PEGASO

Università Telematica

"QUADRO DI RIFERIMENTO NORMATIVO"

PROF. PASQUALE DE ROSA

Indice

1 Introduzione

In Italia, come tutti ben sanno, ci sono una pletora di leggi e tra queste vi sono alcune che parlano delle figure tecniche degli amministratori di rete e degli amministratori di sistema. Come si può immaginare sono leggi abbastanza moderne poiché moderna è la coscienza del legislatore che ha oggi un' occhio diverso verso l'informatica e l'informazione, e con queste leggi su chi amministra l'informazione.

2 Le leggi

Nascono dall'esigenza di regolamentare la figura dell'amministratore di sistema in seno alle leggi sulla tutela della privacy. La figura in esame deriva dal termine **"system administrator",** espressione che in Italia ingloba una varietà di figure relative ai sistemi informativi digitali.

3 Le Regole

Non meno importanti sono le regole inerenti l'uso possibile dei dati personali per finalità di ricerca scientifica e di sperimentazione, regolamentati nel corso del 2007 da due importanti provvedimenti dall'autorità Garante della Privacy: l'autorizzazione per il trattamento dei dati genetici e linee guida per i trattamenti di dati nell'ambito delle sperimentazioni cliniche di medicinali.

Infine, poiché le informazioni sanitarie sono trattate dai sistemi informatici aziendali la cui responsabilità è affidata all'Amministratore di Sistema, ad essi è riferita la regolamentazione emessa dal Garante nel 2008 che ne disciplina il comportamento per tutelare il trattamento sicuro dei dati sanitari.

Le strutture sanitarie in qualità di strutture pubbliche entro il 31 Marzo di ogni anno devono rielaborare le proprie metodologie di sicurezza interna e procedere all'aggiornamento del Documento Programmatico sulla Sicurezza (DPS), che descriveremo in seguito, dove sono esplicitate e recepite le linee guida emesse dal Garante e gli adeguamenti al provvedimento sugli Amministratori di Sistema.

4 Il fascicolo sanitario elettronico o cartella clinica digitale

Oltre alla compilazione online del fascicolo sanitario elettronico o cartella clinica digitale, offerta dai nuovi sistemi informatici, le strutture sanitarie devono anche occuparsi della dematerializzazione dei vecchi documenti sanitari, ovvero la digitalizzazione di ciò che era stato prodotto su carta per i quali devono rispettare, oltre alle linee guida del garante sopraccitate, le due normative Codice dell'Amministrazione digitale (D.Lgs. n.82 del 2005 – CAD) e nella Deliberazione CNIPA (ora DigitPA) n.11 del 19 febbraio 2004.

5 La Normativa

Legge n. 675 del 31 dicembre 1996 *(Abrogata dal 1/1/2004 ex d.lgs. 196/2003)*

Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (testo consolidato con il d. lg. 28 dicembre 2001, n. 467)

È la prima a parlare di trattamento dei dati personali, non annoverava, direttamente, tale tipologia di ruolo. Solo con integrazioni successive si è presa coscienza della figura dell'amministratore di sistema.

6 Decreto del Presidente della Repubblica 28 luglio 1999, n.318

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675 (Pubblicato sulla GU n. 216 del 14-9-1999) - *(Abrogato dal 1/1/2004 ex d.lgs. 196/2003)*

Il D.P.R. n. 318/1999 abrogato, nell' art. 1, comma 1, lett. c ha fornito una prima definizione imponendo quale Amministratore di sistema, quel "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentire l'utilizzazione".

7 Decreto legislativo 30 giugno 2003, n. 196 - Codice della Privacy

(CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

Il Codice del 2003 ha, invece, operato una scelta di tipo diverso rispetto alla disciplina precedente.

Il suo Allegato B ("Disciplinare tecnico in materia di misure minime di sicurezza") ha tralasciato quella figura, preferendo precisare, per l'organizzazione per la privacy, solo le tre generiche tipologie di soggetti (titolare, responsabile ed incaricato di trattamento).

- Il documento *in cui effettivamente si cita* ***l'amministratore di sistema*** *è un provvedimento del Garante della Privacy datato 27 Novembre 2008 dal titolo* ***"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*** *ha due caratteristiche**:***

- ***di essere documento "divulgativo***" (ai sensi dell'art. 154, comma 1, lett. h, del decreto n. 196/2003) in relazione al compito gravante sull'Autorità di promuovere la "conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati";

- ***di essere testo prescrittivo*** (in virtù dell'art. 154, comma 1, lett. c, del vigente Decreto sui dati personali) data la facoltà di prescrivere misure ed accorgimenti, specifici o di carattere generale, rivolti ai titolari di trattamento.

