

---

CATERINA FLICK - VINCENZO AMBRIOLA

---

## **FUNZIONI E RESPONSABILITÀ DI AMMINISTRATORI E OPERATORI DI SISTEMA NELLA SOCIETÀ DELL'INFORMAZIONE E DELLA COMUNICAZIONE**

---

**SOMMARIO:** 1. Introduzione. — 2. Utenti, operatori e amministratori di sistema nel linguaggio informatico. — 3. Amministratore di sistema e privacy. — 4. Aspetti tecnici nella gestione documentale: sistema di protocollo informatico e certificati firma elettronica. — 5. Amministratore di sistema e responsabilità d'impresa. — 6. Reati informatici e abuso della qualità di operatore di sistema. — 7. Un problema comune: il rischio del controllo a distanza del lavoratore. — 8. Conclusioni.

---

### **1. INTRODUZIONE.**

---

L'uso avanzato di sistemi informatici per la gestione delle attività degli enti (imprese e amministrazioni) rende necessario adottare misure e sistemi di sicurezza sempre più complessi, sia dei sistemi che dei dati (personali e non) in essi contenuti. La sicurezza dei dati e dei sistemi è utile agli enti, non solo a tutela dei dati personali trattati, ma anche a tutela del patrimonio dell'impresa e delle relazioni con altri enti, clienti e fornitori. In questo contesto l'attribuzione di compiti e l'assunzione di responsabilità di coloro che svolgono mansioni tecniche deve affiancare e integrare la responsabilità di coloro che svolgono mansioni di carattere organizzativo-amministrativo.

E infatti le norme giuridiche che disciplinano la società dell'informazione e della comunicazione richiamano di frequente le figure tecniche — sistemisti, programmatori, amministratori di sistema — che si occupano della gestione dei sistemi informatici o di attività connesse, i quali non sempre ricoprono ruoli di responsabilità nelle strutture presso le quali operano, riconoscendo loro un ruolo giuridicamente rilevante, dal quale possono derivare responsabilità sul piano civile e penale.

Il ruolo chiave svolto dai tecnici nella società dell'informazione e della comunicazione, in effetti, era già stato evidenziato da diverse norme. Prima fra tutte la Legge 547 del 1993, che ha introdotto nel Codice Penale i reati informatici, che prevede come aggravante speciale il fatto di avere commesso un crimine informatico con abuso della qualità di operatore

---

\* I paragrafi 1, 3, 4, 5, 6, 7, 8 sono riconducibili all'elaborazione esclusiva di Caterina Flick, il paragrafo 2 è riconduci-

bile all'elaborazione esclusiva di Vincenzo Ambriola.

di sistema, e ne fa discendere la procedibilità d'ufficio anche per reati che, nell'ipotesi base, sono procedibili a querela di parte. Ancora, il D.P.R. 445/00, Testo Unico sulla Documentazione Amministrativa, attribuisce al responsabile del servizio per la tenuta del sistema di protocollo informatico delle amministrazioni pubbliche diverse responsabilità per lo svolgimento di attività di carattere tecnico, che presuppongono una buona competenza tecnica. Il D.Lgs. 82/05, Codice dell'Amministrazione Digitale, prevede che coloro che operano come certificatori della firma digitale, i quali devono possedere caratteristiche tecniche ben precise, abbiano i requisiti di onorabilità richiesti per l'esercizio dell'attività bancaria; a carico di tali soggetti, inoltre, la Legge 48 del 2008, che ha dato attuazione alla Convenzione di Budapest sul cybercrime, ha inserito nel Codice Penale la frode nell'attività di certificazione della firma elettronica, che si configura come reato proprio del certificatore. La medesima Legge ha infine introdotto i crimini informatici tra i reati presupposto per l'applicazione della responsabilità amministrativa delle imprese, prevista dal D.Lgs. 231/01, di fatto collocando i responsabili dei sistemi informativi tra i principali destinatari delle procedure aziendali di prevenzione e controllo.

Il provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008 — contenente misure e accorgimenti che i titolari dei trattamenti effettuati con strumenti elettronici devono adottare nell'attribuire le funzioni di amministratori di sistema — pur affrontando, come è logico, esclusivamente i profili connessi con la tutela della privacy, ha il pregio di sottolineare con grande chiarezza l'importanza fondamentale dell'attività svolta da coloro che si occupano della gestione dei sistemi informatici nell'ambito di enti pubblici e privati. Il provvedimento ha tuttavia destato perplessità e critiche, poiché impone ai titolari del trattamento (specie alle organizzazioni aziendali complesse) degli adempimenti onerosi, sia dal punto di vista tecnico che dal punto di vista economico, e difficilmente gestibili dal punto di vista dei rapporti di lavoro.

Ad eccezione del provvedimento del Garante — che introduce definizioni tecniche sulle quali basa gli adempimenti imposti per il trattamento dei dati personali — le norme sopra indicate, pur evidenziando l'importanza di figure e ruoli squisitamente tecnici, non forniscono alcuna definizione, limitandosi tutt'al più a individuare attività e compiti da svolgere.

L'esame del provvedimento del Garante fornisce dunque l'occasione per chiedersi: chi siano le figure tecniche rilevanti; quali funzioni e mansioni svolgano; se vi siano, e quali siano, delle regole di carattere generale a cui devono attenersi.

In questo lavoro si intende dare una risposta a queste domande tenendo conto sia di profili tecnici che delle norme giuridiche.

## 2. UTENTI, OPERATORI E AMMINISTRATORI DI SISTEMA NEL LINGUAGGIO INFORMATICO.

Tutti coloro che operano su un sistema informatico sono individuati mediante un profilo (*account*) definito in base al ruolo ricoperto, alle mansioni svolte e ai dati accessibili. Una volta definito il profilo, l'accesso al sistema da parte di una persona con il proprio profilo avviene utilizzando una cre-

denziale di autenticazione, generalmente consistente in una password (che può essere cambiata solo da chi l'ha creata<sup>1</sup>), tale da permettere al sistema di riconoscere colui che accede e di farlo operare soltanto sui dati e con le attività consentite dal profilo; è evidente che l'accesso al sistema utilizzando il profilo e la password di un altro consente di sostituirsi a quest'ultimo in tutte le operazioni che si compiono sul sistema. A seconda di come è configurato, il sistema può mantenere traccia sia dell'accesso, sia di tutte le operazioni (modifiche) effettuate durante la permanenza sul sistema.

In base al ruolo ricoperto e al profilo attribuito, la persona può accedere solo ad applicazioni e dati (cd. accesso applicativo), oppure direttamente al sistema (cd. accesso di sistema) mediante il cosiddetto account di *root*. A sua volta l'accesso di sistema può essere effettuato con diversi ruoli (di amministratore o di operatore) ma, in ogni caso, comporta per i dati un rischio maggiore, poiché, in teoria, è illimitato. L'accesso di sistema con l'account di *root* permette di accedere a tutti i dati visibili ai diversi profili, ma non alla password scelta dal titolare del profilo; tuttavia se le informazioni sono crittografate (tramite appositi programmi) esse non sono visibili nemmeno da chi ha accesso di *root*.

Dal punto di vista di coloro che accedono e operano su un sistema informatico la prima distinzione fondamentale è quella tra utente e sistemista. L'utente è inteso come colui che utilizza le applicazioni software per svolgere i propri compiti (scrivere una lettera, leggere la posta elettronica, accedere a un sito, aggiornare i dati contenuti in un archivio informatico e così via); i limiti alla sua operatività sono, come detto, impostati nel profilo. Il sistemista è, invece, colui che ha le competenze e i permessi (privilegi) per intervenire direttamente sul sistema (installare una nuova applicazione software, creare un nuovo utente, configurare una stampante e altre attività).

