IL GARANTE DELLA *PRIVACY* E L'AMMINISTRATORE DI SISTEMA*

*di Giovanni Gioffré***

Sommario: *1. Parte generale; 2. La protezione dei dati personali; 3. Dati quasi sensibili; 4. Amministratore di sistema; 5. Requisiti dell'amministratore di sistema; 6. Funzione dell'amministratore di sistema; 7. Attività dell'amministratore di sistema; 8. Verifica dell'attività dell'amministratore di sistema.*

1. PARTE GENERALE

Il "Garante per la protezione dei dati personali" è un'Autorità Amministrativa Indipendente istituita dalla legge 31 dicembre 1996, n . 675 (c.d. legge sulla *privacy)*, per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità della persona nel trattamento dei dati personali.

Le norme sulla *privacy* sono state riprese alla luce del decreto legislativo 30 giugno 2003, n. 196 che è entrato in vigore il 1° gennaio 2004 e rubricato *"Codice in materia di protezione dei dati personali"*.

La parola "garante" (dall'italiano antico e occitano «*guarènto*») indica colui che assicura qualcuno del fedele adempimento di un patto, una convenzione o un risarcimento. Costituisce sinonimo di mallevadore, difensore o protettore.

Nel nostro ordinamento il termine è stato utilizzato per indicare una caratteristica delle "Autorità Amministrative Indipendenti" che hanno appunto una funzione di garanzia, difesa e tutela dei cittadini nei rispettivi settori di competenza. Si parla così di Garante dell'Autorità per le garanzie nelle comunicazioni, dell'Autorità garante della concorrenza e del mercato, del Garante per la protezione dei dati personali (c.d. Garante della *privacy*), ecc. In tale contesto il Garante della *privacy*, nell'ambito del proprio "Laboratorio *Privacy* Sviluppo" pensa ad un'idea e da vita a "Civicrazia" dove il «*cittadino diventa protagonista dei propri diritti, del suo ruolo sociale, della forza propulsiva e di controllo che è capace di esercitare nei confronti del potere pubblico e dove*

oltre 4.000 associazioni di cittadini lavorano affinché il potere pubblico sia davvero accanto e al servizio del cittadino».

Vanno considerati come riferimenti normativi del provvedimento del Garante della *privacy* del 27 novembre 2008, avente ad oggetto *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, il codice in materia di protezione dei dati personali ed in particolare l'articolo 31[1], l'art.154[2] ed il *"disciplinare tecnico in materia di misure minime di sicurezza"* contenuto nell'allegato B) al codice stesso. Come ambito di applicazione, poi, "*il codice disciplina*

[1] Decreto legislativo 30 giugno 2003, n. 196. Art. 31. *Obblighi di sicurezza*

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

[2] Decreto legislativo 30 giugno 2003, n. 196. Art. 154. *Compiti*

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;*(*)*
b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;
d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;
e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;
f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;
g) esprimere pareri nei casi previsti;
h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;
m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:

a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;
b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);
c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;
d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;
e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.

5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

(*) Lettera così modificata dall'art. 4, decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.

il trattamento dei dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato".

2. La protezione dei dati personali

E' stato detto che la tutela della *privacy* è una materia che appartiene alla tradizione anglosassone. Il diritto alla protezione dei dati personali e il diritto alla riservatezza non coincidono; il diritto alla riservatezza è il diritto di escludere altri dalla conoscenza di informazioni private, intime o familiari; è un diritto molto antico e si fonda, essenzialmente, sul concetto de "il diritto di essere lasciato solo" o in maniera più drastica: "il diritto di essere lasciato in pace". Come dire: *"in casa mia son Re ed Imperatore ed ivi incontrastato ìmpero"*.

Questo diritto trova il suo fondamento storico e culturale nel diritto di proprietà; perciò stesso questo diritto tende ad escludere dal "godimento" che altri vengano a conoscenza di notizie o fatti ecc. Cioè quando il soggetto chiude "la porta di casa" metaforicamente parlando, nessuno ha più diritto di accesso.

Il diritto alla protezione dei dati personali è il diritto di esercitare un controllo sui dati e sulle informazioni che lo riguardano[3].

Occorre dire che, ancora oggi, non è completamente chiara l'applicazione di molti aspetti della norma. La norma in questione ha introdotto nel nostro ordinamento il principio della tutela costituzionale della riservatezza intesa sotto vari aspetti. Il diritto alla riservatezza e il diritto alla protezione dei dati personali, sono diversi: entrambi diritti della personalità, entrambi assoluti, non cedibili, imprescrittibili ma a contenuto diverso.