Entrando più nel dettaglio ha due scopi:

- ***richiamare*** tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti

elettronici sulla necessità di prestare la massima attenzione su rischi e su criticità implicite nell'affidamento degli incarichi di amministratore di sistema;

- ***individuare delle prime misure di carattere organizzativo*** atte a rendere più agevole la conoscenza sugli Amministratori di sistema, in termini di esistenza dei loro ruoli, delle loro responsabilità e, in taluni casi, dell'identità dei soggetti che svolgono tale lavoro.

Misure volte a sensibilizzare i titolari, veri destinatari del documento in parola, ad evitare una "preoccupante sottovalutazione dei rischi derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico", poiché l'amministratore di sistema, dice il Garante, ha "di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti".

8 Elementi importanti

Possiamo riassumere alcuni elementi importanti riguardo la figura dell'amministratore di sistema:

1. Sono incluse nelle normative citate sia gli amministratori di sistema che gli amministratori di rete di data base o i relativi manutentori.

2. Gli amministratori di sistema devono conservare per almeno 6 mesi gli access log (i log di accesso) in archivi di cui non sia possibile la modifica e l'alterazione.

   Chiara conseguenza di questo punto è che debbano essere adottati sistemi idonei alla registrazione di questi accessi ai sistemi di elaborazione o agli archivi da parte delle figure amministratrici di sistema e cosa rilevante, questi log devono avere specifiche caratteristiche di completezza (dati temporali certi e descrizione completa dell'evento generatore) e verifica dell'integrità, inoltre devono essere conservati per un periodo minimo di mesi 6, elemento che fa nascere processi di conservazione digitale attualmente ben delineati in ulteriori leggi.

3. I titolari dei dati devono rendere nota la presenza della figura dell'amministratore di sistema, indicando con chiarezza la persona fisica che ricopre questa veste sebbene non sia incaricata o responsabile del trattamento dei dati personali.

   La figura deve essere presente quindi nel DPS (Documento Programmatico per la Sicurezza), deve essere attuato anche in caso dell'outsourcing del servizio e/o sistema. Nella fattispecie il titolare ha l'obbligo di conservare gli estremi identificativi di tali figure.

4. Per i titolari del trattamento è prevista una verifica annuale sull'operato dell'amministratore di sistema.

5. Rivestire la funzione di amministratore di sistema costituisce un'aggravante per determinati reati del codice penale

9 Informazioni sanitarie

Il Garante della Privacy ha voluto regolamentare le informazioni sanitarie specificando le garanzie, responsabilità e diritti sulla condivisione, gestione e trattamento delle informazioni sanitarie da parte di distinti titolari (strutture mediche), ed ha emesso l'**Autorizzazione n. 1/1997 al trattamento dei dati sensibili nei rapporti di lavoro** riconosce espressamente il diritto alla protezione dei dati personali e il tradizionale diritto della riservatezza, per il quale gli esercenti le professioni sanitarie e gli impiegati pubblici sono tenuti rispettivamente al segreto professionale e al segreto d'ufficio; in ambito sanitario e socio-assistenziale è necessario rispettare la disciplina rilevante di settore, quale ad esempio la legge in materia di HIV, procreazione assistita, interruzione volontaria della gravidanza ecc.

10 Deliberazione CNIPA (ora DigitPA) n.11 del 19 febbraio 2004. Codice dell'amministrazione digitale 1

La deliberazione rappresenta le Linee Guida per la dematerializzazione della documentazione clinica in Laboratorio e in Diagnostica per Immagini.

garantire la conformità dei documenti agli originali - articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, **di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. 1** (Deliberazione n. 11/2004).

---

1 Centro Nazionale per l'Informatica nella Pubblica Amministrazione è stato trasformato in DigitPA - Ente nazionale per la digitalizzazione della pubblica amministrazione.
Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a

11 Decreto legislativo 7 marzo 2005, n. 82 – CAD (Codice dell'amministrazione digitale)

Ultimo aggiornamento: 06/11/2012 redatto al solo fine di facilitare la lettura del Codice dell' amministrazione digitale a seguito delle modifiche ed integrazioni introdotte dal decreto legge 22 giugno 2012 n. 83 e 6 luglio 2012 n 95 (convertiti con modificazioni, rispettivamente, dalla L. 7 agosto 2012, n. 134 e L. 7 agosto 2012, n. 135).

12 Amministratore di sistema

Provv. Garante delle Privacy 27/11/2008: "Misure ed accorgimenti effettuati con strumenti elettronici prescritti ai titolari dei trattamenti, relativi alle attribuzioni di ADS"

Garante della Privacy ha imposto che gli Amministratori di Sistema siano persone preparate:

".....L'attribuzione delle funzioni deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato"

Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 12 febbraio 2009 (G.U. n. 45 del 24 febbraio 2009)

Sistema di deleghe

Con il comunicato stampa del 14.01.2009, il Garante della Privacy ha richiamato l'attenzione sul ruolo degli amministratori di sistema, ponendo un termine di quattro mesi per mettere in atto specifiche misure e cautele che consentiranno di poter vigilare sul loro operato. Pare legittimo che, come il responsabile del trattamento e gli incaricati al trattamento di dati personali siano chiamati a rispondere al titolare del trattamento circa il diligente assolvimento delle loro responsabilità, anche l'amministratore di sistema sia tenuto a fare altrettanto.

