L'amministratore del sistema informatico aziendale: regime normativo e obblighi
Articolo di Luca Giacopuzzi 01.02.2010

| sistema informatico aziendale | Luca Giacopuzzi |

L'amministratore del sistema informatico aziendale:

regime normativo e obblighi di legge

di Luca Giacopuzzi

Sommario: 1) Considerazioni preliminari – 1.1) La portata giuridico-formale del Provvedimento – 1.2) Il campo di applicazione del Provvedimento – 1.3) Chi è l'amministratore di sistema? – 2) Gli adempimenti – 2.1) La valutazione delle caratteristiche soggettive – 2.2) Le designazioni individuali – 2.3) L'elenco degli amministratori di sistema – 2.4) I servizi di amministrazione affidati in outsourcing – 2.5) La verifica delle attività degli amministratori di sistema – 2.6) La registrazione degli accessi logici.

La rilevanza dell'amministratore di sistema nell'ambito delle operazioni di trattamento dei dati è stata considerata anche dal Garante per la protezione dei dati personali, il quale, con proprio provvedimento[1], ha ridefinito ruolo e funzioni di detta figura. Gli adempimenti[2] che ne conseguono costituiscono l'oggetto del presente contributo, che, in particolare, intende dar evidenza delle criticità di maggior impatto.

1) Considerazioni preliminari

1.1) La portata giuridico-formale del Provvedimento

Che rilevanza giuridica ha il Provvedimento? L'azienda è tenuta, o meno, a rispettarne le indicazioni? I quesiti che precedono non possono essere lasciati cadere.

Prima di procedere oltre, giova, pertanto, soffermarci sulle sanzioni che possono essere comminate a coloro che, essendovi tenuti, non si conformano alle prescrizioni del Garante.

La questione richiama, all'evidenza, il più generale tema della vincolatività dei provvedimenti dell'Authority.

Al proposito si deve rilevare che il Garante ha facoltà sia di fornire suggerimenti di carattere meramente divulgativo sia di prescrivere l'adozione di misure che i titolari di trattamento sono tenuti ad adottare.

Nella prima ipotesi le indicazioni sono rese ai sensi della lettera h) dell'art. 154, comma 1, D.Lgs. 196/03 [3], nella seconda ai sensi della lettera c) (del medesimo comma).

Nel caso di specie le prescrizioni maggiormente significative sono emanate ai sensi della sopracitata lettera c), di talchè il mancato rispetto delle stesse, ad un tempo, dà luogo ad una violazione amministrativa[4], ad un illecito penale[5] nonché è fonte responsabilità civile (per inosservanza delle misure di sicurezza "idonee", a tale categoria dovendo essere ascritte, a nostro avviso, le prescrizioni impartite).

1.2) Il campo di applicazione del Provvedimento

Il Garante si rivolge, in linea di principio, a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice.

Precisa, tuttavia, il Provvedimento che al rispetto dello stesso non sono tenuti coloro che trattano i dati a fini amministrativo-contabili (ci si riferisce, in particolare, a quei trattamenti già oggetto di misure di semplificazione: art. 29, D.L. 25 giugno 2008, n. 112, convertito con L. 6 agosto 2008, n. 133; art. 34 del Codice; Provvedimento Garante 6 novembre 2008).

L'individuazione dei trattamenti effettuati a meri fini amministrativo-contabili non è, tuttavia, agevole, attese, da una parte, l'assenza di una definizione normativa e, dall'altra, la polisemia di detta locuzione[6].

Per fare chiarezza, ricorreremo, perciò, ad esempi concreti.

Non risponde a finalità amministrativo-contabili il trattamento di dati sensibili[7], di dati giudiziari[8] o di dati biometrici, né il trattamento a mezzo di sistemi di videosorveglianza, né, ovviamente, l'assai diffuso trattamento a fini di marketing, di profilazione o di fidelizzazione della clientela.

Come si evince dall'elenco che precede (tutt'altro che esaustivo), le aziende che possono disattendere, a ragion veduta, le indicazioni del Garante sono ben poche.

Una precisazione ancora.

Come è stato, peraltro, chiarito dall'Authority, gli oneri di cui al Provvedimento riguardano solo quei soggetti che, nel trattare i dati con strumenti informatici, abbiano fatto ricorso alla figura professionale dell'amministratore di sistema, nei termini di cui si dirà.

Va da sé, pertanto, che tutte le imprese che non si avvalgono di una figura professionale per l'amministrazione del sistema informatico, della rete o delle basi di dati non sono tenute all'adozione delle misure individuate dal Provvedimento.

1.3) Chi è l'amministratore di sistema?

Il Codice non ha incluso l'amministratore di sistema tra le proprie definizioni normative (sebbene detta figura fosse già disciplinata dal D.P.R. 318/99, successivamente abrogato).

In assenza, dunque, di una "nozione giuridica" di amministratore di sistema, cosa deve intendersi con tale locuzione?

Il Garante sul punto è inequivoco, e propone una definizione che si discosta da quella tecnica.

Ed invero, mentre in ambito informatico l'amministratore di sistema è quel soggetto incaricato della gestione e della manutenzione di un impianto di elaborazione (o di sue componenti), ai fini "legali" sono considerati tali anche altri soggetti, equiparabili al primo dal punto di vista della sicurezza dei dati personali.

Ci si riferisce, in particolare, agli amministratori di basi di dati, agli amministratori di reti e di apparati di sicurezza, nonché degli amministratori di applicativi complessi[9], che, in quanto tali, presentano profili di criticità rispetto alla protezione dei dati personali.

Non rientrano, invece, nella nozione di amministratore di sistema coloro che intervengono sugli elaboratori solo occasionalmente (per esempio, a scopo di manutenzione).

L'indicazione (fornitaci dall'Authority) viene spesso "ripresa" dagli outsourcers, che, in forza della sporadicità dei loro interventi (specie nelle aziende di piccola e media dimensione), affermano di non poter essere identificabili come amministratori di sistema.

Non ci sentiamo, in verità, di condividere detta "chiave di lettura". Se agli outsourcers l'impresa ha affidato la gestione del proprio sistema (o di parte di esso), l'identificazione dei loro tecnici come "amministratori di sistema" non può essere fondatamente negata.

2) Gli adempimenti

2.1) La valutazione delle caratteristiche soggettive

In ragione della criticità del ruolo di amministratore di sistema, la relativa designazione deve avvenire previa valutazione dell'esperienza, dalla capacità e dell'affidabilità dell'incaricato.

La regola, che impone all'azienda di attenersi a criteri di selezione equipollenti a quelli richiesti per la nomina dei responsabili del trattamento, non ammette deroghe: il titolare dovrà, quindi, vagliare attentamente le qualità (tecniche, professionali o di condotta) del soggetto individuato, anche in considerazione delle responsabilità, specie di ordine civile e penale[10], che possono conseguire ad una designazione inidonea o incauta.

La natura fiduciaria delle mansioni affidate non viene meno allorchè le funzioni proprie dell'amministratore di sistema (o parte di esse) vengano esternalizzate, secondo una prassi assai diffusa in ambito aziendale.

Non è, dunque, inopportuno sottolineare che la selezione dell'outsourcer deve essere compiuta con particolare rigore e che la scelta dovrà necessariamente ricadere su soggetti alle cui dipendenze operino, quali amministratori di sistema, persone aventi le caratteristiche richieste[11].

2.2) Le designazioni individuali

E'obbligo designare individualmente i singoli amministratori di sistema, a mezzo di un atto che deve elencare partitamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Ciò che il Garante intende evitare è, dunque, l'attribuzione di ambiti non sufficientemente definiti, analogamente a quanto richiesto dal comma 4 dell'art. 29 del Codice in relazione ai responsabili del trattamento.

2.3) L'elenco degli amministratori di sistema

I titolari sono tenuti a riportare in un documento interno gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad esse attribuite.

Qualora gli amministratori, nell'espletamento delle proprie mansioni, trattino (o, semplicemente, possano trattare, anche in via fortuita) dati personali dei lavoratori, questi ultimi hanno diritto di conoscere l'identità dei predetti.

In tal caso, è fatto onere all'azienda di rendere noto[12] ai lavoratori dipendenti detto loro diritto.

Sono possibili diverse modalità: a mezzo dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice o tramite il disciplinare interno relativo all'utilizzo del sistema informatico o mediante altri strumenti di comunicazione interna (per esempio, l'intranet aziendale) o, ancora, avvalendosi di procedure formalizzate, attuabili ad istanza del lavoratore.

2.4) I servizi di amministrazione affidati in outsourcing

Il Provvedimento richiede che, nel caso in cui i servizi di amministrazione di sistema siano esternalizzati, l'elenco di cui al punto che precede sia conservato, indifferentemente, dal titolare o dal responsabile esterno del trattamento (id est, dall'outsourcer).

L'opzione (invero non prevista dal Garante prima della modifica del Provvedimento del 25 giugno 2008) risponde a criteri di buon senso, atteso che per l'azienda può essere molto disagevole recuperare il predetto elenco.

Giova, comunque, rilevare una "distonia" tra la prescrizione in esame (lett. d) del Provvedimento) e l'indicazione di cui si è detto al paragrafo 2.3 (lett. c) del Provvedimento).

Ed invero, mentre la lettera c) prescrive che l'elenco degli amministratori di sistema sia conservato presso il titolare (siano essi amministratori interni o meno, poiché nulla è previsto in relazione ai servizi in outsourcing), la lettera d) consente che l'elenco sia tenuto anche dal solo responsabile esterno, come già osservato.

Riteniamo che l'antinomia tra i due precetti sia frutto di una mera svista del Garante, che, dopo aver modificato la lettera d), non si è curato di intervenire parimenti sulla lettera c), introducendo un'opportuna "clausola di riserva[13]".

2.5) La verifica delle attività degli amministratori di sistema

Allo scopo di contrastare la diffusa sottovalutazione, da parte dell'azienda, dei rischi derivanti da eventuali azioni "incontrollate" degli amministratori di sistema, il Provvedimento introduce verifiche ispettive a carico del titolare o del responsabile esterno.

L'operato degli amministratori di sistema, infatti, deve essere oggetto di verifica, con cadenza almeno annuale, per acclarare che le attività svolte dall'amministratore siano in effetti conformi alle mansioni attribuite.

2.6) La registrazione degli accessi logici

Accanto agli oneri di cui ai paragrafi che precedono (di ordine prettamente "organizzativo"), all'azienda è richiesta anche l'adozione di un'importante misura di carattere tecnico: la registrazione degli accessi logici degli amministratori di sistema.

Il Provvedimento, in particolare, prescrive l'impiego di sistemi idonei alla registrazione degli accessi logici[14] da parte degli amministratori ai sistemi di elaborazione e agli archivi elettronici.

Ciascun amministratore, quindi, deve poter essere identificato.

Va da sé che la cattiva prassi di utilizzare un unico "user-name" (di norma "admin", o simili) condiviso tra tutti gli amministratori non è in linea con le disposizioni del Provvedimento.

In verità, l'anzidetto comportamento costituisce violazione, ad un tempo, del Provvedimento e delle regole dell'Allegato B al Codice (il quale richiede che ciascun incaricato sia dotato di credenziali di autenticazioni univoche).

"Le registrazioni" – si precisa – "devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate".

L'indicazione appare tutt'altro che esaustiva e, al cospetto di detta previsione, molte imprese sono disorientate.

Che fare, dunque, in concreto?

Chiariamo, da subito, che, nel contesto che ci occupa, per "access log" si intende la registrazione degli eventi generati dal sistema di autenticazione informatica a sistemi di elaborazione o di reti o a sistemi gestionali di basi di dati (c.d. "DBMS") o ad archivi elettronici.

Trattasi di evidenze informatiche generate all'atto dell'accesso (o del tentativo di accesso) ad un sistema o all'atto della disconnessione da esso.

Per espressa indicazione del Garante, dette devono contenere, oltre che i riferimenti allo "user-name" impiegato, anche informazioni relative alla data e all'ora dell'evento (time stamp), unitamente ad una sintetica[15] descrizione dell'evento medesimo (sistema di elaborazione o software utilizzato, qualificazione dell'evento come "log-in", "log-out" o "condizione di errore").

Ferme le criticità che precedono, il periodo del Provvedimento che dà luogo alle maggiori perplessità operative è, tuttavia, il seguente: "Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste".

Quale completezza e, soprattutto, quale inalterabilità e quale integrità il log deve, quindi, possedere?

Il quesito è di centrale rilevanza: se, per esempio, a garanzia dell'inalterabilità e dell'integrità si individuassero dei livelli di robustezza rigorosi, le aziende sarebbero sicuramente onerate di aggravi economici significativi (conseguenti all'impiego della firma digitale e della marca temporale in fase di conservazione dei log).

Il Garante è opportunamente intervenuto sul punto, precisando che non vi è alcuna pretesa di instaurare in modo generalizzato un rigoroso regime di registrazione degli "usage data" dei sistemi informativi.

E'stato, anzi, specificato che il requisito dell'inalterabilità dei log può essere ragionevolmente soddisfatto con la strumentazione software già in dotazione alle aziende, e con l'eventuale esportazione periodica dei dati dei log su supporti di memorizzazione non riscrivibili.

Solo in casi più complessi (da valutare in rapporto alle condizioni, organizzative e operative, della struttura) i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e "certificati".