La situazione che coinvolge i sistemisti è più complessa: il ruolo tecnico di sistemista è infatti articolato in numerose figure professionali, che si rivolgono a un sistema inteso come un insieme di risorse hardware, software e di rete e si differenziano per le mansioni svolte. In ogni caso esiste una distinzione fondamentale tra « operatore » e « amministratore » di sistema, basata non solo sulle mansioni svolte ma, soprattutto, sulle diverse responsabilità attribuite. Infatti, mentre l'amministratore ha la responsabilità della gestione del sistema e la direzione delle risorse umane, l'operatore agisce in subordine alle indicazioni che gli vengono date dall'amministratore. A seconda delle dimensioni dell'azienda, o delle infrastrutture di cui dispone e con cui opera, vi può essere una sola persona o uno staff di persone che si occupano dell'amministrazione e della gestione del suo sistema informatico; ancora vi può essere un ufficio interno (dipartimento Information Technology o simili) in cui lavorano dipendenti dell'azienda e collaboratori esterni, oppure l'intera attività di amministrazione e gestione del sistema informatico può essere affidata a un soggetto, persona fisica o giuridica, esterno.

Entrando nel merito delle mansioni svolte di norma, l'amministratore di sistema è colui che ha la responsabilità completa del sistema o dei sistemi a lui assegnati e ne risponde direttamente nei confronti della direzione.

<sup>1</sup> Sempre più spesso la credenziale di autenticazione comporta un riconoscimento

to biometrico, attraverso impronta vocale, impronta digitale ecc.

L'amministratore di sistema si caratterizza per la vasta competenza tecnica e per la conoscenza dell'organizzazione aziendale, tali da consentirgli di individuare e risolvere i problemi che si presentano, e per la capacità di assunzione di responsabilità in qualunque evenienza.

I compiti di un amministratore di sistema sono di vario genere e cambiano da un'organizzazione a un'altra; le numerose attività che svolge possono essere classificate per macro categorie: gestione delle risorse hardware destinate a memorizzare i dati (predispersione del piano di sostituzione delle risorse, per evitarne l'obsolescenza simultanea); della configurazione del sistema (configurazione del parco macchine affinché le applicazioni software possano svolgere meglio le loro funzioni); gestione delle risorse di rete, ovvero di tutti gli apparati che collegano i calcolatori tra di loro e verso l'esterno; gestione delle risorse software che interagiscono direttamente con l'hardware e la rete e delle applicazioni software che costituiscono il cosiddetto software applicativo (allineamento con la versione più recente disponibile); gestione dell'utenza (account); gestione dei dati, mediante salvataggio periodico (back-up).

In generale l'amministratore è responsabile della pianificazione e della definizione delle strategie di evoluzione dei sistemi informatici, la supervisione e la formazione degli operatori informatici, la consulenza informatica e il supporto allo staff; l'uso del software applicativo da parte del personale all'interno dell'azienda. Questo comporta la conoscenza dei sistemi operativi e del software applicativo, così come la capacità di individuare problemi hardware e software, ma anche la conoscenza delle ragioni per cui le risorse umane all'interno dell'organizzazione utilizzano le specifiche applicazioni software<sup>2</sup>.

L'amministratore di sistema è responsabile dell'esercizio del software applicativo e non delle sue funzionalità: ciò che caratterizza l'amministratore di sistema è la sua indipendenza dalle applicazioni installate sul sistema, nel senso che l'amministratore non è responsabile del corretto svolgimento delle loro funzioni. In altre parole, se un'applicazione software che realizza la contabilità finanziaria commette un errore di imputazione di una posta in bilancio, la responsabilità è di chi lo ha realizzato e non di chi l'ha installato.

L'operatore di sistema ha una responsabilità limitata alle funzioni a lui assegnate su uno o più sistemi e risponde all'amministratore; l'attribuzione dei compiti agli operatori di sistema è effettuata dall'amministratore, in base alle risorse a sua disposizione. In alcune situazioni può accadere

---

<sup>2</sup> In alcuni casi si tende a precisare maggiormente il ruolo degli amministratori di sistema, con riferimento a particolari mansioni loro affidate: l'Amministratore della sicurezza si occupa di tutte le problematiche relative alla protezione di un sistema informatico nei confronti di attacchi che possono provenire dall'interno (dai calcolatori connessi in rete locale) e dall'esterno (da calcolatori esterni che possono accedere al sistema tramite la connessione internet o altre connessioni in rete non locale), la sua attività include l'amministrazione dei

sistemi di sicurezza, come i firewall, e la consulenza sulla politica di sicurezza e sulle misure specifiche da adottare; l'amministratore web è colui che si occupa della manutenzione del sito e dei servizi web, compresi gli accessi dall'interno e dall'esterno. I suoi compiti includono la gestione dei siti, l'amministrazione della sicurezza, la configurazione delle componenti software necessarie per il funzionamento. Il provvedimento del Garante richiama anche l'amministratore di sistemi software complessi e l'amministratore di basi di dati.

che l'amministratore svolga anche mansioni tipiche dell'operatore, sia perché non vuole delegare altri al loro svolgimento sia perché non dispone di sufficienti risorse umane. Operatore è colui che effettua le operazioni giornaliere (di routine), come la sostituzione di supporti di backup. Generalmente tali compiti richiedono la presenza fisica nella sala macchine dell'organizzazione (il locale tecnico al cui interno sono collocati i server) per cui l'operatore di sistema, pur non possedendo la medesima competenza tecnica richiesta all'amministratore di sistema, deve avere un analogo livello di fiducia, dato che ha la possibilità di accedere a dati importanti e riservati (non solo dati personali).

Tuttavia, gli operatori generalmente non hanno la comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni, semantica delle funzioni). Inoltre, di solito, nelle aziende gli operatori non hanno qualifiche professionali elevate (da un punto di vista gerarchico): in quanto operatori essi sono inquadrati ai livelli più bassi della scala gerarchica e rispondono a persone che sono loro superiori in grado. In sostanza, il fatto di accedere con l'account di *root* non è sufficiente a trasformare l'operatore in amministratore del sistema.

L'accesso ai dati contenuti nel sistema informatico da parte dei sistemisti (amministratori o operatori che siano) in teoria, e a priori, non ha alcun limite. In pratica l'assegnazione delle attività agli operatori di sistema può portare ad una compartimentalizzazione che, di fatto, può limitarne l'accesso. In situazioni limite l'amministratore di sistema non può accedere alle singole risorse hardware perché l'accesso a queste risorse è assegnato direttamente agli operatori di sistema. Per evitare la perdita di controllo si può richiedere che chi ha accesso all'account di *root* di un sistema informatico depositi le relative credenziali in busta chiusa al suo superiore, affinché questi possa usarle in caso di necessità. Si possono inoltre introdurre tecniche di tracciamento automatico delle operazioni svolte dall'account di *root*. Vi può essere il caso dell'amministratore di sistema che nell'attribuire gli incarichi riserva ad altri (operatori) l'accesso all'account di *root*, pur mantenendo la possibilità e la responsabilità di verifica sulle attività svolte dai suoi subordinati.

### 3. AMMINISTRATORE DI SISTEMA E PRIVACY.

Il provvedimento del Garante per la protezione dei dati personali<sup>3</sup> recante «*Misure e accorgimenti prescritti ai titolari dei trattamenti effet-*

<sup>3</sup> Provvedimento generale del 27 novembre 2008, pubblicato in *G.U.* n. 300 del Garante per la protezione dei dati personali 27 dicembre 2008; pubblicato in questa *Rivista*, 2009, 611. I termini per l'adempimento delle prescrizioni sono stati prorogati una prima volta al 30 giugno 2009, con provvedimento del 12 febbraio 2009, recante *Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni*

*delle funzioni di amministratore di sistema* (pubblicato in *G.U.* n. 45 del 24 febbraio 2009). I termini sono stati ancora prorogati al 15 dicembre 2009, con provvedimento del 25 giugno 2009, recante *Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuate con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento* (pubblicato in *G.U.* n. 149 del 30

*tuati con strumenti elettronici relativamente alla attribuzione delle funzioni di amministratore di sistema* » ha il pregio di evidenziare con estrema chiarezza l'importanza che le figure tecniche rivestono nella società dell'informazione e della comunicazione.