La curiosità è che, mentre "responsabile" e "incaricato" sono due figure espressamente previste dal Codice della Privacy, l'"amministratore" non c'è più.

Infatti, se sotto la vecchia normativa della Legge 675/96, con il DPR 318/99 il Legislatore aveva definito l'amministratore di sistema come il "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema o di un sistema di banca dati e di consentirne l'utilizzazione", invece con il Dlgs 196/2003, (che ha abrogato la normativa precedente), dell'amministratore di sistema se ne è cancellata ogni traccia.

Linee guida in tema di referti on-line - 25 giugno 2009 (G.U. n. 162 del 15 luglio 2009)

Registro delle deliberazioni n. 21 del 25 giugno 2009 e nel **19 novembre 2009** le "Linee guida in tema di referti online".

Il documento inerente i referti online riguarda:

- Ambito di applicazione delle linee guida
- Facoltatività del servizio di refertazione online
- Informativa e consenso
- Archivio dei referti
- Comunicazione dei dati all'interessato
- Misure di sicurezza e tempi di conservazione dei dati.

Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario - 5 marzo 2009 (G.U. n. 71 del 26 marzo 2009) **Registro delle deliberazioni - Del. n. 8 del 5 marzo 2009** "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario"

Il documento è diviso in due parti:

la definizione del profilo generale e l'ambito di applicazione, e le "garanzie a tutela dell'interessato" che riguardano:

- diritto alla costituzione di un Fascicolo sanitario elettronico e di un dossier sanitario;
- individuazione dei soggetti che possono trattare i dati;
- accesso ai dati personali contenuti nel Fascicolo sanitario elettronico e nel dossier sanitario;
- diritti dell'interessato sui propri dati personali (art. 7 del Codice);
- limiti alla diffusione e al trasferimento all'estero dei dati;
- informativa e consensi;

- comunicazione al Garante;
- misure di sicurezza.

In sintesi, gli elementi fondamentali vertono sulla libertà del paziente di:

- far costituire o meno un fascicolo sanitario elettronico, con tutte o solo alcune delle informazioni sanitarie che lo riguardano; anche se il paziente non dovesse aderire ha comunque diritto alle prestazioni del SSN;
- manifestare un consenso autonomo e specifico, distinto da quello che si presta a fini di cura della salute; il paziente deve essere informato in modo chiaro, con un linguaggio dettagliato e comprensibile su chi ha accesso ai suoi dati e che tipo di operazioni può effettuare;
- possibilità di "oscurare" la visibilità di alcuni eventi clinici.

Oltre alla compilazione online del fascicolo sanitario elettronico o cartella clinica digitale, offerta dai nuovi sistemi informatici, le strutture sanitarie devono anche occuparsi della dematerializzazione dei vecchi documenti sanitari, ovvero la digitalizzazione di ciò che era stato prodotto su carta per i quali devono rispettare, oltre alle linee guida del garante sopraccitate, le due normative Codice dell'Amministrazione digitale (D.Lgs. n.82 del 2005 – CAD) e nella Deliberazione CNIPA (ora DigitPA) n.11 del 19 febbraio 2004.

Le funzioni principali dell'AdS sono la realizzazione di **copie di sicurezza** (**operazioni di backup e recovery dei dati**) alla **custodia delle credenziali**, alla gestione dei **sistemi di autenticazione e di autorizzazione**. Tali operazioni possono comportare un'effettiva capacità di azione su informazioni da considerarsi a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro " le informazioni medesime.

Da notare poi che, secondo il Codice penale, buona parte delle funzioni tecniche attribuite all'AdS, possono rappresentare una circostanza aggravante, se svolte da chi commette un reato. È il caso ad esempio dell' accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinques). Il provvedimento si rivolge a tutti i soggetti pubblici e privati che trattano dati personali con sistemi di elaborazione elettronica.

13 Responsabilita’

Particolare attenzione deve essere riposta nella definizione delle responsabilità tra le figure coinvolte e nell'integrazione con altre procedure interne (in particolare quelle connesse al Modello di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001).

Compito primario dell'amministratore di sistema deve essere quello istituzionale di proteggere la privacy di quanti affidano i propri dati personali e/o sensibili alla struttura sanitaria.

Gli **Amministratori di Sistema** sono i soggetti a cui è conferito il compito, mediante incarico del Responsabile del trattamento dati, di sovrintendere all'utilizzo, al corretto funzionamento ed alla protezione dei sistemi di gestione ed elaborazione elettronica dei dati.

