FONDAZIONE PONTIROLO ONLUS INTERCOMUNALE
Via Alessandro Volta n. 4 - 20090 Assago (MI)
Tel 02/45.700.758. - Fax 02/89.77.06.74. – E-mail: info@pontiroloonlus.it – Sito Internet: www.pontiroloonlus.it

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

1) Le condotte tipiche.

A seguito della ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001, l'art. 24 del D.Lgs. 231/01 è stato inserito l'art. 24-bis "*Delitti informatici e trattamento illecito di dati*".
Il recepimento della convenzione ha esteso la responsabilità amministrativa degli enti ai seguenti reati informatici:
• *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.):* commette il reato chiunque 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.
Il reato è aggravato se: a) il fatto è commesso da un pubblico ufficiale o da un incaricato di un 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; b) il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; c) 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.
Aggravanti sono previste qualora i fatti riguardino 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.
La norma non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma si propone di tutelare i c.d. beni informatici e di reprimere il dilagante fenomeno dei reati informatici, intesi quali condotte illecite aventi come oggetto o strumento i sistemi di archiviazione/elaborazione di dati ed informazioni oppure la trasmissione automatica degli stessi.
E' reato comune che si perfeziona con la violazione del domicilio informatico.
• *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)*
La norma completa la tutela prevista dall'articolo precedente e punisce l'abusiva acquisizione, in qualsiasi modo, dei mezzi o codici di accesso che consenta a soggetti non legittimati di inserirsi nel sistema informatico o telematico altrui, vanificando l'ostacolo costituito dalle misure di protezione.
E' un reato comune di pericolo che richiede il deliberato fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.
• *Diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)*
La disposizione in esame mira a reprimere il comportamento di colui che diffonde uno dei cosiddetti "programmi virus" il cui effetto è quello di danneggiare od alterare l'hardware, il software o i dati e le informazioni contenuti in un sistema informatico o telematico, nonché l'interruzione, totale o parziale, o l'alterazione del funzionamento di questi ultimi.
E' reato comune, alimentato dallo scopo di danneggiare illecitamente un sistema informatico o telematico.
• *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)*

La norma intende tutelare sia la libertà di comunicare sia il diritto alla riservatezza delle comunicazioni. Viene punita la condotta di chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.
Sono previste aggravanti per il caso in cui il fatto sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; sia commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; sia commesso da chi esercita anche abusivamente la professione di investigatore privato.
• *Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)*
La norma offre una forma di tutela anticipata rispetto ai beni protetti dal precedente articolo, attraverso la previsione di punibilità per comportamenti prodromici rispetto a quelli di vera e propria interferenza nelle comunicazioni informatiche o telematiche.
La condotta punita consiste nell'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico.
• *Danneggiamento di informazioni, dati e programmi informatici (art. 635bis c.p.)*
Viene punito chiunque distrugga, deteriori o renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui. Anche in questo caso il reato è aggravato dalle particolari modalità di commissione del fatto ovvero dalla particolare qualifica (operatore di sistema) dell'autore.
• *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)*
La disposizione appresta tutela penale riguardo ai medesimi fatti sanzionati dall'articolo precedente allorquando l'attività delittuosa si diriga avverso informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
Se dal fatto deriva effettivamente il danneggiamento di informazioni, dati o programmi informatici, la pena è aumentata.
Ulteriore circostanza aggravante è prevista se il fatto è commesso con abuso della qualità di operatore del sistema.
• *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)*
Oggetto giuridico dell'incriminazione è costituito dalla necessità di apprestare tutela all'integrità di quella parte del patrimonio rappresentato dai sistemi informatici. La condotta tipica è quella riconducibile al fenomeno del c.d. hackeraggio, mentre l'evento finale può anche tradursi in un grave ostacolo al funzionamento del sistema: viene infatti punito chiunque, mediante le condotte di cui all'art. 635 bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.
• *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)*
La norma punisce più gravemente il fatto di cui all'art. 635 quater c.p. qualora sia diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità (od anche di privati qualora ricorra il requisito della pubblica utilità) o ad ostacolarne gravemente il funzionamento.

