Il Blog di Luca De Grazia

2 dicembre 2009

A.d.S.: si è riusciti capire cosa sono?

Riprendiamo una analisi effettuata tempo fa per capire se qualcosa sia cambiato….

1. Premessa

In questa sintesi verrà analizzata la portata del Provvedimento del Garante per la Protezione dei dati personali del 27.11.2008, pubblicato nella G.U. del 24.12.2008 (reperibile, tra l'altro, alla seguente url:

L'analisi si baserà fondamentalmente sul dettato della normativa

2. Alcune precisazioni preliminari

Il provvedimento segue altri provvedimenti di (apparente) semplificazione delle misure (minime) di sicurezza, alcuni effettuati con provvedimento legislativo, altri effettuati con provvedimenti del Garante, e segue anche le modifiche al D.Lgs. n.196/2003 introdotte dall'art. 44 del decreto legge 207/2008 (G.U. 31/12/2008), modifiche che hanno inasprito in maniera significativa le sanzioni previste dalla normativa citata.

A.d.S., Amazon, autovalutazione, Avvocatura Generale, C.A.D., chiavetta umts, competenza, computer crimes, D.Lgs. n.196/2003, data

Il commento al provvedimento verrà effettuato in pieno stile da mailing list, ovvero riportando la parte di provvedimento con il commento immediatamente sottostante.

Come riferimento ad un corretto sistema di gestione delle informazioni si fa espresso riferimento a quanto previsto dalla normativa ISO 27001:2005, che a parere del sottoscritto costituisce – pur nascendo in ambiti normativi differenti dal nostro – un ottimo sistema per applicare correttamente ed in maniera organica il disposto del D.Lgs. n.196/2003.

Da ultimo verranno effettuati alcuni cenni alla relazione tra il provvedimento citato e l'applicazione del D.Lgs n.231/2001, in particolare per quanto concerne la repressione dei reati informatici introdotti con l'ultima modifica alla normativa appena specificata.

3. Analisi generale della situazione

Il provvedimento, sia nella parte introduttiva sia nella parte della premessa, richiama espressamente quanto la giurisprudenza ha chiarito in merito alla figura del c.d. "amministratore di sistema" (previsto per la prima volta nelle modifiche al C.P. operate del DPR 513/97, in particolare come aggravante per alcuni reati introdotti da quel DPR).

Inoltre non fa altro che prendere atto della "normale" complessità di gestione di qualsivoglia attività organizzata di una certa dimensione, laddove – per esigenze organizzative – il "titolare del trattamento" decide di gestire i propri sistemi informativi, le proprie infrastrutture, il proprio sistema informatico e telematico non solamente in maniera diretta (il che vuole dire attraverso contratti di lavoro che prevedano il controllo diretto dell'imprenditore sull'operato dei lavoratori – incaricati) ma anche attraverso le varie forme di collaborazione esterna, usualmente denominate "outsourcing", laddove per lo più si tratta di:

a. Contratti di appalto di servizi

b. Contratti d'opera intellettuale se più propriamente consulenza

c. Contratti d'opera (in qualche caso sporadico)

d. Contratti che colleghino le figure innanzi indicate

Inoltre, oserei dire finalmente, l'Autorità prende atto della circostanza che lo "skill" professionale e "morale" (o, quanto meno, "etico") delle persone preposte a determinate attività "dovrebbe" comprendere una analisi a tutto tondo, rifuggendo quindi da persone che abbiano un passato non propriamente limpido.

Si tratta di pratiche che le imprese serie già da tempo mettono in atto ma, in questo senso, la circostanza che un provvedimento di un'Autorità Indipendente precisi tali punti non può che essere produttivo per una vera cultura della sicurezza.

4. Analisi particolare del provvedimento

certa, dato personale, deep link, delitti contro la personalità, diritto d'autore, documento, documento informatico, DPS, frode, furto informatico, Garante per la Protezione dei dati personali, hacker, identificazione, indagini, indirizzo IP, ispezioni, legge Merlin, natura giuridica, netiquette, P.E.C., pagamenti on line, phishing, privacy, proprietà, prostituzione, reati informatici, rete informatica, riconoscimento, router, sicurezza informatica, sito web, standard PCI DSS, TLC, trattamento dati, truffa, wi-fi

4.1. Valutazione delle caratteristiche soggettive.

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.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

Viene riferita anche alla figura dell'A.d.S. la pre – analisi dei requisiti previsti dalla normativa per la scelta del responsabile del trattamento. Il secondo periodo non vuol significare altro che la scelta del soggetto persona fisica che svolga materialmente le funzioni di A.d.S. – e quindi abbia un determinato profilo come incaricato del trattamento – debba tenere conto di quanto previsto dall'art.29.