Ricordo brevemente prima di passare alle sanzioni previste da codice che le funzioni principali dell’AdS sono dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali, alla gestione dei sistemi di autenticazione e di autorizzazione. Tali operazioni possono comportare un'effettiva capacità di azione su informazioni da considerarsi a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro " le informazioni medesime.

Da notare poi che, secondo il Codice penale, buona parte delle funzioni tecniche attribuite all’AdS, possono rappresentare una circostanza aggravante, se svolte da chi commette un reato. È il caso ad esempio dell’ accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinques). Il provvedimento si rivolge a tutti i soggetti pubblici e privati che trattano dati personali con sistemi di elaborazione elettronica.

14 Accesso abusivo a un sistema informatico o telematico

L'accesso abusivo a un sistema informatico o telematico è l'attività tipica posta in essere da un soggetto che si introduce senza autorizzazione in un computer o in un sistema di computer.

In molti ordinamenti questa attività è considerata illecita ed è variamente sanzionata.

Per la configurazione della fattispecie, in molti paesi europei le norme che regolano l'accesso abusivo ad un sistema informatico presentano delle costanti:

- Si richiede che siano state violate delle misure di protezione;
- Si punisce l'accesso abusivo sia da remoto che da locale qualora chi commette il reato non sia autorizzato ad accedere a dei settori di memoria protetti;
- Deve essere minacciata la riservatezza dei dati o dei programmi che il sistema informatico attaccato custodisce.

Ai sensi dell'art. 615-ter del codice penale, l'accesso abusivo ad un sistema informatico o telematico è il reato di chi *abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*.

La norma è stata introdotta con la legge 23 dicembre 1993, n. 547, su sollecitazione comunitaria a seguito della raccomandazione 13 settembre 1989, n. 9, del Consiglio dell'Unione Europea, con la quale si suggerivano misure per la repressione del crimine informatico.

La legge segue peraltro da vicino la revisione delle norme a tutela del diritto d'autore [3], con la quale si è estesa all'ambito informatico la protezione dei diritti sulle opere dell'ingegno, includendovi il software.

15 Sanzioni e aggravanti

La pena ordinaria prevista per il delitto, perseguibile a querela della parte offesa salvo che non ricorra alcuna fra le previste circostanze aggravanti, nel qual caso sarebbe precedibile d'ufficio, è la reclusione fino a 3 anni.

La pena è la reclusione da uno a cinque anni se:

- il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- il colpevole per commettere il fatto usi la violenza contro cose o persone, ovvero se è palesemente armato
- dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La pena è inoltre da 1 a 5 anni se i fatti previsti al comma I riguardano sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, mentre è da 3 a 8 anni se gli ora detti sistemi sono oggetto di quanto di cui al comma II.

15.1. *La lesione del domicilio informatico*

Secondo una tesi avanzata in dottrina, il legislatore mirerebbe ad introdurre la figura del «*domicilio informatico*» inteso come un'espansione ideale dell'area di rispetto pertinente al soggetto interessato. Ciò che si vuole tutelare sarebbe quindi una sorta di *privacy informatica*, ancor prima di verificare se siano state attaccate l'integrità e la riservatezza dei dati.

Si dovrebbe pertanto regolare in analogia con quanto si dispone in materia di violazione di domicilio.

Secondo un'altra tesi, il domicilio informatico non può assolutamente essere comparato alla tradizionale figura di domicilio in quanto non c'è alcuna analogia tra i sistemi informatici e i luoghi privati menzionati dall'art. 614 c.p. A questo si aggiunge il fatto che se il domicilio tradizionale e quello informatico fossero messi sullo stesso piano, non sarebbe comprensibile la scelta del legislatore di tutelare solo i sistemi informatici protetti da misure di sicurezza.

Considerata l'aggravante applicabile (*se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti*) si può assumere che l'art. 615-ter c.p. miri a salvaguardare l'integrità dei dati prescindendo dalla collocazione dell'art. sull'accesso abusivo tra i reati di violazione del domicilio.

Considerando invece la decisione del legislatore di tutelare solo i sistemi protetti da misure di sicurezza pare plausibile, ai sostenitori di questa tesi, l'intenzione di salvaguardare la riservatezza dei dati. Si assume infatti che il titolare debba manifestare il suo interesse a tutelare la riservatezza dei dati, adattando misure di sicurezza indipendentemente dalla loro complessità tecnica di implementazione.

15.2. *L'intrusione abusiva*

L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema. L'art. 615-ter c.p. punisce la semplice intrusione ancor prima di valutare l'ipotesi di danneggiamento o furto dei dati.

Il reato può anche essere causato da soggetti legittimati all'uso del sistema, autorizzati ad accedere solo ad una parte dei dati contenuti in memoria. In tal caso il sistema protetto diviene quella parte di memoria a cui l'accesso non è autorizzato.