Nel primo caso vi è il diritto alla riservatezza e le informazioni, appunto, riservate che si vogliono tenere escluse dalla conoscenza di altri; nel secondo si vogliono proteggere i dati e le informazioni. Il codice per la protezione dei dati personali non è necessariamente da considerarsi come una legge sulla *privacy*. Lo scopo, l'obiettivo invece è quello di regolamentare l'utilizzo delle informazioni: è una legge sull'utilizzo dell'informazione.

E' utile precisare che "le informazioni" non hanno un contenuto riservato, non c'è nessun riferimento ad un contenuto intimo, dato, familiare; queste informazioni possono essere anche informazioni pubbliche: per esempio il numero di telefono di un'utenza fissa, pubblicato su un

[3] Gioffré Giovanni, *"La privacy nella Pubblica Amministrazione e la sua tutela"*, in «Diritto & Diritti» – Rivista giuridica elettronica, pubblicata su Internet all'indirizzo http://www.diritto.it, ISSN 1127-8579, Settembre 2008, pag. http://www.diritto.it/art.php?file=/archivio/26450.html

elenco telefonico, certamente non è un dato riservato però è un dato personale cioè una informazione soggetta al decreto legislativo 30 giugno 2003, n 196.

I diritti che il soggetto può esercitare non sono soltanto a contenuto negativo, di escludere, ma anche di diritto positivo: di controllare, di accedere, di modificare, di integrare i propri dati.

L'art. 4 del decreto legislativo 30 giugno 2003, n 196 compendia tutte le definizioni di dati personali. Sinteticamente la definizione di dato personale è qualunque informazione riferibile direttamente o indirettamente a persona fisica, giuridica, ente, associazione.

Naturalmente ci possono essere dei dati personali che sono anche riservati, per esempio i dati sanitari contenuti nella cartella clinica: il dato personale è "l'informazione"[3]. Quindi la riservatezza è intesa come un vero e proprio bene della vita ed è intesa a far rispettare i diritti di libertà fondamentali nonché la dignità delle persone fisiche. Da quanto precede è facile capire che viene fuori un profilo della tutela della riservatezza soprattutto sotto il profilo dell'identità personale. Occorre evidenziare che il legislatore italiano a differenza di quanto previsto dalla direttiva europea non ha limitato la definizione di dato personale alle persone fisiche ma l'ha estesa alle persone giuridiche, agli enti, alle associazioni; quindi nel nostro ordinamento giuridico il dato personale è l'informazione che si riferisce anche a enti, associazioni, pubblica amministrazione.

Tutte le volte che vengono trattati i dati riguardanti società, associazioni, vengono trattati dei dati sensibili. Avuto riguardo al concetto di dato personale è utile evidenziare che la definizione è assai ampia e dentro vi si comprende tutto; dai dati identificativi come nome, cognome, paternità, eccetera a tutte quelle altre informazioni che possono riguardare il soggetto: la sua condizione personale cioè se è celibe o coniugato, nubile o coniugata, quanto guadagna, dove lavora, se ha delle malattie, le sue preferenze, i gusti nel vestire. Tutto rientra nel concetto di dati personali. In sintesi per dato personale si intende qualunque informazione relativa a persona identificata o identificabile.

Particolare rilievo oggi assume la videosorveglianza. Come lo stesso Garante della *privacy* ha evidenziato, sono stati sottoposti all'esame di questa Autorità numerosi casi, attraverso reclami, segnalazioni e richieste di parere, i quali evidenziano un utilizzo crescente, spesso non conforme alla legge, di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione dei dati. Il Garante, ponendo doverosa attenzione al nuovo diritto alla protezione dei dati personali, consacrato al primo periodo dell'art. 1 del codice in materia di protezione dei dati

personali[4], ha ritenuto di intervenire emanando il provvedimento a carattere generale del 29 aprile 2004 sulla materia inerente la videosorveglianza.

Tra i principi generali il Garante ha inserito:

- il principio di liceità;
- il principio della necessità;
- il principio della proporzionalità;
- il principio di finalità.

Il principio di liceità, secondo il quale il trattamento dei dati attraverso sistemi di videosorveglianza, è possibile solo se è fondato su uno dei presupposti di liceità, appunto, che il codice prevede espressamente.

