

Il provvedimento sugli amministratori di sistema e il commento alle FAQ

Autore: Gabriele Faggioli



Clusit
Education

Il provvedimento del Garante sugli amministratori di sistema

- L'attività regolamentare del Garante ha da ultimo interessato un aspetto molto importante rispetto alla sicurezza informatica aziendale attraverso la previsione di alcune regole concernenti l'attività di amministratore di sistema.
- Con il provvedimento del 27 novembre 2008 (pubblicato sulla Gazzetta Ufficiale lo scorso 24 dicembre) il Garante ha infatti prescritto specifiche misure ed accorgimenti ai titolari dei trattamenti (es. aziende) *“effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*.
- In realtà il provvedimento non riguarda esclusivamente l'attività degli amministratori di sistema intesi tradizionalmente quali **soggetti che svolgono funzioni di gestione e manutenzione dei sistemi informatici** ma anche ad **altre categorie di figure professionali quali gli amministratori di banche dati, di reti e apparati di sicurezza e di sistemi di software complessi**, le cui attività possono comunque in determinati casi comportare dei rischi per la protezione dei dati personali.

Il provvedimento del Garante sugli amministratori di sistema

- Il Garante nel provvedimento ha in primo luogo specificato le ragioni che hanno reso necessaria la previsione di accorgimenti specifici per tali categorie professionali
- Viene in particolare rilevato che le attività di carattere tecnico svolte dagli amministratori di sistema, nell'ampia accezione sopra richiamata (es. backup dei dati, gestione dei supporti di memorizzazione, manutenzione dell'hardware), possono influire sulle informazioni conservate dall'azienda e le stesse attività, in queste circostanze, devono essere qualificate quali trattamenti di dati personali ai sensi del d.lgs 196/2003, cioè *"anche quando l'amministratore non consulti in chiaro le informazioni medesime"*.
- La delicatezza del ruolo di questa figura professionale è ulteriormente dimostrata, si legge nel provvedimento, dal fatto che il nostro legislatore in relazione ad alcune fattispecie di reato informatico (es. accesso abusivo a sistema informatico, frode informatica, danneggiamento di informazioni, dati e programmi informatici) ha previsto specifiche aggravanti in caso di loro commissione con abuso della qualità di amministratore di sistema.

Il provvedimento del Garante sugli amministratori di sistema

- Ai sensi dell'art. 154, comma 1, lett. c) del Codice il Garante ha quindi prescritto l'adozione delle misure enunciate ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed **effettuati con strumenti elettronici**, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), **salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili** che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (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*):
- Quali sono i trattamenti fuori ambito:
 - ◆ Nel provvedimento del 19 giugno 2008 il Garante per la protezione dei dati personali ha emanato un provvedimento contenente “**Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili**” dove si legge: “*Diverse realtà, specie imprenditoriali di piccole e medie dimensioni, trattano dati, anche in relazione a obblighi contrattuali, precontrattuali o di legge, esclusivamente per finalità di ordine amministrativo e contabile (gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti); omississ”*”

Il provvedimento del Garante sugli amministratori di sistema

- **a. Valutazione delle caratteristiche soggettive**
L'attribuzione delle funzioni di amministratore di sistema deve avvenire **previa valutazione delle caratteristiche di esperienza, capacità e affidabilità** del soggetto designato, **il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento**, ivi compreso il profilo relativo alla sicurezza.
- Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

Il provvedimento del Garante sugli amministratori di sistema

- ***b. Designazioni individuali***

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

Il provvedimento del Garante sugli amministratori di sistema

- **c. Elenco degli amministratori di sistema**
Gli **estremi identificativi** delle persone fisiche amministratori di sistema, con **l'elenco delle funzioni ad essi attribuite**, devono essere **riportati nel documento programmatico sulla sicurezza** oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.
- 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 dei lavoratori**, i titolari pubblici e privati **sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni**, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.
- Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (*ad es.*, *intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

