PARTE SPECIALE "C"

Applicazione del Modello con riguardo ai Delitti informatici

1. La tipologia dei delitti informatici (art. 24 bis del D.Lgs. n. 231 del 2001)

Si descrivono brevemente qui di seguito le singole fattispecie contemplate all'art. 24 bis del Decreto.

Accesso abusivo ad un sistema telematico o informatico (art. 615 ter c.p.)

Si tratta di reato la cui condotta tipica (per l' aspetto che ci interessa) riguarda chiunque si serva del proprio elaboratore, collegato alla rete telefonica, e riesca ad entrare in comunicazione con altri sistemi di comunicazione innestati sulla rete stessa, aggirando le misure di sicurezza previste dal titolare del sistema.
Tale fattispecie si realizza anche se non sono state aggirate misure di sicurezza particolari (sono sufficienti le normali protezioni), se vi si è introdotti senza l'assenso del titolare del sistema, se vi si permane allo stesso modo senza consenso o comunque contrariamente alla volontà espressa o tacita del titolare.
Per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche (art. 617 quater c.p.)

Si tratta di reato la cui condotta tipica riguarda chiunque intercetti, fraudolentemente, comunicazioni relative ad un sistema informatico o

telematico o intercorrenti con più sistemi ovvero le impedisca o le interrompa ; allo stesso modo si realizza il reato quando si riveli al pubblico, con qualsiasi mezzo di comunicazione, in tutto o in parte quanto appreso dalle suddette comunicazioni.
Il reato è aggravato se il fatto è commesso in danno di un sistema informatico o telematico utilizzato dallo Stato, da un ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, da un pubblico ufficiale o da un incaricato di pubblico servizio (con abuso di potere di servizio o con abuso della qualifica di operatore di sistema);
tali fattispecie si realizzano con la fraudolenza della condotta atta ad impedire la libertà e la riservatezza nelle nuove forme di comunicazione .
Per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni telefoniche o telematiche (art. 617 quinquies c.c.)

Il reato consiste nell'installare, fuori dai casi consentiti dalla legge, apparecchiature atte ad intercettare/impedire/interrompere comunicazioni relative ad un sistema informatico o telematico o intercorrente tra più sistemi.
Tali fattispecie si realizzano, come nell' articolo precedente, attentando alla libertà e alla riservatezza nelle nuove forme di comunicazione;
per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

Danneggiamento di sistemi informatici e telematici (art. 635 bis c.p.)

Il reato consiste nel distruggere/deteriorare/rendere inservibili in tutto o in parte, sistemi informatici o telematici altrui oppure programmi, informazioni o dati altrui (il reato è aggravato se commesso in qualità di operatore informatico oppure negli altri casi previsti nell' art. 635 c.2); tali fattispecie si realizzano attentando ai nuovi sistemi di comunicazione (di cui questo articolo assicura la tutela).
Per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

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.)

Il reato consiste nel distruggere/deteriorare/rendere inservibili in tutto o in parte, sistemi informatici o telematici oppure programmi, informazioni o dati utilizzati dallo Stato o da un altro ente pubblico o da un ente ad essi pertinente o comunque di pubblica utilità (il reato è aggravato se commesso in qualità di operatore informatico oppure negli altri casi previsti nell' art. 635 c.2 e se dal fatto deriva la distruzione o il deterioramento o la cancellazione o l' alterazione o la soppressione delle informazioni).
Tali fattispecie si realizzano attentando ai nuovi sistemi di comunicazione che riguardano lo Stato e gli enti suddetti (di cui questo articolo assicura la tutela); per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

Danneggiamento di sistemi informatici e telematici (art. 635 quater c.p.)

Il reato consiste, con le condotte esemplificate nell' art.635 bis, o con l'introduzione/trasmissione di dati, nel distruggere/deteriorare/rendere inservibili in tutto o in parte, sistemi informatici o telematici altrui o nell' ostacolarne gravemente il funzionamento (il reato è aggravato se commesso in qualità di operatore informatico oppure negli altri casi previsti nell' art. 635 c.2).
Tali fattispecie si realizzano attentando ai nuovi sistemi di comunicazione; per la sussistenza del reato è necessario anche il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 quinquies c.p.)