Il Garante parte dal presupposto che i tecnici — che, all'interno di aziende e di organizzazioni pubbliche e private, si occupano a qualunque titolo di gestire i sistemi informatici — svolgono mansioni di grande importanza e delicatezza, poiché si trovano nelle condizioni di poter accedere senza limiti ai sistemi e alle informazioni. L'importanza di tali figure non sempre è riconosciuta. Spesso, infatti, i responsabili delle organizzazioni pubbliche e private, grandi e piccole, non sono consapevoli delle criticità insite nello svolgimento delle mansioni connesse con l'amministrazione dei sistemi informatici e al trattamento informatizzato dei dati; a volte anche coloro che dovrebbero essere preposti a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico sottovalutano le criticità e ne trascurano i rischi connessi.

Il provvedimento nasce, dunque, nell'intento di tutelare gli interessati rispetto al trattamento di dati effettuato dagli amministratori di sistema da perseguire attraverso diverse vie.

La prima via è la consapevolezza. È necessario che il pubblico e i titolari del trattamento — che impiegano per la gestione di banche dati o reti informatiche, sistemi informatici utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemiche — siano consapevoli dell'importanza del ruolo e delle mansioni svolte dai sistemisti, nonché dei rischi connessi allo svolgimento di tali mansioni. In particolare, occorre acquisire consapevolezza circa il fatto che i sistemisti, avendo le capacità tecniche e la possibilità pratica di introdursi nel sistema informatico, possono (volontariamente o casualmente) accedere a dati personali a cui non sono legittimati ad accedere.

La seconda via è la cautela. È necessario promuovere l'adozione di cautele specifiche nell'individuazione di coloro che amministrano i sistemi informatici e la predisposizione di misure tecniche e organizzative, dirette a scegliere oculatamente gli amministratori di sistema e ad agevolare l'esercizio dei doveri di controllo da parte del titolare: tali cautele possono essere considerate, a pieno titolo, come misure utili a incrementare la complessiva di sicurezza dei trattamenti svolti. Alla luce di quanto previsto dall'art. 31 del codice, dunque, l'adozione di cautele nell'individuazione di coloro che svolgono le mansioni di amministratore di sistema è per i titolari un obbligo, la cui violazione può comportare l'applicazione delle sanzioni, anche penali previste dallo stesso codice.

La terza via è la trasparenza. È necessario che le attività a rischio possano essere ricostruite. Il Garante ritiene inoltre necessario consentire la conoscibilità dei sistemisti, e di alcune fasi di trattamento, all'interno delle organizzazioni; in quest'ottica il provvedimento individua alcune misure

---

giugno 2009); tale ultimo provvedimento ha anche introdotto alcune modifiche agli adempimenti previsti. Nel frattempo, con provvedimento del 21 aprile 2009 (pubblicato in *G.U.* n. 105 dell'8 maggio 2009) è stata attivata la consultazione pubblica,

all'esito della quale è stata pubblicata una lista di FAQ (Frequent Asked Question) con relative risposte. Con comunicato stampa del 10 dicembre 2009 il Garante ha inoltre dato alcune precisazioni sugli amministratori di sistema.

di carattere organizzativo che favoriscono la conoscenza nell'ambito delle organizzazioni dell'esistenza dei ruoli e delle mansioni svolte dai sistemisti e, in alcuni casi, dell'identità di coloro che operano come sistemisti in relazione ai diversi servizi e banche dati.

Il provvedimento definisce gli amministratori di sistema come «*figure professionali finalizzate alla gestione di un impianto di elaborazione o di sue componenti*» e, per quanto riguarda l'applicazione del provvedimento, assimila ad essi tutti coloro che svolgono «*mansioni analoghe*» a quelle svolte dagli amministratori di sistema, intendendo come tali le mansioni che prevedono lo svolgimento di attività che comportano rischi per la protezione dei dati personali. Sono, dunque, considerati amministratori di sistema tutti i sistemisti che svolgono mansioni che prevedono o permettono di intervenire sui dati personali, anche se le attività da essi svolte non consentono la conoscibilità dei dati (ad esempio in caso di cifratura dei dati). Essi infatti, «*pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo — significato dei dati, formato delle rappresentazioni e semantica delle funzioni — nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati personali*».

A titolo esemplificativo sono richiamate alcune mansioni e funzioni tipiche, in gran parte previste dall'Allegato B al codice, riconducibili agli amministratori di sistema: si va dalla realizzazione di copie di sicurezza — operazioni di *back up* e *recovery* dei dati — alla custodia delle credenziali di gestione dei sistemi di autenticazione e di autorizzazione, all'organizzazione dei flussi di rete, alla gestione dei supporti di memorizzazione e la manutenzione hardware.

Restano esclusi dalla nozione di amministratore di sistema esclusivamente coloro che accedono agli applicativi<sup>4</sup> e i sistemisti che intervengono solo occasionalmente<sup>5</sup> sui sistemi informatici.

L'estensione della nozione di amministratore di sistema, precisa il Garante, è determinata dalla «*particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione"*». Al riguardo il Garante richiama sia le indicazioni desumibili dal Codice Penale, che prevede per i reati informatici la circostanza aggravante, costituita dall'aver agito con abuso della qualità di operatore del sistema, sia la definizione contenuta nel previgente D.P.R. 318/1999 (art. 1, co. 1, lett. c), che qualificava l'amministratore di sistema come soggetto con il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione salvo poi smentire tale richiamo in un secondo momento<sup>6</sup>.

<sup>4</sup> In quanto l'accesso a un'applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati, FAQ 22.

<sup>5</sup> Ad esempio per scopi di manutenzione a seguito di guasti o malfunzioni, FAQ 1

<sup>6</sup> Nella FAQ 1 il Garante infatti af-



Dopo la lunga premessa il provvedimento individua una serie di adempimenti complessivamente volti, nelle intenzioni del Garante, a tutelare gli interessati rispetto al trattamento dei dati personali effettuato dagli amministratori di sistema. Gli adempimenti, unificati con quelli relativi al documento programmatico per la sicurezza (DPS), dovrebbero essere adottati, grazie alla proroga contenuta nel provvedimento del 25 giugno 2009, entro il 15 dicembre 2009. Il provvedimento dello scorso giugno, inoltre, a seguito dei dubbi interpretativi sollevati, ha individuato espressamente, quali destinatari degli obblighi, anche i responsabili del trattamento nominati ex art. 29.

Il Garante, richiamando i poteri attribuiti dall'art. 154, co. 1 lett. c) del codice, ha imposto regole per l'attribuzione delle funzioni tecniche corrispondenti o assimilabili a quelle di amministratori di sistema.

Gli adempimenti previsti sono di diverso tipo:

*Valutazione delle caratteristiche soggettive.* — L'attribuzione delle funzioni di amministratore di sistema deve avvenire sempre con i criteri richiesti dall'art. 29 del codice per la designazione dei responsabili del trattamento, cioè previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato (qualità tecniche, professionali e di condotta), le quali devono essere tali da garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza<sup>7</sup>. La valutazione delle qualità tecniche, professionali e di condotta deve essere fatta anche quando i sistemisti sono designati quali incaricati del trattamento ai sensi dell'art. 30 del codice.

*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 (o la descrizione puntuale degli stessi) evitando l'attribuzione di ambiti insufficientemente definiti, così come previsto dall'art. 29, co. 4 del codice.

*Elenco degli amministratori di sistema.* — Gli estremi identificativi delle persone fisiche amministratori di sistema, cioè i dati utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da tenere aggiornato e disponibile in caso di accertamenti da parte del Garante<sup>8</sup>.

