PARTE SPECIALE

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

art. 24 BIS D.Lgs. 231/2001

COLOPLAST S.p.A.

PARTE SPECIALE RIGUARDANTE ART. 24 BIS - DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

In data 5 aprile 2008 è entrata in vigore la Legge n. 48, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

Con tale norma il Legislatore ha apportato modifiche al codice penale in materia di reati informatici ed ha introdotto al D. Lgs. 231/01, l'art. 24 bis per la punibilità dell'

Ente in relazione ai delitti informatici e al trattamento illecito dei dati, come previsto dagli artt. 491 bis, 615 ter- quinquies, 617 quater e quinquies, 632 bis-quinquies, 617 quater e quinquies, 635 bis-quinquies, 640 quinquies del codice penale.

1. I REATI

Costituiscono reato ai sensi del D. Lgs. 231/01:

- *Documenti informatici (art. 491-bis cod. pen.)*

Tale norma prevede che "se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private", con conseguente punibilità del reato di falsità anche in relazione ai documenti informatici.

- *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter cod. pen.)*

Per la punizione in caso di introduzione in un sistema informatico o telematico protetto da misure di sicurezza ovvero di mantenimento nel sistema contro la volontà espressa o tacita di chi ha il diritto di esclusione.

- *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater cod. pen.)*

Prevede la punibilità nell'ipotesi in cui un soggetto, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure

di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

- *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen.)*

Con le recenti modifiche alla norma è punibile "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici".

- *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater cod.pen.)*

Viene introdotta la punibilità in caso di intercettazione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedimento/interruzione delle stesse rivela, ed anche in caso di rivelazione del contenuto delle comunicazioni mediante qualsiasi mezzo di informazione al pubblico.

- *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (617 quinquies cod.pen.)*

Tale ipotesi di reato punisce l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, salvi i casi previsti dalla legge.

- *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis cod. pen)*

L'ente è punibile anche in caso di reati relativi a distruzione, deteriormento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui.

- *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635 ter cod. pen.)*

Responsabilità dell'Ente anche in tale ipotesi di reato che si configura in relazione a fatti diretti 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.

- *Danneggiamento di sistemi informatici o telematici (art. 635 quater cod. pen)*

L'ipotesi di reato si configura nel caso in cui, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, vi sia distruzione, danneggiamento o inservibilità, in tutto o in parte, di sistemi informatici o telematici altrui oppure grave ostacolo al funzionamento.

- *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies cod. pen.)*

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

- *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cod.pen)*

Il reato è previsto in caso di prestazione di servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, con violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

2 AREE POTENZIALMENTE A RISCHIO

I reati sopra considerati trovano come presupposto l'utilizzo di strumenti informatici e l'abuso di tali strumenti nell'interesse dell'Ente.

In generale, vengono definite **aree a rischio**, tutte quelle aree aziendali che, per lo svolgimento della propria attività, utilizzano strumenti informatici, con particolare riferimento alla divisione informatica e alle funzioni che potrebbero accedere, quanto meno in linea teorica, agli strumenti informatici altrui. Il rischio è ipotizzabile per tutte le funzioni aziendali, stante l'utilizzo quotidiano da parte di tutti degli strumenti informatici, ma solo in linea astratta. In realtà, infatti, la Società non ha alcuna possibilità di accedere ai sistemi altrui, senza autorizzazione e l'ipotesi di abuso è pressoché remota.

Le aree di attività ritenute più specificamente a rischio, quali sono state individuate in sede di identificazione dei processi sensibili, sono state circoscritte nelle seguenti:

1. utilizzo della rete aziendale, del servizio di posta elettronica e di accesso ad Internet;
2. gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché sicurezza informatica;
3. erogazione di servizi di installazione e servizi professionali di supporto al personale (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e *security*).
4. Trasmissione di documenti in formato elettronico alla PA nei casi di partecipazione a procedure di gara o di negoziazione diretta, indette da enti pubblici italiani o stranieri per l'assegnazione di commesse (di appalto, di fornitura o di servizi), di concessioni, di partnership, di attività o altre operazioni similari;
5. Accesso a sistemi informatici e telematici gestiti dalla PA (o anche da privati) per la trasmissione di documenti amministrativi (es. modello F24, ecc.)

Eventuali integrazioni delle suddette aree a rischio, ivi incluse quelle afferenti la mappatura delle aree a rischio, potranno essere disposte dal Consiglio di Amministrazione, anche a seguito dell'esame di attività di reporting periodico da parte dell'OdV e dei soggetti che svolgono attività di monitoraggio e verifica.

Le aree a rischio reato, così identificate, costituiscono il punto di riferimento nella definizione delle procedure di controllo da implementare, ai fini dell'adeguamento del sistema di controlli interno.

3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE

3.1. Principi generali

Obiettivo della presente parte speciale è di fare in modo che tutti i Destinatari,

amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio, nonché collaboratori esterni e partners, nella misura in cui sono coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di condotta conformi a quanto prescritto, dalla parte speciale stessa, al fine di prevenire ed impedire il verificarsi di reati.