Il provvedimento del Garante sugli amministratori di sistema

- ***Quali sono i nuovi obblighi***

- ***d. Servizi in outsourcing***

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

Il provvedimento del Garante sugli amministratori di sistema

- ***e. Verifica delle attività***

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Il provvedimento del Garante sugli amministratori di sistema

■ *f. Registrazione degli accessi*

Devono essere adottati **sistemi idonei alla registrazione degli accessi logici** (autenticazione informatica) **ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.**

- Le registrazioni (*access log*) devono avere **caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità** adeguate al raggiungimento dello scopo per cui sono richieste.
- Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il provvedimento del Garante sugli amministratori di sistema

- A quali trattamenti si applica il provvedimento?
 - ◆ Il Provvedimento non si applica ai trattamenti di dati personali effettuati per finalità amministrativo contabile
 - 2. ai sensi dell'art. 154, comma 1, lett. c) del Codice **prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice** ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), **salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili** che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (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)

Il provvedimento del Garante sugli amministratori di sistema

- **A quali trattamenti si applica il provvedimento?**
 - ◆ **FAQ 6:** Sono esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).
 - ◆ Provvedimento del 19 giugno 2008 “*Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili*” che definisce come tali in via esemplificativa la **gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti.**

Il provvedimento del Garante sugli amministratori di sistema

- **A quali trattamenti si applica il provvedimento?**
 - ◆ **FAQ 24: Si possono ritenere esclusi i trattamenti relativi all'ordinaria attività di supporto delle aziende, che non riguardino dati sensibili, giudiziari o di traffico telefonico/telematico? Ci si riferisce ai trattamenti con strumenti elettronici finalizzati, ad esempio, alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali ecc...)**

Tali trattamenti possono considerarsi compresi tra quelli svolti per ordinarie finalità amministrativo-contabili e, come tali, esclusi dall'ambito applicativo del provvedimento.

Il provvedimento del Garante sugli amministratori di sistema

■ Chi sono gli amministratori di sistema?

- ◆ In realtà il provvedimento non riguarda esclusivamente l'attività degli amministratori di sistema intesi tradizionalmente quali **soggetti che svolgono funzioni di gestione e manutenzione dei sistemi informatici** ma anche ad altre categorie di figure professionali quali gli **amministratori di banche dati, di reti e apparati di sicurezza e di sistemi di software complessi**, le cui attività possono comunque in determinati casi comportare dei rischi per la protezione dei dati personali.

Il provvedimento del Garante sugli amministratori di sistema

■ Chi sono gli amministratori di sistema?

- ◆ **FAQ 1.** In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale **figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali**, compresi i sistemi di **gestione delle basi di dati**, i **sistemi software complessi quali i sistemi ERP** (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati i personali.
- ◆ 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.
- ◆ Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

Il provvedimento del Garante sugli amministratori di sistema

- **Quali caratteristiche devono avere gli amministratori di sistema?**
 - ◆ **Lettera a) Provvedimento.** L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di **esperienza, capacità e affidabilità** del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
 - ◆ Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.
 - ◆ **FAQ 20.** Il riferimento alle caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo, è all'esperienza, alla capacità e all'affidabilità del soggetto *designato*. **Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali.**

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono gli adempimenti da effettuare nella individuazione degli amministratori di sistema?
 - ◆ **Lettera b) Provvedimento.** La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
 - ◆ **FAQ 7.** Il provvedimento prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento.
 - ◆ **FAQ 8.** E' sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.

Il provvedimento del Garante sugli amministratori di sistema

- **Come devono essere gestiti gli adempimenti inerenti l'elencazione e la conoscibilità degli amministratori di sistema?**
 - ◆ **Lettera c) Provvedimento.** Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati ~~nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque~~ in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Il provvedimento del Garante sugli amministratori di sistema

- **Come devono essere gestiti gli adempimenti inerenti l'elencazione e la conoscibilità degli amministratori di sistema?**
 - ◆ **Lettera c) Provvedimento.** 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 dei lavoratori**, i titolari pubblici e privati **sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.** Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 o, in alternativa, mediante altri strumenti di comunicazione interna (*ad es., intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

Il provvedimento del Garante sugli amministratori di sistema

- **Come devono essere gestiti gli adempimenti inerenti l'elencazione e la conoscibilità degli amministratori di sistema?**
 - ◆ **FAQ 18.** Il regime di conoscibilità degli amministratori di sistema è da intendersi per i soli trattamenti inerenti i dati del personale e dei lavoratori.
 - ◆ **FAQ 21.** Gli "estremi identificativi" degli amministratori di sistema sono il minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.