---

ferma: *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.* La precisazione desta qualche perplessità, perché da un lato si limita la platea agli amministratori di sistema, individuando solo gli operatori dotati di specifici privilegi, dall'altro la si

amplia nuovamente (lo si chiarisce nel testo del provvedimento) anche agli operatori, addirittura quando non trattano dati in chiaro.

<sup>7</sup> La formulazione del provvedimento, dispositivo 2.a, che sembra richiedere che sia il soggetto designato a fornire idonea garanzia, è presumibilmente frutto di un errore materiale, sia per il tenore letterale dell'art. 29, espressamente richiamato, sia perché il fornire assicurazioni circa il rispetto delle norme, disgiunta dalla valutazione della professionalità, rischierebbe di trasformarsi nella redazione di un'inutile autocertificazione o di una mera dichiarazione di intenti.

<sup>8</sup> Con il provvedimento del 25 giugno



*Conoscibilità degli amministratori di sistema.* — 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 può avvenire: avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del codice nell'ambito del rapporto di lavoro che li lega al titolare; tramite il disciplinare tecnico che regola l'uso della posta elettronica e di internet sul luogo di lavoro<sup>9</sup>; mediante strumenti di comunicazione interna (ad es., *intranet* aziendale, ordini di servizio a circolazione interna o bollettini); tramite procedure formalizzate a istanza del lavoratore<sup>10</sup>. L'obbligo di conoscibilità è escluso nei casi, e nei settori, disciplinati in modo difforme da un'eventuale disposizione di legge.

Rispetto a questo adempimento il Garante ha precisato che il regime di conoscibilità degli amministratori di sistema è limitato ai soli trattamenti inerenti i dati del personale e dei lavoratori e che «*I titolari sono tenuti a instaurare un regime di conoscibilità dell'identità degli amministratori di sistema, quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori, nel caso in cui un amministratore di sistema, oltre a intervenire sotto il profilo tecnico in generici trattamenti di dati personali in un'organizzazione, tratti anche dati personali riferiti ai lavoratori operanti nell'ambito dell'organizzazione medesima o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti*»<sup>11</sup>.

*Servizi in outsourcing.* — Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare del trattamento deve conservare direttamente e specificamente, per ogni evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Tale compito può essere delegato al responsabile designato ai sensi dell'art. 29, all'atto della designazione o nel contratto di affidamento del servizio<sup>12</sup>.

*Verifica delle attività.* — L'operato degli amministratori di sistema, in particolare la conformità delle attività svolte alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza — 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 (l'adeguatezza deve essere valutata in rapporto alle condizioni organizzative e operative dell'organizzazione). Tale compito può essere delegato al responsabile designato ai sensi dell'art. 29, all'atto della designazione o, nel caso di servizi affidati in *outsourcing*, nel contratto di affidamento del servizio<sup>13</sup>.

2009 è stato eliminato l'obbligo, previsto inizialmente, di riportare l'elenco degli amministratori di sistema nel Documento Programmatico della Sicurezza.

<sup>9</sup> La cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58).

<sup>10</sup> Tale possibilità è stata inserita con provvedimento del 26 giugno 2009.

<sup>11</sup> FAQ 2 e 18.

<sup>12</sup> Tale possibilità di delega è stata inserita con provvedimento del 26 giugno 2009.

<sup>13</sup> Tale possibilità di delega è stata inserita con provvedimento del 26 giugno 2009.

*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.

Sono esclusi dall'ambito di applicazione del provvedimento i trattamenti effettuati a fini amministrativo-contabile — già oggetto, nel corso del 2008, di misure di semplificazione — sul presupposto che essi pongono minori rischi per gli interessati<sup>14 15</sup>.

Il Garante ha infine di recente precisato<sup>16</sup> che le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente, e non si applicano, invece, a quei soggetti che «*generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso*».

#### 4. ASPETTI TECNICI NELLA GESTIONE DOCUMENTALE: SISTEMA DI PROTOCOLLO INFORMATICO E CERTIFICATI FIRMA ELETTRONICA.

Si è evidenziato in premessa come le tecnologie siano determinanti nelle società dell'informazione; nella Pubblica Amministrazione l'uso (adeguato e corretto) degli strumenti informatici ha assunto un ruolo determinante: nella gestione documentale; nell'organizzazione delle attività; nei rapporti con le altre amministrazioni; nel rapporto con i cittadini (comunicazione, servizi, accesso). Nella gestione documentale, inoltre, è determinante l'utilizzo di certificati di firma elettronica rilasciati da soggetti competenti. In questo contesto si deve garantire la sicurezza non solo dei dati personali, ma anche di quelli che riguardano altri tipi di informazioni e i dati di sistema.

Il Testo Unico della Documentazione Amministrativa (T.U.D.A.) disciplina, tra l'altro, il sistema di protocollo informatico, che, da un lato, sostituisce il registro di protocollo, dall'altro costituisce il sistema su cui si basa la gestione documentale della Pubblica Amministrazione<sup>17</sup>. In particolare, il sistema di protocollo informatico deve consen-

<sup>14</sup> Art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Prov. Garante 6 novembre 2008.

<sup>15</sup> Il Garante ha precisato che rientrano nei trattamenti di carattere amministrativo-contabile, come tali esclusi dall'ambito applicativo del provvedimento, quelli fina-

lizzati, ad esempio, alla gestione dell'auto-parco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali, ecc. (FAQ 24).

<sup>16</sup> Comunicato stampa del 10 dicembre 2009.

<sup>17</sup> Per approfondimenti sul tema cfr. G.A. CIGNONI-C.FLICK, *Protocollo! Proto-*

tire ai dipendenti pubblici l'accesso ai dati e ai documenti, secondo profili definiti e nel rispetto della normativa in materia di protezione dei dati personali.

Non sempre la responsabilità della gestione è affidata ai sistemisti. Il T.U.D.A. nella parte in cui individua il responsabile del protocollo informatico attribuisce specifiche mansioni con riferimento alla gestione del registro di protocollo e dei registri di sicurezza. La norma richiede che il responsabile del servizio possieda requisiti professionali idonei, ivi compresa la competenza archivistica, ma non che abbia competenze informatiche, nonostante il suo ruolo possa comportare la necessità di interventi informatici di sistema. Il responsabile infatti: attribuisce il livello di autorizzazione per l'accesso alle funzioni delle procedure (distinguendo tra abilitazione alla consultazione e abilitazione all'inserimento e alla modifica delle informazioni) garantisce il corretto svolgimento di operazioni di registrazione e di produzione e conservazione del registro giornaliero; cura le attività di ripristino delle funzionalità del sistema in caso di guasti e anomalie; conserva le copie (registro di emergenza e registro rimovibile e delle pratiche definite); garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali; autorizza le operazioni di annullamento delle registrazioni (informazioni non modificabili).

Per altro verso, in relazione alla produzione e conservazione di documenti informatici con piena efficacia giuridica, il Codice dell'Amministrazione Digitale richiede ai certificatori di firma elettronica (o loro legali rappresentanti) il possesso dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche<sup>18</sup>; nel caso di certificatori accreditati presso il CNIPA tali requisiti devono essere posseduti anche da coloro che sono preposti all'amministrazione e dai componenti degli organi preposti al controllo. Il certificatore ha diversi obblighi: deve essere o avvalersi di personale tecnicamente competente, in particolare con riferimento alle tecnologie di firma elettronica e le procedure di sicurezza; deve utilizzare tecnologie affidabili; deve adottare misure contro la contraffazione dei certificati.

Il certificatore ha compiti squisitamente tecnici (il rilascio del certificato secondo le norme tecniche in vigore) e giuridici (l'identificazione del richiedente). Il certificatore è responsabile per i danni a terzi, subiti da chi abbia fatto affidamento sul certificato, in caso di eventi connessi con il certificato stesso. Infatti il certificato deve contenere tutte le informazioni, esatte e complete, necessarie per la verifica della firma contenuta nel certificato, la data del rilascio, la completezza dei requisiti necessari per la qualifica di certificato qualificato. Il certificato deve inoltre contenere i dati del firmatario e i dati per la creazione e la verifica della firma. Nello svolgimento della propria attività il certificatore ha diversi obblighi che vanno dall'i-

collo! La difficile integrazione fra informatica e diritto, in *Rass. Giur. Energia Elettrica*, 2003, 705; V. AMBRIOLA-C.FLICK, *La cittadinanza amministrativa telemati-*

*ca fra previsioni normative ed effettività*, in questa *Rivista*, 2006, 825.

