMA**

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i



trattamenti dei dati personali previste dalle norme vigenti. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.