– PARTE SPECIALE B –

REATI INFORMATICI

I REATI INFORMATICI

1. I reati informatici richiamati dall'articolo 24-bis del d.lgs. 231/2001 sono:

Documenti informatici (Art. 491-bis)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico, avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.

Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter)

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, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se 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;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) 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.
Qualora i fatti di cui ai commi primo e secondo 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 pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio[1].

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater)

Chiunque, al fine di procurare a sé 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, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro

[1] Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater[2].

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

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, e` punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

2. Le attività individuate come potenzialmente sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati informatici

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 24-*bis* del D. Lgs. 231/2001.

Di seguito sono elencate le attività sensibili o a rischio identificate con riferimento ai reati informatici:

- Formazione o falsificazione di un documento informatico privato o pubblico – Supporto Logistico e Tecnico
- Introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza – Gestione Sistemi Informativi e Telecomunicazioni

3. Il sistema dei controlli e i presidi a mitigazione dei rischi reato

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati informatici:

- Le Policy e i Regolamenti devono prevedere misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema informatico, al fine di prevenire modifiche non autorizzate, devono prevedere sistemi di protezione dei documenti elettronici e indicazioni comportamentali in materia

[2] Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

- Previsione all'interno di apposito Regolamento o procedura interna di indicazioni sulla gestione delle risorse informatiche e relative attività di monitoraggio.

- In divenire la sottoscrizione di un nuovo contratto di servizio con Phoenix per l'uso del sistema informativo.

4. Allegato – Matrice Processi - Reati 231

Tassonomia processi / Reati 231/2001		REATI INFORMATICI E DIRITTO D'AUTORE								
		Documenti informatici	Accesso abusivo ad un sistema informatico o telematico	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	Diffusione di apparecchiature dispositivi o programmi informatici diretti a danneggiare o interrompere sistemi informatici o telematici	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	Danneggiamento di informazioni, dati, programmi e sistemi informatici (anche utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità)	Frode informatica del soggetto che presta servizi di certificazione elettronica	Delitti in materia di violazione del diritto d'autore
GESTIONE SISTEMI INFORMATIVI E TELECOMUNICAZIONI	Insieme delle attività mirate al governo/ controllo della corretta operatività dei sistemi informativi e dell'infrastruttura di telecomunicazioni e all'evoluzione degli stessi, sulla base degli obiettivi strategici e di sviluppo perseguiti dalla banca.		X	X	X	X	X	X		X
FORMAZIONE	Gestione delle attività volte alla definizione e al soddisfacimento delle esigenze di apprendimento e sviluppo dei dipendenti dell'azienda, tramite l'individuazione delle esigenze formative, la progettazione e realizzazione di corsi di formazione, l'erogazione e la gestione della partecipazione agli stessi.									X
GESTIONE CONSERVAZIONE DOCUMENTI CARTACEI E INF	Insieme delle attività e procedure volte a presidiare la corretta conservazione di documenti cartacei e informatici (a uso interno, della clientela e delle autorità), finalizzato ad assicurare il mantenimento nel tempo delle caratteristiche di integrità, leggibilità e conformità alle norme dei documenti.	X								