<sup>18</sup> Art. 26 del D.Lgs. 385/93, T.U. bancario.

identificare il richiedente e specificare i suoi poteri, previa verifica della documentazione attestante la presenza di tali requisiti; al rilascio del certificato in conformità con le regole tecniche in vigore e seguendo criteri determinati di pubblicità e curarsi di pubblicare tempestivamente l'eventuale sospensione o revoca del certificato; alla corretta tenuta della registrazione delle informazioni per venti anni, utilizzando sistemi affidabili per la gestione del registro<sup>19</sup>.

## 5. AMMINISTRATORE DI SISTEMA E RESPONSABILITÀ D'IMPRESA.

Anche nel settore privato, in particolare nello svolgimento dell'attività imprenditoriale, l'utilizzo di sistemi informatici è di estrema importanza, con conseguente evidente rilevanza dei ruoli tecnici. Per l'impresa la sicurezza dei sistemi e dei dati è fondamentale, da un lato per la tutela del patrimonio, dall'altro per la tutela della riservatezza dei rapporti con clienti e fornitori.

La legge sulla responsabilità amministrativa delle persone giuridiche, società e associazioni (per comodità enti), come novellata nel 2008, ha introdotto i reati informatici come presupposto per l'individuazione della responsabilità dell'impresa, imponendo così alle imprese di adottare modelli organizzativi che tengano conto delle attività svolte dai sistemisti<sup>20</sup>. Al riguardo è importante considerare il fatto che nella gestione dei sistemi informatici gli amministratori di sistema svolgono attività e assumono decisioni che possono sfuggire al controllo degli organi amministrativi, di norma privi di competenze informatiche avanzate, specie se il ruolo di amministratore di sistema è svolto da soggetti che hanno con l'ente un rapporto di *outsourcing*.

Da tali peculiarità deriva la necessità che le procedure di prevenzione e il sistema dei controlli siano definiti, tenendo conto sia delle risorse umane che operano sui sistemi informatici (amministratori di sistema, utenti, sviluppatori ecc.), sia degli strumenti utilizzati (applicazioni acquisite o sviluppate, sistemi di sicurezza ecc.).

Per la corretta gestione del sistema informatico è necessaria l'adozione di misure, di sicurezza, per cui si può fare riferimento a quelle individuate dal Garante a tutela dei dati personali; in particolare si richiama la necessità di individuare di persone competenti, alla luce della valutazione dei rischi connessi con la gestione del sistema, attribuire compiti dettagliati, di tracciare le attività a rischio.

Per escludere la propria responsabilità l'ente deve dimostrare di avere adottato sistemi organizzativi tali da evitare la commissione di reati informatici e comunque consentire di individuare l'autore dei reati stessi. La soddisfazione di tali esigenze deriva dall'aver adottato misure organizzative e tecniche — quali l'individuazione di amministratori di sistema competenti, l'adozione di procedure certificate, la registrazione degli accessi

<sup>19</sup> Con riferimento alle norme applicative si veda il D.P.C.M. del 30 settembre 2009.

<sup>20</sup> D.Lgs. 231/01, novellato con L. 48/02, che ha dato attuazione alla Convenzione di Budapest sul cyber crime.

— richiamate anche nel provvedimento del Garante e procedure di sicurezza adeguate.

In questo caso la previsione di una struttura organizzativa che distingua tra amministratori e operatori del sistema informatico è funzionale alla predisposizione di un modello organizzativo efficace rispetto alla prevenzione dei reati informatici oltre che alla sicurezza dei dati, cioè a tutto vantaggio dell'ente.

## 6. REATI INFORMATICI E ABUSO DELLA QUALITÀ DI OPERATORE DI SISTEMA.

Diversi reati informatici contenuti nel Codice Penale prevedono l'aggravante e la procedibilità d'ufficio per i reati originariamente procedibili a querela di parte, ove il fatto sia commesso con abuso della qualità di operatore del sistema. Si tratta di reati contro la riservatezza dei dati e dei sistemi, reati di danneggiamento e frode informatica.

Il codice penale non definisce chi sia l'operatore di sistema, limitandosi ad affermare la sua più grave responsabilità, ove commetta un reato informatico con abuso della propria qualità.

Nei reati di accesso abusivo a sistema informatico e detenzione e diffusione abusiva di codici di accesso — che riguardano la violazione del domicilio informatico — è punito chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo (articolo 615-ter); e chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee a tale scopo (articolo 615-quater).

Nei reati di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche e installazione di apparecchiature a ciò dirette — che riguardano l'inviolabilità dei segreti — è punito chiunque: fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe, oppure rivela, mediante qualsiasi mezzo di informazione al pubblico il contenuto della comunicazione (articolo 617 quater); installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi (articolo 617-quinquies).

Nei reati di danneggiamento informatico, collocati tra i reati contro il patrimonio e modificati in esito alla legge 48 del 2008, da un lato si distingue tra il danneggiamento di dati, programmi e informazioni (artt. 635-bis e ter) e il danneggiamento dei sistemi informatici (artt. 635-quater e quinques), dall'altro si distingue il danneggiamento che riguarda soggetti privati da quello che riguarda soggetti pubblici, o dati o sistemi di pubblica utilità.

La frode informatica (art. 640-ter c.p.) si configura quando vi sia l'alterazione del funzionamento di un sistema informatico o telematico oppure in caso di intervento senza diritto, con qualunque modalità, su dati, informazioni o programmi contenuti in un sistema informatico o telematico, se da ciò deriva un profitto ingiusto per l'agente o per altri, con correlativo danno.

I reati informatici possono essere commessi da chiunque, indipendentemente dal fatto di avere qualifiche o svolgere mansioni particolari l'aggravante, invece, riguarda solo alcuni soggetti, definiti operatori del sistema. Il legislatore come anticipato non chiarisce chi sia l'operatore di sistema, per cui dottrina e giurisprudenza, nei pochi casi in cui sinora è stata chiamata a pronunciarsi, hanno individuato tale figura, evidenziandone a volte le caratteristiche tecniche, a volte le mansioni di responsabilità<sup>21</sup>.

Diversi aspetti caratterizzano l'aggravante: la capacità (tecnica) di intervenire sul sistema; il rapporto di fiducia esistente tra chi opera e il titolare del sistema, che determina l'affidamento della mansione (resta irrilevante che tale rapporto sia di dipendenza o di collaborazione); l'esistenza (conseguente) di un rapporto privilegiato con il sistema, tale da consentire di accedere con modalità preferenziali (il fatto di essere operatore di quel sistema). La *ratio* dell'introduzione dell'aggravante speciale dell'abuso della qualità di operatore del sistema appare dunque evidente: i reati informatici, che si realizzano mediante l'intervento sul sistema, appaiono particolarmente gravi se compiuti da chi si trova in una posizione privilegiata per intervenire abusivamente sui dati e sui programmi, in virtù delle capacità e della posizione che occupa. Infatti rispetto all'operatore del sistema, da un lato dati e sistemi sono più vulnerabili, dall'altro è maggiore il disvalore connesso alla violazione del dovere di fedeltà nei confronti sia del titolare (o comunque dell'utente) del sistema, sia di coloro i cui interessi (o i cui dati, anche personali) sono gestiti da quel sistema.