Il reato consiste, con le condotte esemplificate nell' art.635 quater, nel distruggere/deteriorare/rendere inservibili in tutto o in parte, sistemi informatici o telematici di pubblica utilità o nell' ostacolarne gravemente il funzionamento (il reato è aggravato se commesso in qualità di operatore informatico oppure negli altri casi previsti nell' art. 635 c.2 e se dal fatto deriva la distruzione o il deterioramento o la cancellazione o l'alterazione o la soppressione delle informazioni).
Tali fattispecie si realizzano attentando ai nuovi sistemi di comunicazione di pubblica utilità; per la sussistenza del reato è necessario an-

che il solo dolo generico ed è ammissibile la sola consumazione dello stesso (non è quindi configurabile il tentativo).

2. Aree a rischio

2.1 Individuazione delle aree a rischio

Nell'ambito della presente sezione sono definite "Aree a rischio" le aree aziendali in cui i soggetti afferenti, per lo svolgimento della propria attività, possono supportare la commissione di reati della presente Parte Speciale.
In considerazione del modello societario e di g*overnance* adottato da AnciLab sono state individuate le seguenti macroaree ritenute più specificamente a rischio per aree e funzioni:

AREA	FUNZIONE
Amministratore Unico e Direzione (apicalità sostanziale)	- Strategie aziendali - Acquisto partecipazioni in altre società - Relazioni con Enti Pubblici ed equiparati - Relazioni con enti non pubblici - Relazioni con enti di credito - Relazioni con i clienti - Selezione e valutazione di dipendenti, collaboratori e soggetti terzi in genere - Acquisizione, trattamento, gestione e finalità delle informazioni/dati in rete telematica/telefonica e con rete telematica/telefonica - Interconnessioni a reti telematiche/telefoniche di terzi - Operazioni di finanziamento - Ricerca, gestione e sviluppo di finanziamenti pubblici, agevolazioni e con-

	tributi - Operazioni societarie che possano incidere sulla integrità del capitale sociale - Informative e rapporti con gli organi di informazione e stampa - Investimenti ambientali, produzione, ricerca e innovazione tecnologica - Trattamento dati - Sicurezza sul lavoro
	- Contabilità - Redizione del bilancio, della relazione di gestione e di altre comunicazioni sociali - Gestione amministrativa contratti attivi - Gestione amministrativa contratti passivi - *Budgetting* e *reporting* - Gestione delle attività di segreteria - Gestione della comunicazione aziendale e delle attività promozionali - Operazioni societarie che possano incidere sulla integrità del capitale sociale - Informative e rapporti con gli organi di informazione e stampa - Gestione beni societari - Relazioni con Enti pubblici ed equiparati - Relazioni con Enti non pubblici - Gestione risorse finanziarie - Gestione flussi in entrata ed in uscita - Operazioni finanziamento - Ricerca, gestione e sviluppo di finan-

	ziamenti pubblici, agevolazioni e contributi - Investimenti ambientali, produzione, ricerca e innovazione tecnologica - Gestione di dipendenti, collaboratori e soggetti terzi in genere - Predisposizione contratti, lettere d'incarico (per fornitori, consulenze esterne, clienti, etc.) - Recupero Crediti - Acquisizione, trattamento, gestione e finalità delle informazioni/dati in rete telematica/telefonica e con rete telematica/telefonica - Interconnessioni a reti telematiche/telefoniche di terzi

Le funzioni considerate a rischio in relazione ai delitti informatici sono tutte quelle che utilizzano reti telematiche/telefoniche aziendali o di terzi e quelle che, all'interno di queste reti, utilizzano, immettono o trattano informazioni e dati.
Eventuali integrazioni delle suddette aree o funzioni a rischio potranno essere previste dall' Organo di amministrazione, anche con suggerimento del Collegio sindacale e dell'Organo di Vigilanza di AnciLab.