Il principio della necessità, secondo il quale, poiché l'installazione di un sistema di videosorveglianza comporta in sostanza una limitazione e, comunque, un condizionamento per il cittadino, va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Il principio di proporzionalità, secondo il quale va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorre un'effettiva esigenza di deterrenza, come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di "prestigio".

Il principio di finalità, secondo cui gli scopi perseguiti devono essere determinati, espliciti e legittimi (art. 11, comma 1, *lett. b)*, del codice). Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza.

Quando per un qualsiasi motivo il trattamento cessa i dati devono essere distrutti.

I propri dati personali devono essere gestiti custoditi e controllati secondo i tre criteri:

- progresso tecnico;
- natura dei dati;
- caratteristiche del trattamento.

Il progresso tecnico, cioè, la sicurezza in materia di dati personali deve andare di pari passo con l'evoluzione della tecnica: infatti se si rimane fermi ai sistemi operativi di qualche anno fa evidentemente sorgeranno problemi sulla problematica di cui si discute.

Il secondo elemento è *la natura dei dati* da tutelare; a tale proposito va detto che il cosiddetto dato personale "normale" non è un dato sensibile e quindi non abbisogna di particolare tutela. Cosa diversa invece è il dato personale sensibile il quale ha bisogno di un grado più elevato di tutela.

[4] Decreto legislativo 30 giugno 2003, n. 196. *"Codice in materia dei dati personali"*.
Art. 1. *Diritto alla protezione dei dati personali*
1. Chiunque ha diritto alla protezione dei dati che lo riguardano. *[Omissis]*

In buona sostanza quello di cui ci si preoccupa è di tutelare il dato personale nell'ambito del trattamento nel momento in cui lo stesso dato viene utilizzato. È utile evidenziare che ciascuno di noi nell'arco della giornata compie almeno una delle operazioni riguardanti il trattamento dei dati personali: raccolta, registrazione, organizzazione, conservazione, elaborazione. Chiaramente all'interno delle macro categorie dei dati personali dobbiamo includervi quella che ormai è conosciuta universalmente come dato sensibile. Cioè quel dato che è idoneo a rivelare l'origine dell'appartenenza etnica, delle convinzioni religiose, le opinioni politiche.

Infine, per quanto riguarda *le caratteristiche del trattamento*, se mai vene fosse bisogno, v'è da dire che oltre al trattamento informatico c'è, ad esempio, il trattamento cartaceo anche se a tale proposito occorre dire che, secondo quanto prescrive la norma sull'amministrazione digitale, in ambito pubblico il sistema cartaceo dovrà essere abbandonato entro il 2012. In ambito privatistico, tendenzialmente e in maniera più spedita, si sta andando verso la eliminazione del cartaceo; il che comporta necessariamente l'utilizzo della posta certificata, per acquisire certezza circa l'invio e il ricevimento della posta trasmessa mediante il sistema informatico: sul punto, è di questi giorni la firma di un protocollo di intesa tra il Ministero per la Pubblica Amministrazione e l'Innovazione e il Presidente dell'Istituto Nazionale della Previdenza Sociale per la diffusione della posta elettronica certificata ai cittadini. Quanto precedentemente detto, secondo uno studio fatto, comporterà a livello nazionale una risparmio di quasi 900 milioni di euro all'anno con grande vantaggio dell'ambiente ove si pensi che meno carta si usa e più alberi vengono risparmiati.

3. DATI QUASI SENSIBILI

Oltre alla categoria dei dati sensibili vi è anche quella dei dati "quasi sensibili" per come definiti ai sensi dell'art. 13 del decreto legislativo 30 maggio 2003, n. 196 secondo cui si intende per dati quasi sensibili: dati personali diversi da quelli sensibili e giudiziari il cui trattamento può comportare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare.

Dato quasi sensibile potrebbe essere per esempio il soggetto che è fallito; oppure una soggetto insolvibile; oppure altre categorie ancora da individuare. Occorre sottolineare che anche i dati giudiziari, necessitano di un livello maggiore di sicurezza informatica rispetto agli altri; sono gli atti relativi ai provvedimenti giudiziari *ex* articolo 686 del codice penale, i procedimenti di condanna sostanzialmente, la modifica del dato da indagato a imputato. I dati giudiziari di cui si è

appena detto sono quelli che necessitano di maggiore sicurezza. Si pensi ad esempio quale nefasta conseguenza provoca ai danni di un soggetto la notizia che appare su un giornale, che da indagato diventa imputato, quindi processato e successivamente viene riconosciuto innocente.