In quest'ottica pare, in primo luogo, evidente la sintonia con l'aggravante comune dell'abuso di relazioni d'ufficio o prestazione d'opera, prevista dal n. 11 dell'art. 61 del codice penale<sup>22</sup>, che si basa sul fatto che l'agente si trova nella condizione di potere più facilmente commettere il reato. Si è chiarito, al riguardo, che l'abuso di relazioni d'ufficio abbraccia, oltre all'ipotesi di un contratto di lavoro, tutti i rapporti giuridici che comportino l'obbligo di un *facere* e che instaurino, comunque, tra le parti un rapporto di fiducia dal quale possa essere agevolata la commissione del fatto. In questi termini, nel caso dell'operatore di sistema occorre che vi sia una condotta abusiva da parte di chi si trova in una particolare relazione con il sistema, in virtù di un rapporto giuridico apprezzabile tra le parti, che non si risolva in un rapporto meramente occasionale ed estemporaneo.

Per altro verso, ci si deve chiedere come si caratterizza la figura dell'operatore di sistema. Deve necessariamente essere un sistemista, un ammini-

<sup>21</sup> In giurisprudenza si è ritenuto che risponde del reato previsto dall'articolo 617-*quater* c.p. l'amministratore di sistema, responsabile dei servizi informatici, che installa un programma per l'intercettazione e la copia in una cartella separata di messaggi di posta elettronica destinati ad altri; in particolare «Non vi è dubbio che la posizione di amministratore di sistema — connessa alla qualità di responsabile dei servizi informatici — conferisce a chi ne sia investito la facoltà di accedere liberamente al sistema stesso, avvalendosi di tutti i privilegi (in senso informatico) che ne derivano, tra cui l'assegnazione delle password ai titolari dei diversi account e

la definizione dei privilegi spettanti a ciascuno. È altrettanto indubbio, peraltro, che una volta ottenuta l'assegnazione della propria password ognuno degli utenti abbia la libertà di sostituirla con altra, a tutela della propria riservatezza; e che l'amministratore di sistema non abbia alcun titolo, né mezzo lecito, per accedere alla casella di posta elettronica del singolo account e prendere conoscenza del suo contenuto» (Cass. Pen. V 31135/07). Cfr., inoltre, Cass. Pen. VI, n. 9755/09 per la nozione di manipolazione del sistema.

<sup>22</sup> In questo senso C. PARODI-A. CALICE, *Responsabilità penali in internet*, Ed. Il Sole 24 ore, Milano 2001, 69.

stratore o un operatore, o può essere un non-tecnico, che ha con il sistema un rapporto privilegiato tale da assumere iniziative che hanno effetti diretti sul sistema?

Non c'è dubbio che il sistemista che conosce il sistema ha la possibilità di aggirare le misure di sicurezza; può essere il depositario dei codici, o comunque può essere in grado di reperirli con facilità; si trova in una posizione privilegiata rispetto al posizionamento e all'uso di sistemi che interferiscono sui sistemi di comunicazione; può intervenire facilmente sui dati. In questo contesto non è rilevante che il sistemista svolga mansioni da amministratore o da operatore, ciò che rileva, giova ripeterlo, è che egli abbia la capacità e la possibilità di intervenire sul sistema. Vi sono però alcuni casi in cui anche un non tecnico può trovarsi nella possibilità di intervenire grazie al rapporto privilegiato che ha con il sistema: un esempio può essere individuato nel responsabile del sistema di protocollo informatico (cfr. *sub* 4).

Secondo alcuni<sup>23</sup> l'operatore di sistema deve essere inteso come quella particolare figura di tecnico informatico che, all'interno di un'azienda, ha il controllo delle diverse fasi del processo di elaborazione dei dati e quindi ha l'opportunità di inserirsi in tutti i settori interni del sistema, attraverso un canale di accesso riservato e privilegiato: in sostanza si tratta del *system administrator* come in precedenza individuato. In quest'ottica non potrà definirsi operatore di sistema, ai sensi e per gli effetti del codice penale, la persona (operatore, analista, data entry ecc.) che pur essendo abilitato a operare su dati e su programmi, disponga solo di una conoscenza limitata e settoriale del sistema o (nel caso, ad esempio, del data entry) svolga operazioni meramente esecutive o materiali.

Secondo altri<sup>24</sup>, invece, nella nozione di operatore di sistema devono essere compresi tutti i tecnici informatici, in quanto persone che comunque operano su un sistema informatico disponendo di una particolare qualifica professionale e competenza tecnica.

Per altri ancora<sup>25</sup>, infine, è operatore di sistema anche chi, pur non essendo un tecnico informatico, si trova comunque in una posizione privilegiata, di garanzia e tutela del sistema nel suo insieme.

Alla luce di quanto chiarito sotto il profilo tecnico, appare evidente che la posizione privilegiata rispetto alla possibilità di aggirare le misure di sicurezza poste a tutela del sistema informatico, di intervenire per installare strumenti che consentono l'intercettazione delle comunicazioni, di alterare in qualsiasi modo i dati deriva, in primo luogo, dal fatto di essere un esperto del sistema su cui si interviene: a nulla serve, infatti, ricoprire un incarico di responsabilità se per operare occorre avvalersi di terzi. Tale posizione privilegiata deriva, in secondo luogo, dal fatto di avere con il (titolare del) sistema un rapporto (rapporto di lavoro, contratto di

<sup>23</sup> C. PECORELLA, *Diritto penale dell'informatica*, ed. CEDAM, Padova 2006, 121. ss.; G. POMANTE, *Internet e criminalità*, Ed. Giappichelli, Torino, 1999, 11.

<sup>24</sup> BORRUSO, *La tutela del documento e dei dati*, in AA.VV., *Profili penali dell'informatica*, Milano, 1994; D'AIETTI, *La tutela dei programmi e dei sistemi informati-*

*ci*, in AA.VV., *Profili penali dell'informatica*, Milano, 1994.

<sup>25</sup> MUCCIARELLI, *Commento all'art. 4 della L. 547/93*, in *Legislazione penale*, 1996; PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Dir. Proc. Pen. Proc.*, 1997.



manutenzione o altro) che impone o consente di operare regolarmente sul sistema. In quest'ottica l'aggravante è dunque applicabile sia all'amministratore di sistema che all'operatore di sistema (anche se dispone di una conoscenza settoriale e limitata di sistema<sup>26</sup>), a seconda delle loro competenze, del rapporto privilegiato con il sistema, del rapporto di fiducia esistente con il titolare. L'aggravante non è invece applicabile al tecnico che sia entrato in contatto con il sistema occasionalmente, mancando in questo caso il rapporto privilegiato e la relazione di fiducia con il titolare.

Diversa è la posizione dell'utente, che non dispone dell'accesso al sistema ma solo agli applicativi. L'aggravante non si applica all'utente, che commetta un crimine informatico accedendo con le credenziali proprie o, abusivamente, con le credenziali altrui. Stando alle premesse, si può invece ritenere che l'aggravante si applichi in quelle situazioni in cui l'utente ha una posizione di responsabilità che gli consente di controllare e gestire il sistema (si pensi ad esempio al responsabile del sistema di protocollo informatico, che può annullare le registrazioni di protocollo o disporre di protocollare sul registro sostitutivo<sup>27</sup>).

In sintesi, per valutare la maggiore gravità della responsabilità nella commissione di reati informatici è del tutto indifferente che colui che ha commesso il reato abbia più o meno privilegi, o maggiore o minore responsabilità nel sistema; l'importante è che egli abbia capacità tecniche sufficienti e una relazione con il sistema tale da essere facilitato nella commissione del reato, così da commetterlo grazie alla (abusando della) propria posizione<sup>28</sup>.

