MODELLO ORGANIZZATIVO

Ex. Art. 6 del D.Lgs. 231/2001

Parte Speciale “C”
Reati informatici

Revisione 0

Approvata dal Consiglio di Amministrazione
con delibera del 24 Settembre 2015

1. DETTAGLIO REATI

La presente parte speciale di riferisce ai "delitti informatici", così come richiamati dall'articolo 24-bis D.Lgs. 231/01 e di seguito descritti:

Falsità in documento informatico (art. 491-bis c.p.)
L'articolo in oggetto stabilisce la punibilità di tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale tra i quali rientrano sia le falsità ideologiche (quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere) che le falsità materiali (quando un documento non proviene dalla persona che risulta essere il mittente o da chi risulta dalla firma – contraffazione - ovvero quando il documento è artefatto - quindi, alterato - per mezzo di aggiunte o cancellazioni successive alla sua formazione) sia in atti pubblici che in atti privati, anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
Questo reato si configura quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, anche quando all'accesso non segua un vero e proprio danneggiamento di dati, ad esempio limitandosi ad eseguire una copia, oppure procedendo solo alla visualizzazione di informazioni.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo. I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche. Tale fattispecie si configura sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra li comunichi senza autorizzazione a terzi e chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
Tale reato si realizza qualora qualcuno, 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, procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici. Tale delitto potrebbe ad esempio configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
Tale ipotesi di reato si configura qualora fraudolentemente si intercettino comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero si impedisca o interrompa tali comunicazioni,

nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. La condotta vietata è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva. Il reato si integra, ad esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
Tale fattispecie di reato si realizza quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

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.)
Tale reato si realizza quando un soggetto 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.
Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha per oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.
Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.
Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
Questo reato si configura quando la condotta di cui al precedente art. 635-quater c.p. sia diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter c.p., quel che si rileva in primo luogo è che il danneggiamento deve avere per oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)
Questo reato si configura quando un soggetto che presta servizi di certificazione di Firma Elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Dal momento che l'Associazione non presta servizi di "certificazione o firma elettronica", l'ipotesi di reato non risulta applicabile.

2. PROCESSI SENSIBILI

Nell'ambito delle attività e dei processi di Croce Bianca Orbassano si sono identificate le seguenti condizioni di potenziale attuazione per cui uno o più tra i reati considerati in questa Parte Speciale.

Processo sensibile	Modalità di compimento
Gestione risorse – infrastruttura e processi informatici	Accesso abusivo ad un sistema informatico di terzi o appartenente alla rete interna per consultazione o danneggiamento di dati. Ottenimento indebito di codici di accesso Falsificazione di documento informatico avente efficace probatoria (nell'ambito delle registrazioni previste per i servizi di assistenza).

3. MISURE DI PREVENZIONE GENERALI

Tutti i destinatari del modello di organizzazione e gestione, secondo i propri ruoli e competenze devono attenersi ai seguenti principi di prevenzione generali:

- rispettare le indicazioni del Codice Etico in relazione alle condotte preventive in relazione ai reati elencati nella presente Parte Speciale, in particolare quanto riportato ai paragrafi riferiti a:
  - relazioni con la Pubblica Amministrazione
  - corretto utilizzo dell'infrastruttura informatica
  - relazioni con organi di vigilanza e controllo
  - tutela della riservatezza
  - relazioni con organi della giustizia

- mettere in atto le indicazioni contenute nel Modello Organizzativo-Parte Generale rilevanti per la prevenzione dei reati trattati nella presente parte speciale;
- rispettare le regole previste e comunicate sul flusso di comunicazione di documenti e dati verso l'Organismo di Vigilanza.

I referenti per le attività sensibili devono far rispettare le regole operative e comportamentali e garantire il corretto flusso di informazioni all'Organismo di Vigilanza.

4. MISURE DI PREVENZIONE SPECIFICHE

In aggiunta a quanto riportato nel paragrafo precedente, la prevenzione dei reati informatici prevede, nell'ambito del modello organizzativo di Croce Bianca Orbassano l'implementazione, l'attuazione ed il monitoraggio delle seguenti misure specifiche.

Misure di prevenzione e controllo relativa all'infrastruttura informatica

Devono essere rispettate le indicazioni previste all'interno del Documento Programmatico per la Sicurezza (redatto ai sensi del Decreto Legislativo 196/03 in tema di "privacy") e della procedura ISO sull'infrastruttura informatica. Le norme di prevenzione sono riferite a:

- gestione delle regole di backup dei dati e restore;
- gestione delle utenze di dominio protette da psw e delle conseguenti profilazioni utente
- attuazione delle misure contro il danneggiamento dei dati (firewall, antivirus);
- implementazione di iniziative informativo/formative rivolte agli incaricati al trattamento dei dati per l'applicazione di regole comportamentali corrette ed idonee, anche relative al corretto comportamento sul Web e per i device utilizzati;
- idonea custodia e protezione della documentazione cartacea ed elettronica.

Referente interno: Web Master / Amministratore di sistema