15.3. *La permanenza nel sistema altrui*

Ha senso parlare di *permanenza non autorizzata* qualora il soggetto responsabile dell'intrusione si sia trovato casualmente in una zona protetta del sistema. Ad una introduzione nel sistema inizialmente autorizzata deve quindi far seguito una permanenza non autorizzata che si realizza allorquando il reo "vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo"[1].

1. Utilizzando un computer esterno, distinto da quello che si intenda attaccare. L'accesso può avvenire attraverso una rete telematica cui il sistema attaccato sia connesso, ad esempio Internet.
2. Accedendo al sistema con la macchina che lo contiene, ad esempio "curiosando" in un computer altrui del quale per qualsiasi motivo si sia avuta temporaneamente nella disponibilità.
3. Violazione del D.Lgs. 29 dicembre 1992, n. 518
4. Senza Id.
5. Negando tutela a quelli privi di misure di sicurezza.

16 Frode informatica Art. 640 ter

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena e' della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto e' commesso con abuso della qualità di operatore del sistema. Il delitto e' punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante (1). (1) Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547.

17 Danneggiamento di sistemi informatici e telematici Art. 635-bis Codice Penale

1. Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

2. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

La pena è della reclusione da sei mesi a tre anni [c.p.p. 235] e si procede d'ufficio, se il fatto è commesso:

1. con violenza alla persona o con minaccia [c.p. 634, 635-bis, 635-ter, 635-quater, 635-quinquies];

2. da datori di lavoro in occasione di serrate, o da lavoratori in occasione di sciopero [c.p. 502, 505], ovvero in occasione di alcuno dei delitti preveduti dagli articoli 330, 331 e 333;

3. su edifici pubblici o destinati a uso pubblico o all'esercizio di un culto, o su cose di interesse storico o artistico ovunque siano ubicate o su immobili compresi nel perimetro dei centri storici ovvero su immobili i cui lavori di costruzione, di ristrutturazione, di recupero o di risanamento sono in corso o risultano ultimati, o su altre delle cose indicate nel n. 7 dell'articolo 625 [c.p. 508]

4. sopra opere destinate all'irrigazione;

5. sopra piante di viti, di alberi o arbusti fruttiferi, o su boschi, selve o foreste, ovvero su vivai forestali destinati al rimboschimento [c.p. 639, 649, 664; c.n. 1123];

5-bis. sopra attrezzature e impianti sportivi al fine di impedire o interrompere lo svolgimento di manifestazioni sportive .

Per i reati di cui al secondo comma, la sospensione condizionale della pena è subordinata all'eliminazione delle conseguenze dannose o pericolose del reato, ovvero, se il condannato non si oppone, alla prestazione di attività non retribuita a favore della collettività per un tempo determinato, comunque non superiore alla durata della pena sospesa, secondo le modalità indicate

---

[1] Giacomo Stalla, *L'accesso abusivo ad un sistema informatico o telematico*

dal giudice nella sentenza di condanna.

17.1. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. Art. 635 ter Codice Penale.*

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata [1 e 2].

17.2. *Analisi della norma*

Secondo alcuni giuristi l'inclusione della norma in seno al codice penale, anziché la sua introduzione attraverso una legge speciale, risponderebbe all'esigenza di non sancire, almeno in quella fase, «*il riconoscimento del "bene" informatico quale oggetto sufficiente ed autonomo di tutela penale*», preferendone una visione meramente strumentale rispetto a beni giuridicamente più tradizionali come «*il patrimonio, la fede pubblica, l'inviolabilità dei segreti, la libertà individuale anche nelle sue implicazioni [...] con la inviolabilità del domicilio*».

Mentre altre fattispecie di crimine informatico potevano agevolmente sommarsi a previsioni di ambiti più generali già vigenti e sufficientemente analoghe (ad esempio la frode, il falso informatico, il danneggiamento e gli illeciti correlati alla comunicazione), l'intrusione nei sistemi altrui trovava una solo labile analogia, e del tutto inapplicabilmente teorica, con la violazione di domicilio, richiedendosi pertanto una figura criminosa specifica.

---

[1] Articolo aggiunto dall'art. 5, L. 18 marzo 2008, n. 48, che ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica.

[2] Per l'aumento della pena per i delitti non colposi di cui al presente titolo commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, vedi l'art. 36, comma 1, L. 5 febbraio 1992, n. 104, come sostituito dal comma 1 dell'art. 3, L. 15 luglio 2009, n. 94.