## 7. UN PROBLEMA COMUNE: IL RISCHIO DEL CONTROLLO A DISTANZA DEL LAVORATORE.

Come si è visto, la tutela della privacy non è che uno degli aspetti da affrontare quando si vuole gestire con sicurezza i sistemi informatici. La so-

<sup>26</sup> Non è condivisibile C. PECORELLA, cit., 122, che ritiene applicabile l'aggravante solo agli amministratori di sistema, ritenendo che essi abbiano *un canale di accesso riservato e privilegiato*; in realtà si è chiarito come l'accesso privilegiato lo possano avere i sistemisti in generale e non solo gli amministratori, e Pomante, cit. 11, che ritiene che l'aggravante debba applicarsi soltanto all'amministratore del sistema — che è responsabile della gestione, manutenzione e sicurezza del sistema usato e, in tale veste, ha accesso all'intera base di dati e programmi, concede agli operatori le chiavi logiche di accesso, assegna i livelli di utenza, è responsabile della gestione, manutenzione e sicurezza del sistema stesso — e non all'operatore, che è titolare del solo permesso di accesso. Pomante, in particolare, afferma che in genere l'amministratore del sistema informatico, responsabile del funzionamento del sistema stesso, abilita gli utenti ad effettuare determinate ope-

razioni, sulla base dei compiti e delle responsabilità di ognuno all'interno dell'organizzazione aziendale, attraverso un sistema di account basato su password, gestito dal sistema operativo e accessibile solo all'amministratore stesso.

<sup>27</sup> In questo senso PARODI-CALICE, cit. 70, secondo cui è operatore di sistema anche chi, pur non essendo un tecnico dell'informatica, si trova comunque in una *condizione privilegiata, di garanzia a tutela del sistema nel suo insieme*.

<sup>28</sup> V.S. DESTITO-G. DEZZANI-C. SANTO-RIELLO, *Il diritto penale delle nuove tecnologie*, ed. CEDAM, Padova 2007, 89; *Diritto penale dell'informatica*, a cura di D. D'Agostini, Ed. EXPERTA, Forlì, 2007, 45, secondo cui il legislatore ha voluto punire in maniera più grave i soggetti che utilizzano la propria competenza tecnica o la conoscenza acquisita per compiere più agevolmente il reato, per cui è necessario valutare in concreto la qualità dell'agente.

luzione di alcune questioni sollevate dal provvedimento del Garante è invece rilevante anche sotto altri profili, in parte esaminati. In particolare, l'attenzione nella nomina degli amministratori di sistema e nella adozione di misure di sicurezza e la possibilità di ricostruire eventi accaduti a livello di sistema sono rilevanti anche per la tutela del patrimonio aziendale e per evitare agli enti di incorrere in sanzioni dovute a comportamenti illeciti degli operatori. D'altra parte, l'introduzione di sistemi di tracciamento e di verifica delle attività svolte dai sistemisti può essere contestata sotto il profilo del controllo a distanza del lavoratore.

Lo Statuto dei lavoratori, articolo 4, da un lato vieta in modo assoluto e inderogabile l'uso di impianti audiovisivi e di altre apparecchiature con finalità di controllo a distanza dell'attività dei lavoratori, dall'altro dispone che gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali o con la commissione interna o con l'intervento della Direzione provinciale del Lavoro.

Dunque lo Statuto dei lavoratori individua due fattispecie: un divieto assoluto e inderogabile di installazione e uso di apparecchiature esclusivamente destinate al controllo dell'attività dei lavoratori, sul presupposto che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada contenuta in una dimensione umana e cioè non esasperata dall'uso di tecnologie che possano renderla continua e anelastica, eliminando ogni zona di riservatezza di autonomia nello svolgimento del lavoro<sup>29</sup>; un divieto flessibile nel senso che, ricorrendo specifiche condizioni e limiti è possibile l'installazione e l'uso di apparecchiature che rispondono a esigenze produttive, organizzative o di sicurezza, che allo stesso tempo rendono possibile il controllo dell'attività dei lavoratori.

Le previsioni dell'articolo 4 evidenziano che il Legislatore non ha inteso circoscrivere il potere direttivo e la libertà di iniziativa economica privando, in assoluto, il datore di lavoro della possibilità di mantenere una memoria delle attività svolte: la distinzione tra le due situazioni dipende dal fatto che, nel primo caso, gli impianti audiovisivi e le apparecchiature sono finalizzate esclusivamente al controllo a distanza del lavoratore; nel secondo caso, invece, tali strumenti hanno la funzione di migliorare gli aspetti organizzativi, produttivi o di sicurezza dell'impresa e solo incidentalmente consentono il controllo dell'attività lavorativa.

Il controllo a distanza si riferisce alla possibilità di esaminare l'attività del lavoratore, contestualmente o in un secondo momento, mediante uno strumento che si sostituisce alla percezione diretta del controllore (quest'ultima sempre lecita anche se continua). Il divieto di controllo a distanza riguarda sia la qualità che la quantità della prestazione, sia le sue modalità di svolgimento. I primi orientamenti interpretativi sul punto, in un'epoca in cui la diffusione e l'uso dei sistemi informatici era ancora molto limitato,

---

<sup>29</sup> Cass. Lav. 8250/00, in *Guida al Lavoro*, n. 29/2000, p. 41.

erano estremamente rigorosi<sup>30</sup>. Di recente, invece, la giurisprudenza ha preso in considerazione le esigenze di sicurezza delle imprese, riconoscendo che l'uso di strumenti di « controllo difensivo » — tesi all'accertamento di eventuali condotte illecite da parte di dipendenti o alla dimostrazione della regolarità dei servizi offerti dall'impresa — non costituisce controllo a distanza e non è quindi soggetto agli oneri contemplati dall'articolo 4 dello Statuto dei lavoratori<sup>31</sup>.

Nella società dell'informazione e della comunicazione, dunque, il datore di lavoro appare legittimato a porre in essere strumenti di controllo a distanza sull'attività dei lavoratori, a difesa dell'azienda o di terzi (beni materiali e immateriali o diritti della persona costituzionalmente garantiti), ad esempio nella predisposizione di strumenti per prevenire situazioni di pericolo o accertare il compimento di crimini informatici o di atti illeciti compiuti dai lavoratori, rilevanti ai sensi delle norme sulla responsabilità amministrativa dell'impresa, delle norme a tutela dei dati personali o di altre norme.

In quest'ottica il controllo di carattere difensivo sull'attività di amministratori e operatori di sistema che non consenta (neppure potenzialmente) la verifica della correttezza e del puntuale adempimento delle obbligazioni inerenti il rapporto di lavoro non rientra in alcun modo nell'ambito di operatività dell'articolo 4 dello statuto dei lavoratori.

## 8. CONCLUSIONI.

Alla luce dalle considerazioni che precedono si deve riconoscere che il provvedimento del Garante sugli amministratori di sistema ha il pregio di sottolineare l'importanza e la delicatezza del ruolo assunto dai tecnici informatici e di richiamare l'attenzione sulla necessità di valutare l'attribuzione di tale ruolo e la gestione delle attività. Adeguarsi agli adempi-

<sup>30</sup> Si è affermato infatti che: « l'installazione di una apparecchiatura elettronica, che registri le operazioni effettuate da un operatore individuato dal suo codice e che consenta di effettuare una analisi di tali dati, viola il disposto del comma 1 dell'art. 4 statuto dei lavoratori [...]. È vietato installare uno strumento elettronico che permetta di verificare a distanza e in tempo reale se un dipendente sta o meno operando », Pretura Milano, 21 dicembre 1984, Riv. Giur. Lav. 1985, IV, 209; « a norma dell'art. 4 dello Statuto dei Lavoratori, deve ritenersi illegittimo il sistema dei controlli in cuffia effettuati nei confronti dei centralisti telefonici, perché vessatori e contrari al diritto alla privacy che deve ritenersi uno degli interessi primari della collettività », Pretura Milano, 12 maggio 1972, in Orient. Giur. Lav. 1972, 260.