4. Amministratore di sistema

Il legislatore ha previsto la figura di amministratore di sistema con il decreto del Presidente della Repubblica 28 luglio 1999, n. 318, all'art. 1, che, da un punto di vista tecnico, sostanzialmente non era adeguato anche perché interpretava l'amministratore di sistema come soggetto al quale era affidato il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione[5]. Da quanto precede si evince che la definizione poteva considerarsi abbastanza limitata. Con il sistema della norma 196 del 2003 - codice in materia di protezione dei dati personali - l'amministratore di sistema non è scomparso, perché lo ritroviamo indirettamente nel disciplinare. Infatti le funzioni tipiche dell'amministrazione di sistema sono richiamate nel menzionato allegato B), nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione.

Con il consenso del Garante, in dottrina è stata ipotizzata la figura del responsabile esterno che è quel soggetto a cui compete normalmente il trattamento del dato all'esterno: si pensi alle banche, al commercialista, all'avvocato, a coloro che si occupano delle paghe per conto dei datori di lavoro e tutte le società che gestiscono servizi per conto terzi. I soggetti di cui si è appena detto sono i responsabili esterni.

Sebbene manchi una definizione, possiamo dire che *l'amministratore di sistema è quella figura professionale finalizzata alla gestione e alla manutenzione dell'impianto di elaborazione o dei suoi componenti*.

Il Garante prevede altre figure che sono equiparati all'amministratore di sistema come, ad esempio, quello che si occupa della protezione dei dati, delle reti, degli apparati di sicurezza.

---

[5] Decreto del Presidente della Repubblica 28 luglio 1999, n. 318. *"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675"*.

Art. 1. *Definizioni*.

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini si intendono per:

a) *[Omissis]*;

b) *[Omissis]*;

c) "amministratori di sistema": i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

L'amministratore di sistema riveste particolare importanza nell'ambito della sicurezza dei dati personali. Sul punto va evidenziato che nel nostro ordinamento non esistendo una norma che prevedesse tale figura e non c'era l'obbligo di designarlo.

Si tratta di una figura che nel nostro ordinamento è considerata rilevante, fondamentale soprattutto nelle organizzazioni medio grandi. Nelle organizzazioni piccole non è fondamentale se non per certi aspetti confidenziali, cioè non è necessario che sia data all'esterno la figura di amministratore di sistema perché può essere benissimo gestita all'interno.

Va evidenziato tuttavia che molte realtà quali società o enti pubblici hanno ritenuto giustamente di individuare tale figura anche se ciò, si ripete, non era obbligatorio; tanto è vero che spesso questa figura la si trova nel DPS (Documento Programmatico per la Sicurezza).

Il termine per la nomina dell'amministratore di sistema scadeva il 30 giugno 2009; il Garante, con proprio provvedimento, ha prorogato tale scadenza, salvo ulteriori proroghe, al 15 dicembre 2009.

5. Requisiti dell'amministratore di sistema

La prima cosa che pretende il legislatore è quella di individuare un soggetto idoneo a cui affidare le mansioni di amministratore di sistema. A tale proposito occorre evitare assolutamente gli incauti affidamenti nel senso che occorre accertarsi che chi è chiamato a svolgere le mansioni di amministratore di sistema sappia fare bene il suo "mestiere" e che abbia adeguate dimestichezze con le strutture che possono essere la Provincia, la Regione, i grandi Comuni, gli Ospedali eccetera. Occorre quindi fare una valutazione di quelle che sono le caratteristiche del soggetto che poi sarà incaricato del compito di amministratore di sistema. Sul punto va evidenziato che la designazione da parte del titolare è facoltativa ma se è designato occorre osservare il disposto dell'art. 29 del decreto legislativo 30 giugno 2003, n. 196.[6]

Uno concetto che va sottolineato è quello della affidabilità che viene applicato in tutti quegli ambiti pubblici e privati in cui il trattamento viene effettuato per fini amministrativi e contabili.

[6] Decreto legislativo 30 giugno 2003, n. 196. Art. 29. *Responsabile del trattamento*

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Spesso accanto i profili di carattere amministrativo-contabili di cui si è detto ci sono profili di dati sensibili, di dati giudiziari.