18 Obblighi quale Amministratore di sistema

Il Responsabile, in relazione alle attività oggetto del presente contratto che comportano la gestione, manutenzione ed utilizzo dei sistemi, si impegna ad operare e porre in essere le misure prescritte dal provvedimento del Garante della privacy del 27 novembre 2008 sugli amministratori di sistema. In particolare, si impegna a:

tenere aggiornata la lista dei propri operatori designati Amministratori di sistema, correlata con gli ambiti di competenza affidati,

mantenere per un periodo minimo di 6 mesi i log degli accessi degli amministratori di sistema per tutti i sistemi affidatigli.

fornire, su richiesta del Mandante o in caso di richiesta dell'Autorità Garante, l'elenco degli amministratori di sistema con relativi ambiti di competenza (da esso detenuto o fornito dall'outsourcer cui siano stati affidati parzialmente o integralmente servizi IT).

19 CCNL, posizione organizzativa/coordinamento: riconoscimento economico e di responsabilità

Quanto detto fino ad ora, fa comprendere le avanzate conoscenze e capacità che deve possedere un amministratore di sistema. Il possesso di un titolo che ne attesti tali è indispensabile per esercitare ed individuare tale figura professionale, responsabile e competente, per cui è necessario una figura professionale con funzioni specialistiche.

Il riconoscimento di tale figura, attualmente in Italia non è ancora ben definita e nelle realtà sanitarie, l'applicazione ed il riconoscimento del ruolo di amministratore di sistema si è insediata in maniera differente e variegata.

Di fatti in alcuni casi l'amministratore di sistema non è un operatore sanitario.

In casi dove lo è non ha titolo professionale e ne riconoscimento di progressione di carriera e/o di coordinamento. In oltre il 50% delle realtà sanitarie italiane l'amministrazione del sistema è affidata a ditte esterne. Quest'ultime con ridotte o assenti capacità cliniche. Il sistema informatico digitale per il suo corretto esercizio richiede capacita sia tecniche che cliniche ed essendo risorsa assegnata alle aziende ospedaliere è indispensabile la sua gestione da parte del personale che ne fa uso.

Le aziende sanitarie ed i contratti collettivi di lavoro (CCNL) tutt' oggi non ancora hanno le idee chiare su tale figura e sulle potenzialità che essa ha a livello aziendale, sia sull'aspetto gestionale che produttivo. Di fatti tale funzione e relativo profilo professionale non ancora è ben legiferata e sono ancora poco chiare le responsabilità da assegnare.

Un punto di partenza è stato dato dalla legge n. 43 del 1 febbraio 2006, (regolamento delle professioni sanitarie) che all' art. 6 comma 1 lettera c, individua la funzione di coordinamento ai professionisti specialisti in possesso di master di 1° livello rilasciato dalle università. Di fatti le

ultime riforme universitarie (D.M. 509/99) ed i recenti ordinamenti didattici prevedono master specialistici per le professioni sanitarie tra cui quello in "Scienze Tecniche Applicate alla Gestione dei Sistemi Informatici" al quale accesso è indispensabile la laurea di 1° livello in "Tecniche Sanitarie di Radiologia Medica e Radioterapia".

Inoltre le nuove contrattazioni a livello sanitario (CCNL) prevedono come titolo preferenziale il master per esercitare la funzione di coordinamento (ART. 10 CCN sanità). Come sopra detto l'amministratore di sistemi informatici è la figura che coordina le risorse tecnologiche come hardware e software per garantire il loro corretto funzionamento ed utilizzo, gestendo il flusso di dati e fornendo informazioni all'azienda utili per i programmi di miglioramento.

Detto ciò è facile intuire che spetta ad un operatore sanitario esperto la figura di Amministratore di Sistemi Informatici ed il riconoscimento della funzione di coordinamento con relativa indennità. Oltre alla possibilità di progressione di carriera.

Inoltre considerando i vari compiti ed al tempo necessario per svolgerli, è indispensabile che le aziende permettano al professionista specialistico l'autonomia dei giorni di lavoro e dell'orario garantendo comunque continuità e sicurezza operativa.

20 Posizione organizzativa

L'interrogativo che ci poniamo è: come può una figura chiave come l'amministratore di sistema, sul quale ricadono responsabilità da far venire la pelle d'oca (basti pensare a compiti inerenti la preservazione dei dati aziendali a partire dal classico back-up) al direttore generale di una qualsiasi ASL (e qui basti pensare all'imponente mole di dati che ogni giorno fluiscono dai database di ogni ospedale….), essere individuato "generalmente" in modo del tutto ibrido ?

Riteniamo decisamente che, al Titolo IV del Dlgs 196/2003 dove troviamo i "Soggetti che effettuano il trattamento", come l'articolo 28 definisce la nozione di "titolare del trattamento", l'articolo 29 quella di "responsabile del trattamento", e l'articolo 30 quella dell' "incaricato al trattamento", debba necessariamente essere inserito anche la figura di "amministratore di sistema", assegnando a questo un ruolo formale, ben chiaro e definito, per evitare annacquamenti delle responsabilità che questo deve assumersi, evitando altresì che la sua non menzione nel testo ufficiale di Legge finisca per svilire di fatto l'importante ruolo chiave che invece svolge nella quotidiana gestione dei dati.

