– 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)

L'art. 615-quater punisce chiunque al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo.

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

La fattispecie richiede che la condotta sia tenuta a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e-mail, da parte di chi, pur non essendo mosso da specifica finalità di lucro o di determinazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

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

L'art. 615-quinquies punisce chiunque abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, o i dati e i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
Tali fattispecie, perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in esame possono risultare propedeutiche.

Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.);

L'art. 635-bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.

Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a questi concessi in licenza dai legittimi titolari.

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.);

L'art. 635-ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte previste dall'articolo che precede dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano, pertanto, in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie prescindono dal prodursi in concreto del risultato del danneggiamento che, qualora si verificasse, costituirebbe circostanza aggravante della pena.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.

Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.);

L' art. 635-quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Il reato in oggetto si consuma quando il sistema su cui si è perpetrata la condotta criminosa risulta danneggiato o è reso, anche in parte, inservibile o ne risulta ostacolato il funzionamento.

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.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.);

L'art. 635-quinquies c.p. punisce le medesime condotte descritte nell'articolo 635-quater che mettano in pericolo sistemi informatici o telematici di pubblica utilità. La norma, a differenza di quanto previsto all'art. 635-ter, non fa riferimento all'utilizzo da parte di enti pubblici, essendo sufficiente che i sistemi aggrediti risultino "di pubblica utilità", anche se utilizzati da privati.

Entrambe le fattispecie prescindono dal prodursi in concreto del risultato del danneggiamento che, qualora si verificasse, costituirebbe circostanza aggravante della pena. Entrambe, inoltre, sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema.

È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora le prime rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615-ter c.p.

Frode informatica del soggetto che presta servizi di certificazione di firma

elettronica (Art. 640-quinquies c.p.);

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Documenti informatici (Art. 491-bis 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, contemplate e punite dagli articoli da 476 a 493 del Codice Penale. Si ricordano, in particolare, i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare meno ricorrente l'alterazione successiva alla formazione.

Il reato di uso di atto falso (art. 489 c.p.) punisce chi, pur non avendo concorso alla commissione della falsità, fa uso dell'atto falso essendo consapevole della sua falsità.

Tra i reati richiamati dall'art. 491-bis, sono punibili, altresì, a querela della persona offesa, la falsità in scrittura privata (art. 485 c.p.) e, se riguardano una scrittura privata, l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

Le condotte prese in esame possono essere ricondotte alle seguenti categorie:

- accesso illegale (intenzionalmente e senza diritto) a tutto o a parte di un sistema informatico;
- attentato all'integrità di un sistema informatico o telematico o dei dati in esso contenuti (danneggiamento, cancellazione, deterioramento, alterazione o soppressione) effettuato intenzionalmente e senza autorizzazione;
- uso intenzionale e senza autorizzazione (consistente nella produzione, vendita, ottenimento per l'uso, importazione, diffusione e in ogni altra forma di messa a disposizione) di dispositivi specialmente concepiti per consentire l'accesso a tutto o a parte di un sistema informatico (parole chiave, codici di accesso o strumenti analoghi) o che, comunque, possano favorire la commissione dei delitti sopraelencati;
- falsità riguardante un documento informatico pubblico o privato; frode realizzata da soggetto che presta servizi di certificazione di firma elettronica

al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno.

La pena per taluni dei reati indicati risulta aggravata nel caso in cui il comportamento illecito sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o, comunque, di pubblica utilità.

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:

a) Elaborazione, produzione e gestione di documenti informatici pubblici o privati rivolti alla clientela e/o terzi - Processo Gestione Sistemi Informativi e Telecomunicazioni
b) Introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza – Processo Gestione Sistemi Informativi e Telecomunicazioni
c) Gestione dei profili di accesso al sistema informatico o telematico – Processo Gestione delle misure di sicurezza dell'infrastruttura tecnologica

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:

a) Elaborazione, produzione e gestione di documenti informatici pubblici o privati rivolti alla clientela e/o terzi - Processo Gestione Sistemi Informativi e Telecomunicazioni

Presidi:

- Le Policy e i Regolamenti prevedono misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema informatico, al fine di prevenire modifiche non autorizzate, sistemi di protezione dei documenti elettronici e forniscono indicazioni comportamentali in materia;
- Rispetto dei principi previsti dal Regolamento di Sicurezza informatica e dal Regolamento di Sicurezza Utenti, emanati dalla Capogruppo CCB, che disciplinano i vari ambiti operativi degli utenti quali:
  - 2.1 CLEAR DESK AND CLEAN SCREEN POLICY;
  - 2.2 UTILIZZO DEI DISPOSITIVI DI INFORMATICA INDIVIDUALE;
  - 2.3 IDENTITA' ELETTRONICA;
  - 2.4 UTILIZZO DELLA POSTA ELETTRONICA;
  - 2.5 CONDIVISIONE DI DOCUMENTI ELETTRONICI (FILE SHARING E APPLICATION SHARING);
  - 2.6 USO DI INTERNET;
  - 2.7 INSTALLAZIONE DEI SOFTWARE;
  - 2.8 END-USER COMPUTING (EUC);
  - 2.9 UTILIZZO DEGLI STRUMENTI DI ARCHIVIAZIONE DI MASSA;
  - 2.10 ACCESSO DA REMOTO;
  - 2.11 ACCESSO DA RETI PUBBLICHE;
  - 2.12 UTILIZZO DEI DISPOSITIVI PERSONALI;
  - 2.13 UTILIZZO DEI SOCIAL MEDIA.

UO coinvolte:

- Direzione Generale
- Ufficio Organizzazione Tecnologie e Sistemi

b) Introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza – Processo Gestione Sistemi Informativi e Telecomunicazioni

Presidi:

- L'utilizzo del sistema informativo è messo a disposizione della Banca da parte di una società del Gruppo in funzione di uno specifico contratto di servizio, in cui sono indicati i servizi e i relativi SLA;
- Tracciabilità delle attività svolte dagli utenti con i sistemi informativi della Banca;
- Monitoraggio, nel rispetto di quanto disposto dallo statuto dei lavoratori e dal Decreto Legislativo 196/03 ("Codice Privacy"), circa gli accessi agli applicativi da parte di dirigenti e dipendenti;
- Creazione dei profili d'autenticazione degli utenti da parte della U.O. competente sulla base della richiesta di profilazione avanzata dall'Ufficio/Struttura di riferimento;
- Predefinizione dei livelli di navigazione in internet;
- Creazione dei profili d'autenticazione degli utenti da parte della U.O. competente sulla base della richiesta di profilazione avanzata dall'Ufficio/Struttura di riferimento;
- Il sistema dispone di un sistema di tracciatura dei log che consente il riscontro dell'accesso.

UO coinvolte:

- Ufficio Organizzazione Tecnologie e Sistemi

c) Gestione dei profili di accesso al sistema informatico o telematico – Processo Gestione delle misure di sicurezza dell'infrastruttura tecnologica

Presidi:

- Impossibilità nei sistemi della Banca di installare software o utilizzare dati provenienti da fornitori diversi da quelli autorizzati dall'azienda ovvero scaricati da internet in assenza di previa autorizzazione da parte dell'unità organizzativa preposta;

- Monitoraggio, nel rispetto di quanto disposto dallo statuto dei lavoratori e dal Decreto Legislativo 196/03 ("Codice Privacy"), circa gli accessi agli applicativi da parte di dirigenti e dipendenti;
- Creazione dei profili d'autenticazione degli utenti da parte della U.O. competente sulla base della richiesta di profilazione avanzata dall'Ufficio/Struttura di riferimento;
- Predefinizione dei livelli di navigazione in internet;
- Adozione del registro delle violazioni informatiche (data breach);
- Il sistema dispone di un sistema di tracciatura dei log che consente il riscontro dell'accesso.
- Rispetto dei principi previsti dal Regolamento di Sicurezza informatica e dal Regolamento di Sicurezza Utenti, emanati dalla Capogruppo CCB, che disciplinano i vari ambiti operativi degli utenti quali:
  - 2.1 CLEAR DESK AND CLEAN SCREEN POLICY;
  - 2.2 UTILIZZO DEI DISPOSITIVI DI INFORMATICA INDIVIDUALE;
  - 2.3 IDENTITA' ELETTRONICA;
  - 2.4 UTILIZZO DELLA POSTA ELETTRONICA;
  - 2.5 CONDIVISIONE DI DOCUMENTI ELETTRONICI (FILE SHARING E APPLICATION SHARING);
  - 2.6 USO DI INTERNET;
  - 2.7 INSTALLAZIONE DEI SOFTWARE;
  - 2.8 END-USER COMPUTING (EUC);
  - 2.9 UTILIZZO DEGLI STRUMENTI DI ARCHIVIAZIONE DI MASSA;
  - 2.10 ACCESSO DA REMOTO;
  - 2.11 ACCESSO DA RETI PUBBLICHE;
  - 2.12 UTILIZZO DEI DISPOSITIVI PERSONALI;
  - 2.13 UTILIZZO DEI SOCIAL MEDIA.

UO coinvolte:

- Ufficio Organizzazione Tecnologie e Sistemi