Riportiamo, adesso, il punto 19, dell'allegato B):

«Documento programmatico sulla sicurezza. 19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. *per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.»*

In questo documento (DPS) ci sono tutti gli elementi; l'elemento di amministratore di sistema richiama la distribuzione dei compiti e quello di responsabilità nell'ambito delle strutture preposte al trattamento dei dati personali quindi l'analisi dei rischi, le misure da adottare per garantire la protezione dei dati, la protezione degli ambiti locali, la custodia e l'accessibilità.

L’amministratore di sistema allo stesso modo del responsabile, deve essere nominato per iscritto e nell'atto di nomina devono essere indicati quali sono i suoi compiti. Occorre evidenziare che sull’atto di nomina va apposta la firma a cura del “nominato”.

Va detto immediatamente che lo stesso amministratore di sistema è autorizzato a gestire il sistema ma non anche a guardare la posta o gli stessi dati del sistema stesso senza alcun consenso.

Sul punto occorre dire che sono state fatte delle segnalazioni e dei ricorsi al Garante perché è stato appurato che qualche amministratore di sistema in precedenza si divertiva a “sbirciare”, non autorizzato, nella posta elettronica dei dipendenti, a sbirciare tra gli accessi ad Internet violando così la *privacy*. Questo ha determinato una serie di ricorsi con richieste di risarcimento danni.

Recentissimamente il Garante ha stabilito il divieto di *“sbirciare nei dati personali durante il collegamento a Internet”*. Nell’ambito del lavoro se, per ipotesi, viene provato da parte di chi è interessato che l'amministratore di sistema ha “curiosato” nei suoi dati personali durante il collegamento a Internet, il titolare è chiamato a rispondere di questa violazione e può essere richiesto del risarcimento dei danni. Il titolare dei dati, a sua volta, chiamerà in causa l'amministratore di sistema. Un'altra richiesta di risarcimento può essere formulata ai sensi dell’articolo 11 del codice il quale è un articolo che stabilisce le modalità del trattamento dei dati nelle sue diverse componenti.[7]

Chiaramente sbirciare nei dati personali del dipendente è una violazione dell'articolo 11 che può comportare in sede civile l'obbligo del risarcimento non patrimoniale che pone l'articolo 2050 del codice civile. Sul punto spetterà al titolare dimostrare di avere posto in essere tutti quegli accorgimenti per impedire il danno sotto il profilo della violazione della *privacy*. Occorre evidenziare che in termini civili rispondono sia il titolare dei dati personali che l'amministratore di sistema mentre in termini penali risponde il titolare del trattamento dei dati personali.

Quando l’amministratore di sistema può accedere direttamente o indirettamente ai dati che riguardano il personale è importante che il datore di lavoro renda conoscibile l'identità dell'amministratore di sistema attraverso varie informative da dare ai dipendenti come ad esempio quella prevista dall'articolo 13 del codice che riguarda il trattamento dei dati, i conseguenti scopi ecc. ecc.. A mo' di esempio si può dire che il dipendente viene informato che i suoi dati personali

[7] Decreto legislativo 30 giugno 2003, n. 196. Art. 11. *Modalità del trattamento e requisiti dei dati*

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   c) esatti e, se necessario, aggiornati;
   d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

potranno essere trattati sia pure occasionalmente dall'amministratore di sistema che è il signor tal dei tali e per gli scopi che si dichiarano.

Per quanto riguarda gli estremi identificativi dell'amministratore di sistema sono riconducibili sostanzialmente al nome, al cognome al riferimento nell'ambito dell'organizzazione, alle funzioni.

La legge dispone di ridurre per quanto possibile i rischi di accesso non autorizzato al sistema informatico. Lo stesso Garante nel suo provvedimento sottolinea che lo stesso amministratore di sistema deve trovare un blocco da qualche parte per impedire venga a conoscenza di dati sensibili.

Il momento più cruciale per l'amministratore di sistema è il rischio di perdita dei dati personali. Il trattamento dei dati personali è considerata alla stessa stregua del trasporto di merci pericolose ai sensi dell'articolo 2050 del codice civile. Così come chi trasporta merci pericolose in caso di incidente dovrà dimostrare di aver sposto in essere tutte le misure idonee a scongiurare tali incidenti analogamente lo stesso amministratore di sistema dovrà dimostrare di aver posto in essere tutte quelle misure idonee ad evitare la perdita dei dati personali.