La presente parte speciale ha la funzione di:

a) fornire i principi generali e procedurali specifici cui i Destinatari, in relazione al tipo di rapporto in essere con la Società, sono tenuti ad attenersi per una corretta applicazione del modello
b) fornire all'OdV e ai responsabili delle altre funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Nell'espletamento di tutte le operazioni, oltre alle regole di cui al presente Modello, i Destinatari devono, in generale, conoscere e rispettare, con riferimento alla rispettiva attività, le regole e i principi contenuti nel Codice Etico e in tutti i documenti aziendali atti a regolare tali attività. A titolo esemplificativo, ma non esaustivo:

- *il codice etico*
- *ogni altro documento/procedura instaurata relativamente al trattamento dei dati tramite supporti informatici*
- *ogni altra normativa relativa al sistema di controllo interno in essere*

Ai collaboratori esterni deve essere resa nota l'adozione del modello e del codice etico, da parte della società: il rispetto dei principi contenuti in tali documenti costituisce obbligo contrattuale a carico di tali soggetti.

La presente parte speciale prevede l'espresso DIVIETO, a carico degli esponenti aziendali, in via diretta, e a carico dei collaboratori esterni, tramite apposite clausole contrattuali, di:

1. porre in essere comportamenti tali, da integrare le fattispecie di reato informatico e trattamento illecito di dati come individuate nella presente Parte Speciale
2. porre in essere comportamenti che, sebbene non risultino tali da costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

a) effettuare accessi e qualsiasi operazione ai sistemi informatici altrui e ai dati altrui, se non autorizzata da apposito accordo contrattuale e comunque con violazione delle procedure esistenti in materia di trattamento dei dati personali ex D. Lgs. 196/2003;
b) utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico e ai principi inclusi nel presente Modello;

Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al Modello e alla presente Parte Speciale, i Destinatari sono tenuti a conoscere ed osservare tutte le regole e i principi contenuti nei seguenti documenti:

1) la politica aziendale relativa alla gestione degli accessi logici a reti, sistemi, dati e applicazioni;
2) la politica aziendale relativa alla gestione delle credenziali personali (username e password);
3) l'impegno alla corretta gestione delle informazioni di cui si viene a conoscenza per ragioni operative.

Ai fini dell'attuazione dei comportamenti di cui sopra COLOPLAST si è dotata di apposite procedure volte ad attuare i principi di cui al D. Lgs. 196/2003 in materia di privacy ed ha nominato un Responsabile in materia per il controllo

degli adempimenti di legge e le opportune verifiche in merito alla effettiva operatività delle procedure. Le stesse impediscono ai soggetti che utilizzano strumenti informatici l'accesso a banche dati non connesso alle effettive necessità legate alla funzione aziendale svolta.

Inoltre la Società organizza periodici corsi di formazione e aggiornamento in materia di trattamenti dei dati al fine di formare e sensibilizzare in merito all'importanza di accessi a dati e strumenti altrui solo nel rispetto dei diritti e della riservatezza altrui.

I medesimi principi sono attuati nel trattamento da parte della Società dei dati e degli strumenti in uso ai dipendenti.

Coloplast inoltre assolve i seguenti adempimenti:

1) fornisce, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli *user-id* e delle *password* per accedere ai principali sottosistemi informatici utilizzati presso la Società;
2) limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
3) effettua, per quanto possibile, nel rispetto della normativa sulla *privacy*, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
4) predispone e mantiene adeguate difese fisiche a protezione dei *server* della Società;
5) predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

3.2. Principi procedurali specifici

In particolare, si elencano qui di seguito le regole che devono essere rispettate dai Destinatari della presente Parte Speciale, meglio individuati al Capitolo precedente, nell'ambito delle Attività Sensibili:

1) i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;
2) è vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
3) è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
4) è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
5) è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
6) è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
7) è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
8) è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
9) è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è

autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

10) è vietato comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

11) è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati.

Contratti

Nei contratti con i collaboratori esterni deve essere contenuta un'apposita clausola, che regoli le conseguenze della violazione, da parte degli stessi, delle norme di cui al Decreto, nonché dei principi contenuti nel Modello.

Istruzioni e verifiche dell'Organismo di Vigilanza

E' compito dell'OdV:

a) verificare l'emanazione e l'aggiornamento di istruzioni standardizzate, che devono essere scritte e conservate su supporto cartaceo o informatico, relative all'uso degli strumenti informatici e alla riservatezza nel trattamento dei dati
b) verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe in vigore, raccomandando le opportune modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali e/o al responsabile interno (o ai responsabili interni) o ai sub-responsabili interni
c) verificare periodicamente, con il supporto delle altre funzioni competenti, la validità delle clausole standard finalizzate:
    - all'osservanza da parte dei destinatari delle disposizioni del Decreto

- alla possibilità per la società di effettuare efficaci azioni di controllo nei confronti dei destinatari del modello, al fine di verificare il rispetto delle prescrizioni in esso contenute
- all'attuazione di meccanismi sanzionatori, quale ad esempio il recesso dal contratto nei riguardi di collaboratori esterni, qualora si accertino violazioni delle prescrizioni

d) esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi o da qualsiasi esponente aziendale, ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute