L'AMMINISTRATORE DEL SISTEMA INFORMATIVO:

CHI E' COSTUI?

di Avv. Luca Giacopuzzi (www.studiogiacopuzzi.it)

Nell'*incipit* dell'VIIII capitolo de "I promessi sposi" Don Abbondio, uno dei più noti personaggi del famoso romanzo, è nella sua stanza che legge un panegirico in onore di San Carlo Borromeo in cui viene citato il filosofo Carneade di Cirene. E' a questo punto che, tra sé e sé, si pone la fatidica domanda, destinata a divenire celebre: *"Carneade! Chi era costui?"*. Ed aggiunge: *"Carneade! questo nome mi par bene di averlo letto o sentito; doveva essere un uomo di studio, un letteratone del tempo antico: è un nome di quelli; ma chi diavolo era costui?"*. Nonostante l'importanza della figura, ai nostri giorni sono ancora troppi coloro che, sebbene ne abbiano sentito parlare, ignorano chi sia realmente l'amministratore del sistema informativo e quali mansioni detto sia chiamato a svolgere. Ad essi sono dedicate le brevi note che seguono.

Lascereste le chiavi di casa alla colf senza averne previamente verificato la rettitudine e, soprattutto, senza controllarne l'operato?

La risposta è scontata. E allora, *mutatis mutandis*, perché mai non si presta altrettanta attenzione all'individuazione del soggetto idoneo a svolgere le mansioni di amministratore di sistema e alle criticità insite nell'affidamento dei relativi incarichi?

Eppure l'amministratore del sistema informativo ricopre un ruolo che andrebbe ben presidiato, perché l'esecuzione dei compiti che gli sono propri comporta la capacità di accedere in modo privilegiato, vuoi per atto intenzionale vuoi per caso fortuito, a risorse del sistema informativo ed a dati personali che non avrebbe altrimenti la concreta possibilità di trattare.

Tuttavia, come già rilevato, la sottovalutazione dei rischi derivanti dall'azione incontrollata da chi dovrebbe, invece, tutelare il corretto utilizzo del sistema informativo è, purtroppo, all'ordine del giorno. Complici anche, diciamolo chiaramente, designazioni incaute e controlli assenti.

In precedenza ho richiamato la figura della colf, sottolineando come nessuno consegnerebbe mai alla predetta le chiavi della propria casa in modo imprudente.

Ebbene, in tema di amministratore di sistema un incauto affidamento ha effetti ancor più devastanti.

Se qualcuno ruba in casa, è facile accorgersene; se, invece, l'amministratore di sistema sottrae qualche dato (asset strategici inclusi) quale titolare del trattamento ha la capacità di venirne a conoscenza (o, nella migliore delle ipotesi, di farlo per tempo)?

E ancora. La privata dimora non è luogo in cui si custodiscono beni altrui; l'azienda, invece, spesso detiene dati di terzi, della cui perdita è chiamata, conseguentemente, a rispondere. Trattasi di una ipotesi ordinaria per le aziende del settore IT (che hanno *data center* ove risiedono dati dei clienti) o per le agenzie di comunicazione o, più in generale, per numerosi altri soggetti.

Quanto precede spiega i motivi per i quali il Garante, con proprio Provvedimento del 27 novembre 2008 (attualissimo, in verità), richiama l'attenzione dei titolari del trattamento dei dati sulla necessità di un'attenta valutazione delle caratteristiche soggettive dei candidati a ricoprire la funzione di amministratore di sistema.

Si ricordi, peraltro, che la natura fiduciaria delle mansioni affidate non viene meno allorchè le incombenze 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.

Altra prescrizione impone di 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 in relazione ai responsabili del trattamento.

I titolari, ancora, 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.

Con la precisazione che, 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. Identità che, pertanto, va resa o nota o conoscibile (magari all'esito di una procedura formalizzata, attivabile a istanza del dipendente).

Allo scopo di contrastare la diffusa sottovalutazione dei rischi cui abbiamo accennato in precedenza, il Provvedimento introduce, altresì, verifiche ispettive a carico del titolare o del responsabile esterno. L'operato degli amministratori di sistema, infatti, deve essere oggetto di verifica, a cadenza almeno annuale, per acclarare che le attività svolte dall'amministratore siano in effetti conformi alle mansioni attribuite.

Accanto agli oneri di cui s'è detto (di ordine prettamente "organizzativo"), al titolare 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 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).

A conclusione di queste brevi note mi permetto di rammentare che il mancato rispetto delle indicazioni previste dal Provvedimento di cui si è detto dà luogo ad una violazione amministrativa (sanzionata con il pagamento di una somma da 30.000 a 180.000 euro) nonché è fonte di responsabilità civile per inosservanza delle misure di sicurezza "idonee" (a tale categoria dovendo essere ascritte, a mio avviso, le prescrizioni ivi impartite).