Questo per quanto riguarda gli amministratori di sistema ‘’tout court’’, propriamente detti.

Inoltre ci sarebbe da ascrivere un'altra differenza, oltre alla sopracitata; la distinzione di una nuova figura professionale operante in una frazione dell' ormai gigantesco universo dei dati sensibili, coloro che già oggi, seppur limitatamente, si occupano dei dati che circolano in un settore strategico di ogni azienda ospedaliera, la Diagnostica per Immagini.

21 Bibliografia

- D.L.vo 196/03 "Codice in materia di protezione dei dati personali"
- D.L.vo 82/05, Codice dell'amministrazione digitale
- Deliberazione CNIPA n. 11/04 (dematerializzazione)
- Provvedimento del Garante Privacy, 27 novembre 2008
- Linee guida per la dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini.
- Linee guida sulla Teleradiologia (2004 SIRM)
- L'atto medico radiologico (2007 SIRM)
- Decreto legislativo 187/00
- D.Lgs n. 159 dell'aprile 2006.
- Decreto 'anti-crisi' (D. L. 185/2008
- Testo Unico n. 445/2000
- www.wikipedia.it
- P. Subioli, La svolta del documento informatico, 6 febbraio 2006, in Cronache dell'e-government
- ISSN 1123-3117
- Rapporti ISTISAN 07/26
- ALESSANDRI, Criminalità informatica, RTDPE, 1990, 653ss;
- ATERNO, Non sussiste il reato di accesso abusivo se sul sistema informatico "attaccato" mancano le misure di sicurezza (art. 615 ter c.p.), vedi http://www.penale.it/page.asp?mode=1&IDPag=175;
- ATERNO, sull'accesso abusivo a un sistema informatico o telematico, in Cass. pen., 2000, p. 2995 ss;
- ATERNO, la cassazione non convince in materia di intercettazioni telematiche, in Cass. pen.,2005; A.A.V.V., Informatica e criminalità organizzata (atti della tavola rotonda di Palermo, 4-2-1984), Milano;
- ATERNO – CUNIBERTI – GALLUS – MICOZZI, La legge di ratifica della Convenzione di Budapest del 23 novembre 2001, in http://www.altalex.com/index.php?idnot=41438;

- A.A.V.V., Problemi giuridici dell'informatica nel MEC, a cura di P. Galdieri, Milano, 1996, 190 ss (Atti sul convegno di studi su "La libera circolazione dei beni e dei servizi informatici nel MEC oggi chiamato SEE, Spazio Economico Europeo", curato dalla Facoltà di Giurisprudenza della LUISS di Roma nell'ottobre 1994);
- BERGHELLA, BLAIOTTA, Diritto penale dell'informatica e beni giuridici, in Cass. pen., 1995, p.2330 ss; BERNASCONI, La prevenzione del computer crime nel settore bancario, (l'esperienza svizzera), DII, 1988, p.723 ss;
- BORRUSO-BUONOMO – CORASANITI – D'AIETTI, Profili penali dell'informatica, Milano, 1994; CASO, Criminalità informatica:"bombe logiche" e danneggiamento di software, For. It., 1991, II, 228;
- F.G.CATULLO, Il caso vierika: un interessante pronuncia in materia di virus informatici e prova digitale, commento a Trib. Bologna, 22 dicembre 2005, in Diritto dell'internet, n. 2, 2006, p.153 ss.,
- CECCACCI, Computer Crimes. La nuova disciplina dei reati informatici, Milano, 1994.
- G. CORRIAS LUCENTE, Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi, in Dir.inf., 2001, p. 492, ss;
- G.CORRIAS LUCENTE, Diritto penale e informatica, in Dir. Inf., 2003, p.49;
- CRESCENZI, Riconoscimento giuridico del documento informatico e suo valore probatorio, in Docum. Giust., 1997, n. 9, 1989 ss.
- M. CUNIBERTI – G.B.GALLUS – F.P.MICOZZI, I nuovi reati informatici, Giappichelli, Torino, 2009;
- L. CUOMO, La tutela penale del sistema informatico, in Cass. Pen. 2000, p. 2999 ss;
- L. CUOMO – B. IZZI, Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico, in Cass.pen.,2002, 1018 ss;
- DE SANTIS, Tipologia e diffusione del documento informatico. Pregresse difficoltà di un suo inquadramento normativo, in Corr. Giur., 1998, n. 4, 383ss. ;
- FLOR R., Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus, in Cass. pen., 2009, 4, 1502;
- FLOR R., Frodi identitarie e diritto penale, in Riv. Giur. Ec. Az., 3, 2008 ; vedi anche http://www.penale.it/page.asp?mode=1&IDPag=730
- FLOR R., Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto, in Dir. pen. proc., 2008, 106 e ss. ;