<sup>31</sup> « Il controllo a distanza dell'attività

dei lavoratori cui si riferisce il divieto ex art. 4 legge 300/70 è cosa diversa dall'utilizzo di strumenti cosiddetti di "controllo difensivo" tesi all'accertamento di eventuali condotte illecite da parte dei propri dipendenti, ovvero, in caso di contestazioni da parte degli utenti, a provare la regolarità del servizio offerto dalla impresa » Tribunale di Milano, 5 luglio 2006, in Orient. Giur. Lav. 2006, 3, 611; « il controllo a distanza sull'attività dei lavoratori, di carattere difensivo, in quanto diretto ad accertare comportamenti illeciti, non è soggetto agli oneri contemplati dall'art. 4 dello statuto dei lavoratori, solo se questo controllo è diretto alla tutela di beni estranei al rapporto di lavoro. Trova invece applicazione detto articolo se il controllo difensivo tende ad accertare l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro » Cass. Civ. sez. lav., n. 15892/2007.

menti previsti può essere utile non solo per essere « privacy compliant », ma anche per tutelare i dati e i sistemi nel loro complesso.

Correttamente, in quest'ottica, il provvedimento richiede al titolare e al responsabile del trattamento di valutare con attenzione l'attribuzione dei ruoli e l'assegnazione dei compiti, nonché di valutare sotto il profilo tecnico e professionale le persone designate alla gestione dei sistemi e degli archivi informatici. Il provvedimento inoltre deve essere valutato in un contesto più ampio, insieme ai provvedimenti sulla sicurezza informatica e sulla gestione della posta elettronica e di internet sul luogo di lavoro<sup>32</sup>.

Tuttavia alcuni adempimenti destano perplessità e non appaiono funzionali per raggiungere gli obiettivi proposti.

In primo luogo desta perplessità l'estensione della nozione di amministratore di sistema anche a figure che svolgono incarichi di operatore, per il solo fatto che in concreto hanno la possibilità di accedere a dati personali, senza porsi il problema del ruolo effettivamente svolto, cioè senza valutare se essi abbiano o meno la responsabilità rispetto alla gestione del sistema. Il fatto di distribuire le responsabilità su un ampio gruppo di persone rischia di limitare, se non addirittura escludere, la responsabilità organizzativa e gestionale che spetta a coloro che effettivamente amministrano il sistema.

Al contrario, per ottenere un'effettiva assunzione di responsabilità, è opportuno distinguere tra chi svolge un'attività (gli operatori) e chi, conoscendo il dominio applicativo, è responsabile di come è organizzato il lavoro (gli amministratori) e ha il compito di coordinare e controllare le attività. Giova ribadire al riguardo che il solo fatto di accedere con l'account di *root* non trasforma un operatore in amministratore di sistema.

A tale scopo la distinzione tra amministratori e operatori può essere recepita nell'attribuzione di incarichi per il trattamento dei dati personali individuando, ai sensi del Codice della privacy, gli amministratori quali responsabili *ex art. 29* e gli operatori quali incaricati *ex art. 30*. È d'altra parte evidente che il fatto di essere semplice incaricato del trattamento non vale ad escludere la responsabilità personale dell'operatore (sotto il profilo disciplinare, civile o penale) che abbia disatteso le direttive impartite dal responsabile o abbia violato regolamenti o norme di legge, in particolare quelli posti a tutela della riservatezza e sicurezza dei dati personali. L'individuazione di responsabilità in base alle mansioni svolte, per altro verso, consente anche di evitare rivendicazioni, sul piano lavoristico, da parte degli operatori.

La distinzione tra gli amministratori-responsabili e gli operatori-incaricati consente infine di ottemperare con maggiore semplicità ed efficacia agli adempimenti previsti dal provvedimento. Infatti la nomina quale responsabile ai sensi dell'art. 29 prevede per legge: la valutazione delle caratteristiche soggettive al momento dell'attribuzione delle funzioni, anche sotto il profilo del rispetto delle norme in materia di trattamento

<sup>32</sup> Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali, provvedimento del 13 ottobre 2008, pubblicato in *G.U.* n. 287 del 9

dicembre 2008; Linee guida per l'uso della posta elettronica e di internet sul luogo di lavoro, provvedimento del 1 marzo 2007, pubblicato in *G.U.* n. 58 del 10 marzo 2007.

dei dati personali; la designazione individuale e l'indicazione analitica, per iscritto, dei compiti affidati dal titolare; la verifica periodica sulla conformità dell'attività svolta alle istruzioni impartite dal titolare; la conoscibilità dei responsabili da parte degli interessati. Per quanto riguarda gli operatori, la valutazione delle loro capacità e la verifica sulla correttezza del loro operato dovrebbe essere demandata agli amministratori.

Ancora, la richiesta di designazione individuale e indicazione dettagliata delle attività svolte come incaricati del trattamento appare poco funzionale e ridondante, anche a fronte di quanto previsto dall'Allegato B in materia di misure di sicurezza, che alla regola 15 prevede la possibilità dell'individuazione preliminare dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici e la redazione della lista degli incaricati, e dei relativi profili di autorizzazione, anche per classi omogenee di incarico.

Per quanto riguarda gli ulteriori adempimenti, non si comprende la previsione che i dati degli incaricati siano resi pubblici, all'interno dell'ente, a tutti i dipendenti dato che si tratta di una disposizione che non ha riscontro nel testo normativo per nessun'altra situazione, anche in caso di trattamento di dati sensibili. Al contrario, l'informativa ex art. 13 impone di comunicare all'interessato soltanto i nominativi del titolare e del responsabile, o dei responsabili, del trattamento, proprio perché ad essi ci si deve rivolgere per qualunque istanza connessa al trattamento.

Ben venga, invece, la registrazione degli accessi al sistema e la conservazione dei relativi dati, al fine di verificare, se necessario, se siano stati compiuti atti illeciti, risalire all'autore di tali atti e ripristinare i dati; al riguardo è appena il caso di ricordare che la valida ricostruzione delle attività dipende, in primo luogo, dall'organizzazione. Resta comunque aperta la questione dei tempi di conservazione dei dati relativi agli accessi per un periodo « congruo » non inferiore a sei mesi, poiché non essendo individuato alcun parametro di riferimento, rischia di trasformarsi in una conservazione *sine die* o effettuata in base a valutazioni discrezionali.

Le considerazioni esposte valgono a maggior ragione nel caso di servizi di amministrazione di sistema affidati in *outsourcing*. Il titolare del trattamento dovrà farsi carico di precisare nel contratto gli obblighi posti a carico dell'affidatario del servizio, richiedendo, e conservando gli estremi identificativi delle persone fisiche responsabili dell'amministrazione del sistema, sarà poi onere di questi ultimi organizzare le attività in conformità con le prescrizioni in materia di tutela dei dati personali.

Infine, si ritiene che l'esigenza di semplificazione delle procedure, invocata da più parti, non può portare a diminuire il livello di sicurezza nella gestione dei sistemi informatici, che — come si è evidenziato — è indispensabile a tutela di diversi interessi. Ciò anche in quei casi che sono stati oggetto di misure di semplificazione, in relazione al trattamento dei dati personali per ragioni amministrativo-contabili. Imporre una valida organizzazione delle attività, distribuendo adeguatamente i compiti e le responsabilità, comporta la semplificazione delle procedure e, conseguentemente consente, anche limitando i casi di esclusione dall'ambito di applicazione del provvedimento, il protrarsi di quelle situazioni di scarsa consapevolezza delle criticità e di sottovalutazione dei rischi connessi alla gestione dei sistemi informativi che è stata rilevata e sottolineata dal Garante per la protezione dei dati personali.

In conclusione è auspicabile che il provvedimento del Garante sia l'occasione per promuovere una cultura della sicurezza informatica ad ampio raggio, fornendo lo spunto per studiare linee guida tecniche e organizzative, di cui il Garante stesso potrebbe farsi promotore<sup>33</sup>.

---

<sup>33</sup> Si richiamano, in particolare, l'art. 36 del Codice privacy, che prevede l'aggiornamento dell'All. B a cura del Ministero della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore, e l'art. 71 del

Codice dell'Amministrazione Digitale, che prevede l'adeguamento delle regole tecniche a cura del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate.