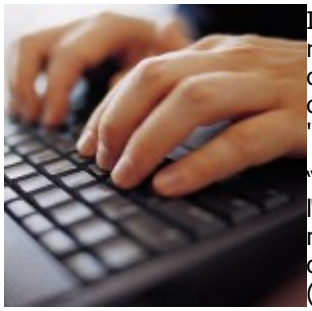
L'amministratore di Sistema, passato, presente, e futuro in vista del Regolamento UE

Mercoledì 22 Ottobre 2014 04:19 Gloriamaria Paci Visite: 9005



In un periodo storico in cui la tecnologia impone il ricorso a strumenti sempre più avanzati per la raccolta, il trattamento e la conservazione dei dati, è comprensibile che si debba affidare ad esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali. Alla prima domanda delle Faq, "Cosa deve intendersi per "amministratore di sistema", il Garante risponde:

"In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti 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". E ancora. "Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi. Anche il riferimento al d.P.R. 318/1999 nella premessa del provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento. Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software".

Sulla base delle indicazioni fornite dal Garante si evince che sono molteplici le mansioni in capo a tale figura. Dal garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto, al coadiuvare il Titolare, o il responsabile se nominato, nella definizione della politica di sicurezza consigliando la scelta delle dotazioni informatiche fino al corretto funzionamento degli applicativi necessari al funzionamento dell'organizzazione. E ancora. Disporre di competenze su gestione e configurazione degli apparati di trasmissione, conoscenza delle architetture hardware dei sistemi, conoscenze di sicurezza delle reti, dei sistemi e delle applicazioni fino a svolgere un ruolo di prima interfaccia nel caso di incidenti di qualsiasi genere che riguardino la rete preoccupandosi di erogare una corretta informazione verso gli utenti interni ed esterni. Compito quest'ultimo attualmente in capo alle compagnie telefoniche e fornitori di servizi internet. Recependo le Direttive comunitarie sulle comunicazioni elettroniche (la 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e del regolamento (CE) n. 2006/2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori), il Decreto Legislativo 28 maggio 2012, n. 69, ha di fatto modificato il Codice Privacy, obbligando società telefoniche e fornitori di servizi Internet alla tempestiva segnalazione di eventuali violazioni subite dai propri database, pena l'applicazione di sanzioni di tutto rispetto.

In sintesi, questi Titolari dovranno avvisare il Garante e gli utenti quando i dati trattati per fornire i servizi subiscono gravi violazioni a seguito di attacchi informatici o di eventi avversi, come incendi o altre calamità che possano comportare perdita, distruzione o diffusione indebita di dati. Nella prevenzione dei cosiddetti *data breach*, vi è anche l'obbligo di comunicare, entro 24 ore dalla scoperta, le violazioni dei dati personali al Garante. Ma non solo. Nei casi più gravi di violazione, società telefoniche e fornitori di servizi Internet avranno l'obbligo di informare entro tre giorni "ciascun utente coinvolto, facendo riferimento ad alcuni parametri fondamentali quali il grado di pregiudizio che la perdita o distruzione dei dati possa comportare, ma anche i gradi di attualità, qualità e quantità di quest'ultimi.

L'avvento del Regolamento Europeo sulla protezione dei dati di prossima approvazione, prevederà la violazione dei dati personali, non solo a carico di compagnie telefoniche e fornitori di servizi internet ma per le eventuali violazioni commesse da tutti i Titolari del trattamento nello svolgimento delle proprie attività. Alle luce di quanto appena esposto, l'Ads diverrà una figura ancor più rilevante. Spetterà anche a lui concorrere alla riduzione dei rischi dovuti a violazioni.

Subito dopo però, con una disposizione abbastanza atipica, ma significativa nel voler attribuire un alto livello di attenzione, il Provvedimento prevede come anche quando le funzioni di amministratore di sistema o assimilate sono attribuite ad una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il Titolare ed il Responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili ai sensi dell'art. 29. Con una precisazione: l'impossibilità di effettuare designazioni per classi omogenee per gli addetti IT, semplificazione a dire il vero molto apprezzata con l'introduzione del Codice, ma non percorribile per le nomine dei *system administrator*, poiché in tale caso è obbligatoria una designazione individuale.

Senza entrare nel merito della scelta effettuata dal Titolare per ricoprire la figura dell'Ads (Responsabile/Incaricato), con il Provvedimento del 2008 il Garante ha lanciato un monito chiaro: tale incarico può essere attribuito unicamente a soggetti che siano affidabili, prima di tutto, oltre che capaci ed esperti, poiché devono fornire idonea garanzia del pieno rispetto delle disposizioni in materia di corretto trattamento, compreso il profilo relativo alla sicurezza informatica (in considerazione anche delle responsabilità, di natura penale e civile, che possono derivare in caso di incauta o inidonea designazione).
La nomina dell'Amministratore di sistema deve avvenire ovviamente in forma scritta indicando con esattezza ed in maniera analitica le aree su cui dovrà essere espletata l'attività. Va da se perciò che è indispensabile che il Titolare individui con estrema chiarezza le mansioni che l'Ads dovrà rispettare nello svolgimento del proprio incarico.