- *Frode informatica e sostituzione dell'identità digitale (art. 640 ter comma 3 c.p.)*

La disposizione è stata introdotta dal D.L. 14.08.2013, n. 93, convertito in L. 15.10.13, n. 119, con l'intento di rendere più efficace il contrasto del preoccupante e crescente fenomeno del cosiddetto "furto d'identità digitale", attraverso il quale vengono commesse frodi informatiche, talora con notevole nocumento economico per la vittima.
La disposizione punisce la condotta di chi commetta furto o faccia indebito utilizzo dell'identità digitale altrui, in danno di uno o più soggetti.
La particolare pericolosità che tali condotte determinano per la sicurezza dei commerci telematici e delle relative transazioni, ha indotto il legislatore ha prevedere la procedibilità d'ufficio.
• *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies)*
La ratio della norma è ravvisabile nella necessità di sottoporre a sanzione penale la condotta del certificatore di firma elettronica che agisce in violazione degli obblighi di legge, ma senza commettere atti di alterazione o di intervento abusivo sul sistema informatico o telematico e perciò sfugge all'ambito applicativo della fattispecie generale di frode informatica prevista dall'art. 640 ter c.p.
La condotta materiale del reato consiste nella violazione di uno qualunque dei numerosi obblighi previsti a carico del certificatore da una norma di legge ed in particolare dall'art. 32, co. 3, D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale).
• *Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491bis c.p.)*
L'art. 491-bis c.p. dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previsti e puniti dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessi da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessi da persone esercenti servizi di pubblica necessità, uso di atto falso.
Per "documento informatico" s'intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti così come riportato dall'art. 1 lettera p) del D.Lgs. 82/05.
La disposizione in esame si propone la tutela della fede pubblica attraverso la salvaguardia dell'integrità del documento informatico nella sua valenza probatoria.

2) Aree a rischio.

In relazione ai reati ed alle condotte criminose sopra citate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente parte speciale, i luoghi di lavoro relativi all'area medica ed amministrativa, forniti di terminali informatici anche collegati in rete, nonché ogni altro luogo di pertinenza dell'Ente, accessibile al lavoratore nell'ambito del proprio lavoro, in cui sia previsto l'utilizzo di un terminale informatico.
Nell'ambito di dette aree sono ricomprese le attività:

- svolte tramite l'utilizzo dei Sistemi Informativi interni, compresi i servizi di posta elettronica e dell'accesso ad Internet;
- di gestione dei Sistemi Informativi al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione nonché la sicurezza informatica in funzione del progresso tecnologico;
- di gestione dei flussi informativi elettronici con la pubblica amministrazione.
- di gestione e protezione delle postazioni di lavoro, oltre che delle credenziali di accesso (password);
- di gestione degli accessi verso l'esterno;

- di gestione e protezione delle reti;
- di gestione degli *output* di sistema e dei dispositivi di memorizzazione;
- di sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);
- di verifica periodica, almeno annuale, di tutti i profili di autorizzazione e di accesso ai dati;
- di attivazione e verifica di un efficace sistema di backup dei dati;
- di distruzione di tutti i supporti rimovibili non più utilizzati;
- di adeguate procedure per il trattamento informatico dei dati personali sensibili;
- di un adeguato sistema di registrazione degli accessi dell'Amministratore di sistema effettuati su tutte le postazioni di lavoro dotate di dati personali comuni o sensibili.

3) Destinatari.

La presente parte speciale si riferisce a comportamenti posti in essere dai dipendenti, amministratori e consulenti (anche medici con contratto a libera professione).
Obiettivo della presente parte speciale è garantire che i destinatari mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.
L'Ente, ha adottato il Documento Programmatico sulla Sicurezza (d'ora in poi D.P.S.) ai sensi del D.Lgs. 196/03, che qui si intende integralmente richiamato ed efficaci politiche di sicurezza informatica e misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.
Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che l'Ente si pone sono i seguenti:
- *riservatezza*: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati;
- *integrità*: garanzia che ogni dato sia quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- *disponibilità*: garanzia di reperibilità di dati in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.
In particolare nell'espletamento delle attività considerate a rischio è fatto divieto ai destinatari di:

- alterare documenti informatici, pubblici o privati;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni o al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

Pertanto, i destinatari dovranno:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza autorizzazione scritta;
- in caso di smarrimento o furto di apparecchiature informatiche contenenti dati personali o delle credenziali di accesso (password) avvisare immediatamente l'Amministratore di sistema ed il

Responsabile Privacy dell'Ente che provvederanno a presentare denuncia all'Autorità Giudiziaria preposta;