Il provvedimento del Garante sugli amministratori di sistema

- **Come devono essere gestite le relazioni con gli outsourcer e quali sono gli obblighi in carico agli stessi?**
 - ◆ **Lettera d) Provvedimento.** Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* ~~il titolare deve~~ il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.
 - ◆ **FAQ 23.** (Si chiede se sia necessario conformarsi al provvedimento nel caso della fornitura di servizi di gestione sistemistica a clienti esteri (*housing, hosting, gestione applicativa, archiviazione remota...*) da parte di una società italiana non titolare dei dati gestiti). **Il provvedimento si rivolge solo ai titolari di trattamento.** I casi esemplificati prefigurano al più una responsabilità di trattamento (secondo il Codice italiano), e sono quindi esclusi dall'ambito applicativo del provvedimento.

Il provvedimento del Garante sugli amministratori di sistema

- **Quali verifiche periodiche occorre fare almeno annualmente?**
 - ◆ **Lettera e) Provvedimento.** L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari **o dei responsabili** del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.
 - ◆ **FAQ 5.** E' da sottoporre a verifica l'attività svolta dall'amministratore di sistema nell'esercizio delle sue funzioni. Va verificato che le attività svolte dall'amministratore di sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.
 - ◆ **FAQ 14.** Gli scopi di verifica sono quelli descritti al paragrafo 4.4 del provvedimento e ribaditi al punto 2, lettera e). L'adeguatezza è da valutare in rapporto alle condizioni organizzative e operative dell'organizzazione.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **Lettera f) Provvedimento.** Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 4.** Anche i client, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS.
 - ◆ Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.
 - ◆ Sarà comunque con valutazione del titolare che dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei log centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 9.** Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.
 - ◆ Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato...).

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 10.** Qualora il sistema di *log* adottato generi una raccolta dati più ampia, comunque non in contrasto con le disposizioni del Codice e con i principi della protezione dei dati personali, il requisito del provvedimento è certamente soddisfatto.
 - ◆ Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei *logfile* al fine di selezionare i soli dati pertinenti agli AdS.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 11.** La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di *log*, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai *log* qui richiesti.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ FAQ 12. Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di *log* sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito *software*. Il requisito può essere ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati".
 - ◆ E' ben noto che il problema dell'attendibilità dei dati di *audit*, in genere, riguarda in primo luogo la effettiva generazione degli *auditable events* e, successivamente, la loro corretta registrazione e manutenzione. Tuttavia il provvedimento del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del *log* degli "accessi" (*log-in*) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli *usage data* dei sistemi informativi.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 13.** Non sono previsti livelli di robustezza specifici per la garanzia della integrità. La valutazione è lasciata al titolare, in base al contesto operativo (cfr. faq n. 14).
 - ◆ **FAQ 15.** Il provvedimento non chiede in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema.
 - ◆ **FAQ 22.** L'accesso a livello applicativo non rientra nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati. L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del provvedimento del Garante, sottoporlo a registrazione.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?
 - ◆ **FAQ 19.** Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei *data base management systems* (DBMS), che vanno registrate.