4.2. Designazioni individuali.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

A parere del sottoscritto anche in questo caso la locuzione "individuale" non vada intesa come "ad personam" ma riferita ad un (corretto) organigramma funzionale / operativo, che alla luce delle modifiche normative dovrà (se necessario) essere integrato con "…l'elencazione analitica degli ambiti di operatività…".

E' appena il caso di notare come questo modo di inquadrare i soggetti operanti nell'ambito di serie organizzazioni complesse sia già da tempo operante; nello specifico si tratterà di effettuare un ulteriore controllo dei profili utente (già previsti sin dall'inizio dall'allegato B) ed eventualmente apportare qualche modifica specifica.

In sostanza, non occorre una elencazione di nominativi (si utilizza appunto la locuzione individuale, non personale e/o nominativa), ma una corretta gestione delle entità logico – organizzative, con annesso elenco delle persone che ricoprano pro-tempore la funzione.

In pratica, non il contenuto della variabile (A), ma una corretta individuazione delle funzioni spettanti alla variabile (A); per inciso, mi sembra ovvio che qualora la persona fisica che ricopra un certo ruolo venga magari trasferito ad altro lavoro, ed al suo posto venga inserita persona con caratteristiche simili, il riferimento continui ad essere alla funzione, non alla persona.

4.3. Elenco degli amministratori di sistema.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza, oppure, nei casi in cui il

titolare non é tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Norma totalmente inutile per quanto concerne l'inserimento nel DPS; sarebbe stato sufficiente applicare a tutti i casi la necessità di un documento interno. Ricordiamo comunque che il DPS dovrebbe essere classificato come documento riservato, non accessibile a tutti, e che non necessariamente il DPS debba avere la forma monolitica di un romanzo di appendice, ben potendo ricorrere agli allegati.

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, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione é prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 <http://www.privacy.it/garanteprovv20070301.html> (in Gazzetta Ufficiale 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).

Precisazione anche in questo caso inutile, in quanto deriva direttamente dalla applicazione della normativa; nel momento in cui l'Autorità da rilievo specifico ad una figura che prima non aveva rilievo normativo (ma che magari già esisteva nella organizzazione aziendale) ne consegue la necessità di aggiornare tutti i documenti che in qualche modo facciano riferimento a tale figura.

Forse anche in questo caso è opportuno precisare che laddove si sia svolto un corretto e paziente lavoro di inquadramento delle figure professionali esistenti, sia siano correttamente parametrati gli organigrammi funzionali con quanto previsto dal D.Lgs. n.196/2003, probabilmente sarà necessario solamente un "link" tra le figure esistenti [ivi compresa ovviamente una dettagliata descrizione dei poteri / doveri ad esse attribuiti] e la "nuova" figura normativamente qualificata.

Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

A stretto tenore letterale della norma, nel caso in cui venga svolto in outsourcing SOLAMENTE il servizio di A.d.S. (ed aggiungo configurando il rapporto come titolare – responsabile) il Titolare dovrà pretendere dal Responsabile l'elenco dei soggetti preposti a tali funzioni.

In realtà occorrerà controllare ancora una volta quali funzioni siano affidate all'outsourcer e conseguementente gli atti di individuazione dovranno subire un "upgrade" (dovuto per legge).

4.4. Verifica delle attività.

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 rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Si tratta semplicemente di inserire un'altra attività da monitorare in previsione della redazione del DPS.

A mio giudizio un termine trimestrale o al massimo quadrimestrale di aggiornamento della situazione, anche per rispettare quanto previsto dal D.Lgs n.231/2001, non potrà che essere utile per il rispetto delle normative citate, anche se la normativa parla di termine annuale.

4.5. Registrazione degli accessi.

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.

Nulla di nuovo, lo prevedeva già l'Allegato B

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.

Finalmente si fa riferimento alla necessità – peraltro da tempo affermata dalla letteratura "tecnica" – di inalterabilità dei log; i riscontri ed i riferimenti alla c.d. "forensic" mi sembrano del tutto chiari.

Come sempre – e correttamente – l'Autorità non "dice" cosa utilizzare, anche perché – ormai – il panorama tecnico – legislativo italiano è sufficientemente esteso per fornire soluzioni "per tutti i gusti e tutte le tasche".

Si va dalla firma elettronica avanzata alla firma digitale, alla marca temporale, alla conservazione sostitutiva dei documenti, ovvero ad un insieme di tali tecniche / servizi esistenti.

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.

Corretta la necessità di inserimento dei riferimenti temporali, senza i quali sarebbe praticamente impossibile ricostruire a posteriori cosa esattamente sia accaduto.

Qui – però – siamo in completa contro tendenza con quanto in genere previsto dall'Autorità (il tempo di conservazione dei trattamenti deve in linea di massima essere il minimo necessario) ma, oggettivamente, mi trova perfettamente concorde il periodo di "almeno sei mesi"

Ritengo che ormai i tempi siano maturi per comprendere che non è “cancellando i dati” che si protegge l’individuo (e non solo, l’interessato per il D.Lgs. n.196/2003 non è solamente la persona fisica) ma, anzi, magari si sottrae al soggetto leso la possibilità di ricostruire cosa sia successo, specialmente in caso di reati e/o abusi perpetrati attraverso il mezzo internet.