Tutte le volte che viene affidato all'esterno il trattamento di dati personali al riguardo occorre sottolineare che ai sensi del punto 25 del citato disciplinare tecnico in materia di misure minime di sicurezza *"Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico."*

6. Funzione dell'amministratore di sistema

Il Garante evidenzia la necessità di sottolineare al titolare del trattamento dei dati personali di sviluppare una serie di cautele atte a garantire che lo svolgimento dei compiti dell'amministratore di sistema avvenga in conformità del più volte citato disciplinare e quindi del codice della *privacy*.

In altri termini il titolare dei dati è chiamato a porre in essere un sistema di controllo idoneo, sull'amministratore di sistema, che gli permetta di capire se questi "sta lavorando bene o meno." Infatti l'esigenza nasce dalla impellente necessità di tutela dei dati che sono sensibili come ad esempio: le credenze religiose; i gusti della gente in merito a questo o quel determinato prodotto; gusti alimentari. Queste notizie notoriamente vengono sfruttate in ambito commerciale e ciò di cui si discute non va d'accordo con l'esigenza della tutela della *privacy*.

In tale ambito occorre dunque fissare dei veri e propri paletti nei riguardi dell'amministratore di sistema stabilendo con precisione quali sono i limiti entro cui si può muovere. Ovviamente il titolare dei dati personali ha una posizione un po' delicata perché sua è la responsabilità circa la scelta dell'amministratore di sistema il quale se si rivela inidoneo può causare dei problemi al titolare che lo ha nominato, specialmente quando l'amministratore di sistema è scelto all'esterno dell'Ente.

Se il titolare dei dati non nomina l'amministratore di sistema con tutte le garanzie che la legge prevede può andare incontro a della responsabilità penali e civili stabilite dall'articolo 15 del codice della *privacy*. L'articolo suddetto stabilisce che chiunque cagiona danni per effetto del trattamento dei dati personali è tenuto al risarcimento dei danni ai sensi dell'articolo 2050 del codice civile.

7. Attività dell'amministratore di sistema

Dopo aver individuato il soggetto a cui affidare le mansioni di amministratore di sistema occorre stabilire che tipo di attività deve svolgere.

Quel che qui interessa è che l'incaricato deve svolgere bene il lavoro che gli viene affidato. A tale proposito, a seguito delle attività ispettive disposte dal Garante si è visto che la gran parte delle aziende e organizzazioni pubbliche e private hanno individuato nei loro DPS queste figure individuandole come responsabili.

Naturalmente alcuni adempimenti, che possono essere individuati, e le attività che occorre inserire nell'atto di nomina, se ci riferiamo a quello che dice il Garante, effettivamente sono pochissime cose del tipo: svolgere la supervisione dal punto di vista tecnico informatico nella gestione dei sistemi di certificazione e autorizzazione, assicurare la gestione degli aspetti tecnici informatici non attribuiti al singolo utente del sistema, effettuare delle copie di sicurezza per garantire l'integrità del sistema, gestire i sistemi di autenticazione in chiave, assicurare la custodia, supportare, dal punto di vista informatico, il titolare del trattamento dei dati personali nei controlli circa il corretto uso di Internet, di posta elettronica e degli altri strumenti elettronici utilizzati per fini lavorativi nel rispetto di quanto previsto dalla normativa e dal disciplinare. Si suggerisce di inserire quanto si è appena detto nell'atto di nomina dell'amministratore di sistema.

Occorre fare attenzione che se non è stato elaborato l'apposito disciplinare e se lo stesso non è stato approvato dai rappresentanti sindacali, ai sensi dell'articolo 4, della legge 20 maggio 1970, n. 300 (c.d. statuto dei lavoratori) non è possibile fare né controlli né contestazioni. Questo è un

argomento molto importante. Così anche sulla posta elettronica accenniamo brevemente: se c'è bisogno di accedere alla posta elettronica del collega o della collega in qualità di titolare o in qualità di amministratore di sistema occorre che questa eventualità sia prevista nel disciplinare altrimenti si commetterebbe un abuso. Va precisato che per quanto riguarda la posta elettronica si violerebbero le norme in materia di segreto epistolare e conseguentemente apprezzabile penalmente (se ci pensiamo un momento, questo tipo di controllo non deve essere inteso come un qualcosa che limiti la libertà personale di ognuno di noi nell'ambito lavorativo; è semplicemente, riteniamo, uno controllo sicuramente antipatico, se vogliamo, ma dovuto per accertarsi che in effetti non vi siano abusi circa l'uso di Internet che non può essere fatto per scopi personali, assolutamente estranei a quella che normalmente è l'attività del lavoratore; lo stesso uso della posta elettronica non può essere fatto per scopi personali ma esclusivamente al servizio dell'Ente).