Il provvedimento del Garante sugli amministratori di sistema

- Quali sono le finalità perseguibili nel controllo dei log?
 - ◆ **FAQ 16.** La raccolta dei *log* serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso...). L'analisi dei *log* può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

Alcuni profili di criticità

■ L'articolo 4 dello Statuto dei Lavoratori

- ◆ E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori
- ◆ 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, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro provvede la Direzione Regionale del Lavoro omississ

Alcuni profili di criticità

■ L'articolo 4 dello Statuto dei Lavoratori

- ◆ La giurisprudenza (Cassazione civile , sez. lav., 06 marzo 1986, n. 1490) ha ulteriormente chiarito che il divieto posto dall'art. 4 st. lav. per il datore di lavoro di far uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori non è escluso:
 - né dalla circostanza che tali apparecchiature siano state solo installate ma non siano ancora funzionanti
 - né dall'eventuale preavviso dato ai lavoratori, i quali quindi siano avvertiti del controllo suddetto
 - né infine del fatto che tale controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente

Alcuni profili di criticità

■ La giurisprudenza in materia di controlli difensivi

- ◆ Secondo l'orientamento giurisprudenziale prevalente (anche se più risalente nel tempo) i controlli difensivi rientrerebbero nell'applicazione dell'articolo 4 comma 2 St. Lav:
 - La Corte di Cassazione ha ritenuto illegittima l'installazione di alcuni impianti audiovisivi destinati al controllo dell'uso e della conservazione dei cartellini segna-orario sistemati in apposite custodie all'ingresso dello stabilimento senza che il datore di lavoro avesse ottenuto, come alternativamente richiesto, nè il consenso dei sindacati, nè l'autorizzazione dell'ufficio del lavoro (Cassazione civile, sez. lav., 06 marzo 1986, n. 1490)
 - La Corte di Appello di Milano (sentenza 688/2005) ha recentemente confermato questo orientamento rilevando che l'installazione di strumenti che consentono il controllo elettronico centralizzato deve avvenire nel rispetto delle procedura di cui dell'articolo 4 comma 2 St. Lav. (a nulla rilevando che i dati siano utilizzati per finalità di carattere difensivo)

Alcuni profili di criticità

■ La giurisprudenza in materia di controlli difensivi

- ◆ Secondo un orientamento giurisprudenziale minoritario i controlli difensivi non rientrerebbero invece nell'applicazione dell'articolo 4 comma 2 St. Lav. Una sentenza della Corte di Cassazione (Cassazione civile , sez. lav., 03 aprile 2002, n. 4746 ha stabilito per esempio che:
 - Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate
- ◆ Il Tribunale Milano, con sentenza del 31 marzo 2004 ha confermato che:
 - “Il divieto del controllo a distanza dell'attività dei lavoratori posto dall'art. 4 st. lav. non si estende ai cosiddetti controlli difensivi, i quali, peraltro, non costituiscono una categoria a sè esentata, a priori, dall'applicabilità delle previsioni dell'art. 4, ma semplicemente un modo per definire controlli finalizzati all'accertamento di condotte illecite del lavoratore che non rientrano nell'ambito di applicazione del divieto perché non comportano la raccolta anche di notizie relative all'attività lavorativa”

Alcuni profili di criticità

■ La giurisprudenza in materia di controlli difensivi

- ◆ Recentemente il Tribunale di Perugia ha confermato la legittimità dei controlli relativi alle connessioni ad internet di un dipendente (analisi dei file di log) posti in essere senza attivazione della procedura di cui dell'articolo 4 comma 2 St. Lav.
- ◆ Il Tribunale, in particolare conformandosi all'orientamento minoritario a cui si è accennato prima (Cass. Civ. n.4746 del 3 aprile 2002) ha ritenuto che l'analisi dei file di log relativi alla navigazione possa rientrare non già in una forma diretta o indiretta di verifica dell'attività lavorativa, ma si sostanziasse in un cd. "controllo difensivo", volto ad accertare le condotte illecite dei lavoratori”

Sanzioni

- Il provvedimento del Garante è stato adottato ai sensi dell'art. dell'art. 154, comma 1, lett. c) del Codice.
- L'art. 162 comma 2 ter (inserito dall'articolo 44, comma 3, lettera c), del D.L. 30 dicembre 2008, n. 207) prevede che: “In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro”.
- In pratica questa nuova disposizione diviene applicabile in caso di violazione di tutti i provvedimenti generali del Garante adottati ai sensi dell'art. 154 comma 1 lett. c) del Codice.

Grazie per l'attenzione!

gabriele.faggioli@islconsulting.it