- evitare di trasferire all'esterno dell'Ente e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Ente stesso, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del Responsabile Privacy.
- evitare l'utilizzo di *password* di altro utente, neanche per l'accesso ad aree protette in nome e per conto dello stesso;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- segnalare immediatamente all'Amministratore del Sistema Informatico utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature dell'Ente solo prodotti software ufficialmente acquisiti dall'Ente stesso;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- non disattivare mai l'antivirus ed il firewall preimpostato dal sistema operativo nelle singole postazioni di lavoro;
- non forzare l'accesso a cartelle e/o files dedicate/i (il cui utilizzo è consentito, quindi, solo a predeterminate postazioni di lavoro);
- interpellare l'amministratore del sistema informatico per procedere alla forzatura delle cartelle dedicate: questi potrà procedere alla forzatura, e quindi allo sblocco, a favore di altri utenti solo se autorizzato dal Responsabile Privacy dell'Ente.

4) Linee di condotta finalizzate ad evitare la commissione di reati.

Il D.P.S. adottato dall'Ente ai sensi del D.Lgs. 196/03 prevede numerosi adempimenti, alcuni dei quali idonei anche a prevenire la commissione dei reati di cui alla presente parte speciale.
Fermo quanto sopra, è opportuno che per una maggiore sicurezza e per un costante monitoraggio di accesso ai sistemi informatici e telematici vengano pianificate, per quanto mancanti, con l'ausilio dell'amministratore del sistema informativo, eventuali contromisure da porre in essere nell'ipotesi in cui siano identificate vulnerabilità, carenze di protezione, minacce, danni con riferimento a hardware, software, documentazione, atti, ecc...

5) Istruzioni e verifiche dell'organismo di vigilanza.

L'attività dell'OdV sarà svolta in stretta collaborazione con tutti i destinatari del modello, in particolare con coloro che utilizzano, anche non regolarmente, video terminali, nonché con l'amministratore del sistema informatico.
I controlli svolti dall'OdV saranno diretti a verificare il rispetto sia delle regole procedurali già in essere in attuazione di quanto previsto dal D.P.S. sia di quelle precedentemente esposte, la loro osservanza, attuazione e, soprattutto, adeguatezza rispetto alle esigenze di prevenire la commissione dei reati in esame, nonché la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.
A tal fine, si ribadisce che all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di attività sensibili, a semplice richiesta.

6. Protocolli specifici di prevenzione.

Al fine di dare concreta attuazione ai principi esposti ai precedenti punti 3) e 4), i protocolli prevedono che:

a) Gestione del database:

- siano sempre identificati, tramite idonea documentazione, i soggetti ai quali consentire l'accesso al proprio *database;*
- sia custodita copia della predetta documentazione per l'intera durata delle credenziali di autenticazione concesse. La custodia dei documenti è affidata all'ufficio Segreteria generale;
- il Responsabile privacy, unitamente all'Amministratore di sistema, ed in collaborazione con l'eventuale *software house* esterna, all'atto dell'installazione, e successivamente tramite cicliche rivalutazioni:

1) accerta l'impossibilità per gli operatori di accedere ai dati archiviati per distruggerli, deteriorarli, cancellarli, sopprimerli o alterarli sotto ogni forma, in tutto o in parte;
2) effettua un costante monitoraggio dell'integrità dei sistemi informatici, dei livelli ed autorizzazioni di accesso, del corretto trattamento delle *password* e delle credenziali di accesso al sistema informatico;

- dovrà essere vietato agli operatori cedere a terzi le proprie credenziali di autorizzazione e prevedere che le *password* di accesso alla rete interna ed alle diverse applicazioni siano custodite dagli operatori secondo criteri idonei ad impedirne una facile individuazione ed un uso improprio;
- i livelli di autorizzazione all'accesso (alla rete aziendale e/o ad altri sistemi di proprietà di terzi) dovranno essere registrate su archivi informatici ai fini della loro tracciabilità nelle diverse aree a rischio.

b) Gestione delle cartelle cliniche:

- il direttore sanitario o un suo delegato deve esaminare, con cadenza almeno annuale, un campione significativo di cartelle cliniche anche attraverso procedure di autocontrollo proceduralizzate, verificando la congruenza o la completezza dei dati ivi riportati;

c) Rilascio certificati e notificazioni:

- l'amministratore di sistema verifica l'impossibilità da parte degli operatori di sistema di modificare le informazioni oggetto di certificazione tramite un'opportuna organizzazione di profili operatore e regole di sistema, che garantiscano l'impossibilità di alterare il dato inserito da altri ed anche, se trascorso un rilevante lasso di tempo, dallo stesso operatore.