Pur considerando la delicatezza del ruolo, il Garante ha dovuto fare una precisazione importante. Alla domanda (vedere Faq. n. 20) "se nella designazione degli amministratori di sistema occorre valutare i requisiti morali, l'Autorità risponde di no

sottolineando però che la figura dovrà tuttavia possedere caratteristiche quali esperienza, capacità e affidabilità, qualità tecniche, professionali e di condotta, non di requisiti morali".

Pur puntualizzando che nell'ambito delle proprie competenze l'Ads non abbia accesso ai dati in chiaro, così come precisato nella Faq n. 17 si definisce "consultazione in chiaro ossia quelle mansioni che comportino la potenzialità di violazione del dato personale anche in condizioni in cui ne sia esclusa la conoscibilità, come può avvenire, per esempio, nel caso della cifratura dei dati", il Garante si è affrettato a scansare eventuali dubbi sulla non obbligatorietà della nomina: non ritenendo questa circostanza sufficiente per escludere i Titolari obbligati a tale nomina dall'area applicativa del Provvedimento. Una doccia fredda per tanti addetti ai lavori che da sempre portano avanti la tesi secondo la quale gli Ads non procedono ad un trattamento dati limitandosi ad effettuare operazioni di manutenzione o simili.

Un nodo cruciale lo ha rivestito, e lo riveste tutt'ora la possibilità di far il ricorso a soggetti esterni per la gestione dei servizi informatici. A questo proposito il Provvedimento impone che il titolare conservi direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Se dall'applicazione di tale precetto ne deriva un gravoso onere a carico dei provider di tali servizi, che dovranno fornire all'appaltante un elenco dettagliato ed aggiornato di tutti i soggetti che curano le attività affidate all'esterno, il Titolare non può che appoggiare tale richiesta del Garante.

Pensiamo infatti alle nuove tecnologie che consentono di usufruire di servizi sempre migliori a così ragionevoli. Le cloud computing, in particolare, garantiscono soluzioni innovative per gestire molteplici attività con efficienza e margini di risparmio. D'altra parte però presentano criticità e rischi per la privacy da tenere in seria considerazione. Come lo stesso Garante ha precisato in mini guide ed opuscoli divulgativi, prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è necessario sempre porsi alcune domande, scegliendo con cura la soluzione più sicura per le attività istituzionali o per il proprio business. Il cloud offre infatti, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore. In sintesi, tutto può essere demandato all'esterno, in outsourcing, e a un costo potenzialmente limitato, in quanto le risorse informatiche necessarie per i servizi richiesti possono essere condivise con altri soggetti che hanno le stesse esigenze. Poco importa della scelta sul tipo di cloud computing (private o public cloud) o del modello di servizio prescelto (Cloud Infrastructure as a Service - IaaSclassificati , Cloud Software as a Service – SaaS, Cloud Platform as a Service – PaaS ecc), poiché ogni tipo di cloud ha le sue caratteristiche peculiari, il Titolare dovrà valutare con attenzione alcuni aspetti vista l'attuale assenza di un quadro normativo aggiornato – non solo in tema di privacy, ma anche in ambito civile e penale – che tenga conto di tutte le novità introdotte dal cloud computing e sia in grado di offrire adeguate tutele nei riguardi delle fattispecie giuridiche connesse all'adozione di servizi distribuiti di elaborazione e di conservazione dati. Poiché in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell'eventuale illecito, non sarà sufficiente, per giustificare una eventuale violazione, affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo più stringenti (non dimentichiamo che tali servizi sono in mano a pochi colossi che operano a livello mondiale!!!). Oltre al fatto che il cliente avrebbe potuto servirsi di un altro fornitore, non bisogna dimenticare che il Titolare ha l'onere di esercitare un potere di controllo nei confronti del Responsabile del trattamento (in questo caso il cloud provider), verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati.

Prima di affidare a terzi l'intero patrimonio informativo, è giusto porsi altresì alcune domande: in caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? In quanto tempo può essere ripristinato il sistema? Esistono piani di emergenza per i servizi essenziali?

Dott.ssa Gloriamaria Paci - info@consulenzepaci.it

Ti può interessare anche:

I feed del Corriere della Privacy
Il Garante introduce una nuova guida ad uso del paziente
Garante Privacy: in caso di contenzioso l'azienda può
conservare i file del dipendente ma non può accedervi
tenendoli a disposizione del Giudice