E’ necessario sanzionare velocemente e pesantemente l’abuso (del trattamento) dei dati, non l’esistenza dei medesimi.

5. Tempi di adozione delle misure e degli accorgimenti.

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che é congruo stabilire, in centoventi giorni dalla medesima data.

Molto semplicemente i Titolari del trattamento dovranno, entro il **15 dicembre 2009**, adeguare le proprie organizzazioni a quanto stabilito dal provvedimento.

5. Possibili conclusioni

Provvedimento sostanzialmente corretto nella sostanza, con le solite complicazioni burocratiche che discendono – purtroppo ed ancora – dalla mancata conoscenza da parte dell’Autorità della realtà organizzativa delle imprese italiane, molto tardivo (in realtà poteva costituire una parte dell’Allegato B), ma che forse, alla fine, per alcuni principi introdotti, potrà contribuire ad una corretta applicazione della cultura della sicurezza (informatica)

Va da sé che l’ulteriore layer di codificazione (ora anche necessariamente normativa) della figura analizzata non potrà che essere d’aiuto anche nella corretta applicazione del D.Lgs n.231/2001, tenendo presente che ambedue le normative citate dovrebbero “prevenire” certi accadimenti.

E passiamo alla registrazione degli accessi, croce e delizia degli informatici…e dei loro consulenti.

4.5 Registrazione degli accessi
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 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.
[…omissis…]

TUTTO CIÒ PREMESSO IL GARANTE:

Il provvedimento vero e proprio ….[…omissis…]

f. Registrazione degli accessi
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;

L'esegesi letterale della norma sembrerebbe portare alle seguenti considerazioni (fermo restando che – come ho già evidenziato in altro scritto – sicuramente si poteva fare di meglio quanto a chiarezza del provvedimento):

Quello che deve essere adottato (laddove non già presente) è:
1. un sistema idoneo alla registrazione degli accessi logici intesi come autenticazione informatica ai sistemi di elaborazione
2. un sistema idoneo alla registrazione degli accessi logici agli archivi elettronici
a. in ambedue i casi quando uno degli accessi appena citati venga effettuato da un amministratore di sistema (d'ora in avanti AdS)

I log degli accessi appena menzionati devono essere, praticamente, "forensic ready" e la locuzione "… *adeguate al raggiungimento dello scopo per cui sono richieste…"* sta a significare che a posteriori si dovrà poter ricostruire quello che è accaduto; se non si raggiunge tale scopo, l'apparato che sarà stato messo in piedi non sarà servito a nulla.

Altra domanda: quali sono esattamente gli AdS?

Posto che nella parte preliminare del provvedimento l'Autorità non solo volutamente non ha voluto effettuare una elencazione delle funzioni che ricadano in tale ambito, ma espressamente ha fatto riferimento anche ad altre normative, non ultima la Legge 547/93 che all'epoca introdusse i reati informatici nell'ordinamento italiano, e che prevede espressamente come ipotesi aggravata l'atto compiuto dal c.d. "operatore di sistema", soggetto che la giurisprudenza in materia ha individuato in un soggetto che sicuramente ha molti meno "poteri" di quello che viene considerato dalla letteratura tecnica un AdS, mi sembra che la soluzione – come spesso è consuetudine nel diritto – non possa essere totalmente univoca, ma debba essere sempre e comunque contestualizzata.

Ma non è sicuramente finita qui….

3 Commenti a “A.d.S.: si è riusciti capire cosa sono?”

1. *Invest $ 1193 and get $ 6673 every month: https://get-1-btc-per-day.blogspot.com.tr?h=06* scrive:
   Scritto il 21-11-2019 alle ore 12:04

   Just how would certainly you use $79868 to make more cash: https://make-3-btc-per-day.blogspot.jp?f=03

2. *Just how would you utilize $92347 to make even more cash: https://make-3-btc-per-day.blogspot.in?i=21* scrive:
   Scritto il 22-11-2019 alle ore 09:09

   How to earn on investments in Cryptocurrency from $ 4977 per day: https://kl-po-lo.blogspot.ie?jc=23

3. *Быстрый и Большой заработок в интернете от 6077 р. в сутки: http://onobisoxubyq.gq/7n5r* scrive:
   Scritto il 25-11-2019 alle ore 06:35

   Зарабатывай 8068 р. в сутки: https://jtbtigers.com/zarabotaymillion957475

Scrivi il tuo commento!

Nome (obbligatorio)

E-mail - non verrà pubblicata - (obbligatorio)

Sito web

Avvisami dei nuovi commenti tramite e-mail

Invia commento