



TERRE DELLA ROCCA

PARTE SPECIALE B – REATI INFORMATICI



TERRE DELLA ROCCA

I REATI INFORMATICI

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

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

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.

Detenzione diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (Art. 615-quater c.p.)

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 ad un sistema protetto da misure di sicurezza, o comunque fornisce indicazioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater.

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.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies c.p.)

Chiunque, 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,



TERRE DELLA ROCCA

o l'alterazione del suo funzionamento, 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, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

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.

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

La condotta punita dall'art. 617-quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse.

Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.

L'impedimento o l'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware). L'impedimento od interruzione delle comunicazioni può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche, ad esempio, sovraccaricando il sistema con l'immissione di numerosissime comunicazioni artefatte.

Salvo che le condotte non siano state commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema, il reato è perseguibile a querela della persona offesa.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies c.p.)

L'art. 617-quinquies punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Tale fattispecie di reato prevede la reclusione da uno a quattro anni.

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.



TERRE DELLA ROCCA

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 ostacolano 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.



TERRE DELLA ROCCA

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.



TERRE DELLA ROCCA

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

1. Produzione e gestione di documenti informatici
2. Gestione misure di sicurezza sull'infrastruttura tecnologica
3. Distribuzione di apparecchiature / dispositivi per effettuare pagamenti digitali

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:

- Tracciabilità delle attività svolte dagli utenti con i sistemi informativi della Società;
- Impossibilità nei sistemi della Società 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 delle normative di settore e dalla normativa in materia di Privacy, circa gli accessi agli applicativi da parte di dirigenti e dipendenti;
- Osservanza dei principi enunciati nel Codice Etico che disciplina i comportamenti da tenere da parte di tutti i dipendenti e gli esponenti aziendali.

4. I flussi periodici per l'OdV 231

Al fine di rendere effettivo l'esercizio delle sue funzioni, l'Organismo di Vigilanza deve poter essere informato in merito a fatti od eventi che potrebbero ingenerare responsabilità della Società ai sensi del D. Lgs. n. 231/2001. È necessario che sia definito ed attuato un costante scambio di informazioni tra i destinatari del Modello 231 e l'OdV stesso.

In particolare, nel Modello 231 adottato vengono individuate due tipologie di flussi informativi diretti all'OdV:

- 1) **SEGNALAZIONI**, da inviare in caso di rilevazione di gravi comportamenti illegali (frode, corruzione, etc.) o più in generale di comportamenti non corretti nella conduzione del lavoro e degli affari in violazione del Modello 231.

Tutti soggetti coinvolti nelle attività sensibili sono, infatti, tenuti a segnalare tempestivamente all'OdV, tramite i canali informativi specificamente identificati:

- violazioni di leggi e norme applicabili;
 - violazioni, conclamate o sospette, del Modello o delle procedure ad esso correlate o degli elementi che lo compongono;
 - comportamenti e/o pratiche non in linea con le disposizioni del Codice Etico e delle Policy adottate;
 - eventuali deroghe alle procedure decise in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.
- 2) **FLUSSI INFORMATIVI PERIODICI**, richiesti dall'ODV alle singole Funzioni aziendali coinvolte nelle attività a rischio, relativi alle notizie rilevanti ed alle eventuali criticità individuate nell'ambito



TERRE DELLA ROCCA

dell'area aziendale di appartenenza, al fine di consentire all'Organismo stesso di monitorare l'insorgenza di attività sensibili, il funzionamento e l'osservanza del Modello.