2.2 Aree a rischio - Principi generali del sistema organizzativo

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal presente Modello adottato da AnciLab, alla cui osservanza tutti gli amministratori e dipendenti della società sono tenuti.

Nell'espletamento delle operazioni della gestione sociale devono essere adottate e rispettate:

- le procedure aziendali, la documentazione, le disposizioni inerenti la struttura organizzativa gerarchico-funzionale e la normativa vigente;
- le norme inerenti il sistema informatico, amministrativo, contabile, finanziario e di controllo di gestione di AnciLab ;
- il Modello.

Il Modello, prevede l'espresso divieto di:

- porre in essere, collaborare o dare causa all'adozione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate (art. 24 bis del Decreto);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo in quanto idonei e diretti in modo univoco alla loro commissione;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

3. Destinatari della parte speciale – principi generali di comportamento nelle aree di attività a rischio

Destinatari della presente Parte Speciale "C" sono gli amministratori, il Revisore, i dirigenti ed i loro dipendenti/collaboratori in linea gerarchica, che operino nelle aree di attività a rischio (di seguito i "destinatari").

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, nella misura in cui possano essere coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di

condotta conformi a quanto prescritto al fine di prevenire ed impedire il commettersi di delitti informatici.

Ai destinatari è fatto espresso obbligo di:

a) tenere un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e regolamentari vigenti e delle procedure aziendali interne, nello svolgimento di tutte le attività eseguite con sistemi informatici o telefonici, al fine di garantire un uso appropriato delle apparecchiature informatiche/telefoniche, delle informazioni e dei dati in esse contenute o desunte ed un comportamento nella rete telematica/telefonica leale e rispettoso delle norme che regolano l' accesso, l' uso e la permanenza nelle stesse .

   In ordine a tale punto, è fatto specifico obbligo di:

osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità delle reti, delle informazioni, dei dati e di tutti i terzi con i quali si hanno relazioni informatiche/telefoniche e di agire sempre nel rispetto delle procedure interne aziendali, che su tali norme si fondano, al fine di non ledere le garanzie dei terzi in genere;

b) assicurare il regolare funzionamento di AnciLab , garantendo e agevolando ogni forma di controllo interno previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

   In ordine a tale punto, è fatto divieto di tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento delle attività di controllo o di revisione ;

c) effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità pubbliche di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

   In ordine a tale punto, è fatto divieto di:

   - omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, la tra-

smissione di dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;
- esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti ;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);

d) tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione.

4. Procedure per le aree a rischio

4.1 Individuazione dei responsabili delle aree a rischio reato

Occorre dare evidenza delle operazioni svolte nelle aree a rischio del precedente paragrafo; a tal fine gli amministratori ed i dirigenti responsabili delle funzioni, nelle quali sono svolte operazioni a rischio, sono responsabili di ogni operazione da loro direttamente svolta o attuata nell'ambito della funzione a loro facente capo (detti responsabili sono i soggetti referenti dell'operazione a rischio).
I controlli sulle operazioni in questione sono implementabili dal l'Organo di amministrazione di AnciLab in collaborazione con l'Organo di Vigilanza.

4.2 Individuazione dei processi per le aree a rischio reato

In riferimento alle aree e funzioni a rischio della presente Parte Speciale, i controlli interni si articolano in tutti i processi:

P.01	Processo commerciale

P.02	Processo acquisti
P.03	Processo di selezione, scelta e gestione dei collaboratori esterni
P.04	Processo di selezione, scelta e gestione dei dipendenti
P.05	Processo amministrativo (registrazione, redazione e controllo dei documenti contabili ed extra contabili) e finanziario

La procedura e le specifiche attività di ciascuno di tali processi sono esposte all'Allegato al Modello e ne costituiscono parte integrante;
le procedure sono strutturate a modello delle indicazioni previste dalla norma UNI EN ISO 9001:2008 e dal Trattamento dati, sia per uniformare le stesse al Sistema di Qualità adottato da AnciLab, sia perché tale schema ha il vantaggio di una facile comprensione.