Ci sentiamo di condividere tale impostazione, che, peraltro, riteniamo aderente al dato letterale del Provvedimento.

Detto, infatti, non richiede che il log sia inalterabile "di per sé", ma, piuttosto, esso deve possedere caratteristiche di inalterabilità e possibilità di verifica della loro integrità "adeguate al raggiungimento dello scopo per cui sono richieste". Scopo che, nel caso di specie, è (unicamente) quello, minimale, di verificare "anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, ecc.)" (così, testualmente, il Garante).

Giova sottolinearlo: il Provvedimento non prescrive "misure di polizia" nei confronti dell'attività compiuta dagli amministratori di sistema.

L'operato di questi ultimi, infatti, deve essere oggetto di analisi nel rispetto del principio di proporzionalità (art. 11 del Codice), oltre che, in relazione agli amministratori di sistema "interni" all'azienda, anche della regola di condotta di cui all'art. 4, L. 300/70.

Nessun margine di errore, peraltro, è ammesso in relazione alla tempistica di conservazione dei log, imposta per un "congruo periodo", comunque "non inferiore a sei mesi".

---

[1] Provvedimento 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008 (di seguito "il Provvedimento"), e modificato.

[2] Trattasi di misure di carattere prevalentemente organizzativo, la cui mancata adozione (su cui si tornerà), è sanzionata in termini assai rigorosi.

[3] Decreto Legislativo noto come "Codice in materia di protezione dei dati personali" (di seguito "il Codice").

[4] Sanzionata con il pagamento di una somma da trentamila euro a centottanta mila (cfr. art. 162, comma 1-ter, del Codice) e con l'eventuale pubblicazione, a spese del trasgressore, dell'ordinanza-ingiunzione in uno o più giornali indicati nel provvedimento che applica detta sanzione accessoria (cfr. art. 165 del Codice).

[5] La sanzione è costituita dalla reclusione da tre mesi a due anni (cfr. art. 170 del Codice); quale pena accessoria è prevista la pubblicazione della sentenza (cfr. art. 172 del Codice).

[6] La quale, in via di approssimazione, individua il trattamento dei dati (attinenti ad imprese, amministrazioni, clienti, fornitori e dipendenti) utilizzati in relazione ad obblighi contrattuali e/o normativi.

[7] Sebbene siano esentati dal rispetto del Provvedimento i soggetti che trattano come unici dati personali sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali (cfr. art. 34 del Codice).

[8] Si ricordi che, per espressa definizione normativa, è dato giudiziario (solo) quel dato idoneo a rivelare "provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (cfr. art. 4, comma 1, lett. e) del Codice). E dunque, per esempio, ai fini "privacy" non sono dati personali di carattere giudiziario le generalità del debitore nei confronti del quale si è proceduto al recupero coattivo del credito, in via giudiziale.

[9] Quali per esempio i sistemi ERP ovvero, a nostro avviso, i programmi per la fatturazione elettronica, per la conservazione sostitutiva o per la gestione dell'impianto di videosorveglianza.

[10] Cfr. artt. 15 e 169 del Codice.

[11] Si eviti l'errore (per il vero tutt'altro che infrequente) di designare la società che presta i servizi quale "amministratore di sistema", atteso che solo la persona fisica può essere oggetto di detta nomina. L'outsourcer (cui competerà l'onere di designare i singoli amministratori) va, invece, nominato "responsabile (esterno) del trattamento", nelle forme di cui all'art. 29 del Codice.

[12] Trattasi di una regola "di trasparenza", espressione del principio di correttezza del trattamento (cfr. art. 3 del Codice).

[13] Quest'ultima, nel prescrivere l'obbligo del titolare di riportare gli estremi identificativi degli amministratori in un documento interno, avrebbe dovuto far salvo quanto previsto in relazione ai servizi affidati in outsourcing.

[14] Ciò avviene all'atto dell'autenticazione informatica, che costituisce una misura "minima" di sicurezza, prevista dall'Allegato B al Codice (c.d. "Disciplinare Tecnico").

[15] Come meglio si dirà trattando del profilo della "completezza" del log, è da rilevare che l'onere della registrazione dell'accesso è soddisfatto con la tenuta della sola riga relativa all'"access log". Ne deriva che, qualora il sistema di log generi una stringa più ampia, detta deve preferibilmente essere oggetto di filtraggio al fine di selezionare i soli dati pertinenti agli amministratori di sistema (ciò anche per non violare il principio di necessità, di cui all'art. 3 del Codice).

(da www.altalex.it)