Il soggetto che dovrà svolgere l'incarico di amministratore di sistema deve essere una persona fisica. Infatti il provvedimento si riferisce ad una serie di elementi personali che difficilmente possono essere imputate ad una società. Da quanto precede è evidente che se la designazione avviene all'interno della società questa deve ricadere necessariamente su una persona fisica perché ci sono dei profili di responsabilità che assolutamente non possono essere aggirati.

Va evidenziato detto che, soprattutto in certi casi, il soggetto deve essere individuato all'esterno perché ci sono delle realtà talmente piccole che non hanno al loro interno la professionalità necessaria per lo svolgimento di tale importante compito.

In questo caso queste realtà potranno rivolgersi all'esterno per individuare il soggetto cui affidare l'incarico di amministratore di sistema anche in forma associata per sopportare meglio i costi.

Secondo quanto ritenuto dal Garante l'affidamento è di tipo fiduciario ma niente impedisce che si proceda mediante selezione ad evidenza pubblica scegliendo poi il soggetto che offre le migliori garanzie delle quali si è discusso in precedenza.

Va anche detto come annotazione che ogni volta che si candida il soggetto che svolge l'incarico di amministratore di sistema non è necessario cambiare anche il DPS semplicemente lo si aggiorna allegando allo stesso, come allegato "A", per esempio, l'atto di nomina in maniera tale che lo stesso documento della sicurezza sia sempre aggiornato.

8. Verifica dell'attività dell'amministratore di sistema

Vediamo ora che cosa si intende per operato dell'amministratore di sistema, soggetto a controllo annuale. Quello che va sottoposto al controllo sono le attività che sono stabilite nell'atto di

nomina; si tratta di un controllo mirato e relativo all'attività tecnica organizzativa e l'attività relativa alla sicurezza. Quindi specificatamente un'attività rivolta all'amministratore di sistema.

Per quanto riguarda l'amministratore di sistema è stato detto che questi sono soggetti ad una verifica dell'attività; questa secondo quanto ci dice il provvedimento del Garante deve essere con cadenza almeno annuale; ciò non significa che debba essere fatta necessariamente soltanto una volta all'anno, in effetti tale verifica può essere fatta più volte in un anno in maniera tale da controllare la rispondenza alle misure organizzative e tecniche e di sicurezza rispetto al trattamento dei dati personali previste dalle norme vigenti.

Da quanto precede non si può non desumere una circostanza che non è assolutamente secondaria. Infatti per il titolare del trattamento dei dati personali nelle realtà piccole, dove non ci sono i soggetti che hanno le conoscenze necessarie, diventa difficile fare la verifica allora potrebbe essere necessario affidarsi al consulente per controllare l'amministratore di sistema.

Nel merito va ricordato che è obbligatorio che ciascuna impresa, ciascuna amministrazione pubblica sia dotata di un disciplinare interno sull'uso degli strumenti informatici da parte dei dipendenti, quindi, Internet e posta elettronica. Questo disciplinare è importante perché ci legittima ad effettuare dei controlli circa gli abusi che ci possono essere avuto riguardo al collegamento a Internet nonché eventuale accessi alla posta elettronica. Senza il disciplinare i controlli di cui si discute sarebbero illegittimi.

E' stato chiarito prima. Se ci si trova in una piccola realtà dove non c'è una ditta esterna né, tantomeno, l'amministratore di sistema, non è obbligatorio nominarlo ma è sufficiente fare acquisire le opportune conoscenze al personale interno; lo dice il Garante anche nella parte introduttiva del provvedimento stesso.

<<<<<<<<<<§>>>>>>>>>>

** In «ALTALEX» – Quotidiano scientifico di informazione giuridica, pubblicato su Internet all'indirizzo http://www.altalex.com, ISSN 1720-7886, Ottobre 2009, pag. http://www.altalex.com/index.php?idnot=47812*

*** Segretario Generale della Città di Norcia (PG)*