- FLOR R., Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente, in Riv. it. dir. proc. pen., 2007, 899 e ss. ;
- FLOR R., Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios, in Dir. Pen. Proc., 2005, 81 e ss.
- FONDAROLI, La tutela penale dei beni informatici, DII, 1996, 91 ss;
- FROSINI, Informatica e criminalità organizzata, DII, 1993, p.75;
- GALDIERI, Teoria e pratica nell'interpretazione del reato informatico, Milano, 1998;
- GALDIERI, La tutela penale del domicilio informatico, in AAVV, Problemi giuridici dell'informatica nel MEC, a cura di P. Galdieri, Milano, 1996, 189 ss;
- GALDIERI, Reti informatiche: nella violazione del domicilio è difficile stabilire il luogo del commesso reato, in Guida al Diritto, Sole 24 ore, aprile 1995;
- GALDIERI, Internet e l'illecito penale, GM, 1998, 856 ss;
- P. GALDIERI, L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker, in Guida Dir. , 2001, n. 8, p.81;
- GIANNANTONIO, i reati informatici, DII, 1992, 335;
- E. GIANNANTONIO, L'oggetto giuridico dei reati informatici, in Cass.pen., 2001, 2244 ss;
- D. LUSITANO, In tema di accesso abusivo a sistemi informatici, in Giur. It, 1998, p.1923;
- MANNA, Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso di mezzi di pagamento elettronici, DII, 2002, 955; MASI, frodi informatiche e attività bancaria, RPE, 1995, n. 4, 427 ss;
- MAZZEI, Appunti sulla repressione penale dei computer crimes, RTDPE, 1992, 693;
- MILITELLO, Nuove esigenze di tutela penale e trattamento elettronico delle informazioni, RTDPE, 1992, 369 ss;
- MINOTTI, I reati commessi mediante Internet, in Internet. Nuovi problemi e questioni controverse (a cura di G. Cassano), Milano, 2001;
- MUCCIARELLI, «Computer (diritto penale) », in Digesto pen., Torino, 1989;
- MUCCIARELLI, Commento agli articoli1,2,4,10 della legge 23.12.1993 n. 547, Legislazione Penale, 1996, n. ½, 57 ss;
- PAGLIARO, Informatica e crimine organizzato, IP, 1990, 414 ss; PALOMBI, PICA, Diritto penale dell'economia e dell'impresa, I, Torino, 1996;

- PARODI-CALICE, Responsabilità penali e Internet, Milano, 2001;
- PAZIENZA, In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547, RIDPP, 1995, 750 ss e 1089;
- C. PECORELLA, Diritto penale dell'informatica, Milano, 2000;
- PETRONE, Le recenti modifiche del codice penale in tema di documento informatico: problemi e prospettive, DII, 1995, 259;
- PICA, La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche, Riv. Pen. Economia, 1995, IV, 403, ss;
- PICA, Diritto penale delle tecnologie informatiche, Torino, 1999;
- PICOTTI, Commento agli artt. 3,5,7,8, L. 23.12.1993 n. 547, Legislazione penale, 1996, n.1/2, p.62 ss, 109;
- PICOTTI, Problemi penalistici in tema di falsificazione di dati informatici, in F.FERRACUTI, Trattato di criminologia medicina criminologia e psichiatria forense, X, Il cambiamento delle forme di criminalità e devianza, Milano, 1988;
- PICOTTI, Profili penali delle comunicazioni illecite via Internet, DII, 1999, II, n. 2, 283;
- PICOTTI, Reati informatici, in Enc. Giur., Roma, 2002;
- PICOTTI, Fondamento e limiti della responsabilità penale dei service -providers in Internet, DPP, 1999;
- PICOTTI, Internet e responsabilità penali, in Diritto e Informatica, a cura di PASCUZZI, Milano, 2002;
- POMANTE, Internet e criminalità, Torino, 1999; RESTA, i computer crimes tra informatica e telematica, Padova, 2000;
- S. SABATTINI, Profili penali in tema di accesso abusivo ad un sistema informatico, in Crit. dir. 2001, p.407 ss;
- SARZANA di S. IPPOLITO, Informatica e diritto penale, Milano 1994;
- SEMINARA, La responsabilità penale degli operatori su Internet, DPP, 1998, 745 ss;
- SIEBER, Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di internet, RTDPE, 1997, 743 ss;
- D. TRENTACAPILLI, Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione, in Dir. Pen. e proc., 2002, 1280 ss;
- TROIANO, Gli illeciti attraverso internet: problemi di imputazione e responsabilità, AIDA, 1998, 405 ss;

- P.VENEZIANI, I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali, in Ind. Pen. 2000, 139 ss.;
- Vincenzo Zeno-Zencovich, I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari), DII, 1999, 1050.