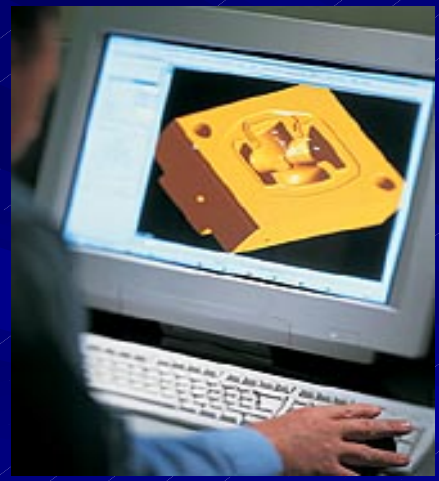
L’amministratore di sistema



di

Michele Iaselli

Definizione

L’Amministratore di sistema viene definito dal provvedimento dell’Autorità Garante del 27 novembre 2008 come una figura professionale destinata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

La definizione un po’ troppo generica è stata successivamente meglio inquadrata dall’Autorità con la pubblicazione delle FAQ dove ha precisato che alla gestione e manutenzione degli impianti di elaborazione va **associato lo specifico trattamento di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi *software* complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.**

In altri termini la figura dell'amministratore di sistema è necessaria qualora vi sia una condivisione nell'ambito del sistema informatico di archivi contenenti dati personali. In caso contrario non ha ragione di esistere.

Nell'ambito della figura degli amministratori di sistema rientrano anche gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.

Chi può essere nominato amministratore di sistema?

In realtà non viene creata una nuova figura nell'ambito del trattamento dei dati personali, ma con amministratore di sistema si intende una mansione specifica altamente specializzata che può essere attribuita ad un responsabile o ad un incaricato purché sia una designazione di carattere individuale.

In linea generale sembra più opportuno che tale figura sia attribuita ad un incaricato del trattamento di dati personali, perché spesso il responsabile del trattamento è il capo del centro elettronico o della struttura informatizzata, cui l'azienda si appoggia. E' naturale, quindi, che a fianco di questo responsabile, operi un incaricato, che ad esempio può costruire i privilegi di accesso ai dati, secondo le istruzioni che vengono impartite dai responsabili coinvolti.

In considerazione delle particolari caratteristiche della funzione di amministratore di sistema, il Garante non esclude nel suo provvedimento la possibilità di avere più amministratori di sistema nell'ambito di una stessa realtà organizzativa, purché gli estremi identificativi delle persone designate con l'elenco delle funzioni ad essi attribuite vengano riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Avuto riferimento a diverse realtà professionali (notai, avvocati, commercialisti), nel caso di grossi studi, il professionista, decide, in genere, di farsi assistere per la propria organizzazione informatica da società esterne che oltre ad assumere la responsabilità del trattamento individuano anche gli amministratori di sistema. In altri casi, però, non si esclude che il professionista possa nominare amministratore di sistema un proprio dipendente purché siano state valutate le caratteristiche soggettive del dipendente e quindi l'esperienza, capacità ed affidabilità. In altri termini il soggetto designato deve fornire un'idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Come si verifica l’attività dell’amministratore di sistema?

Il provvedimento del Garante al punto e) dice: “l’operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un’attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti”. In effetti questo punto va letto in stretto collegamento con quello successivo che parla di registrazione degli accessi logici degli amministratori di sistema. Difatti è grazie a quest’ultima che sarà possibile accertare che le attività svolte dall’amministratore di sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica 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.

Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.

Ma cosa si intende per inalterabilità dei log?

Si intende capacità di mantenimento dell'integrità dei dati raccolti dai sistemi di *log*, requisito che in genere è disponibile nei più diffusi sistemi operativi, o può essere agevolmente integrato con apposito *software*.

Il requisito può essere, quindi, ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati".

Quali sono le responsabilità dell’amministratore di sistema?

Come sottolineato dall’Autorità Garante nel proprio provvedimento, gli amministratori di sistema pur non essendo preposti ordinariamente ad operazioni di carattere amministrativo che comportano un concreto trattamento di dati personali, nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Basti pensare ad 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* che comportano, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Si configurano così una serie di reati informatici che possono essere commessi dall'amministratore di sistema. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 *ter*) e di frode informatica (art. 640 *ter*), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 *bis* e *ter*) e di danneggiamento di sistemi informatici e telematici (artt. 635 *quater* e *quinques*) di recente modifica.

Queste sono le fattispecie di reato che possono vedere responsabile direttamente un amministratore di sistema, ma qualora si configuri una violazione del trattamento dei dati personali non vanno dimenticate le ulteriori fattispecie di violazioni amministrative ed illeciti penali previste dal Codice per la protezione dei dati personali dagli artt. 161 e ss.

In quest’ultimo caso la responsabilità dell’amministratore di sistema dovrà essere accertata caso per caso in quanto se è nominato un responsabile del trattamento dei dati personali, la violazione potrebbe essere anche a suo completo carico.

Cosa succede nel caso in cui un professionista, qualora vi sia tenuto, non nomini un amministratore di sistema?

Il professionista violerebbe un provvedimento di carattere generale emanato dall'Autorità Garante ai sensi dell'art. 154 del Codice per la protezione dei dati personali comma 1 lett. c) ed h).

Tale violazione, al di là degli eventuali risvolti penalistici, comporta l'applicazione della sanzione amministrativa del pagamento di una somma da trentamila euro fino a centosettantamila euro (art. 162 co. 2-ter).