PARTE SPECIALE

E

REATI INFORMATICI

INDICE

TESTO INTEGRALE DELLE NORME INCRIMINATRICI

EX D. LGS. N. 231/2001

REATI INFORMATICI

Frode informatica (art. 640 *ter* c.p.)

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

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.)

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.)

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

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

Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.)

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.)

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

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

Documenti informatici (art. 491 *bis* c.p.)

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.)

FRODE INFORMATICA

Art. 640 *ter* c.p.

1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

2. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

3. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

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 E DIFFUSIONE ABUSIVA DI CODICI DI 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, 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 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

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

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

Art. 617 *quater* c.p.

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) 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, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE

Art. 617 *quinquies* c.p.

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI

Art. 635 *bis* c.p.

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

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.

Salvo che il fatto costituisca più grave reato, chiunque 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, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI

Art. 635 *quater* c.p.

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 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 è punito con la reclusione da uno a cinque anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ

Art. 635 *quinquies* c.p.

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.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

DOCUMENTI INFORMATICI

Art. 491 *bis* c.p.

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

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.

Soggetti coinvolti e Controlli in essere

I soggetti coinvolti dalla presente Parte Speciale sono tutti gli utilizzatori di strumenti informatici.

Dalle informazioni e dai questionari ricevuti si evince l'esistenza di alcune prassi e/o procedure che definiscono le modalità di accesso ai terminali, le attività di protezione dei dati sensibili e le modalità di utilizzo dei sistemi informatici di GENERAL COM S.p.A..

A tale proposito si segnalano alcuni controlli in essere rilevanti ai fini del presente Modello di Organizzazione, Gestione e Controllo:

- è presente un responsabile della sicurezza informatica cui è affidata la gestione delle linee guida di accesso ai server, alle reti e ai *personal computer* nonché la verifica dei backup mensili;
- esiste una procedura di assegnazione ad ogni utilizzatore dei terminali di un nome utente e una password personale che prevede l'assegnazione di un *user-id* e di una *pssw* affidati al sistema *Active Directory* dei *server Microsoft Windows*;
- il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse di rete;
- tutte le password vengono modificate con cadenza mensile;
- i terminali per cui è prevista una condivisione di utilizzo consentono comunque di garantire la necessaria riservatezza poiché ogni utente accede al dominio con account proprio e deve obbligatoriamente effettuare il log-off ogni volta che si allontana dalla postazione.

Criticità e principi procedurali migliorativi

- Non sono previsti filtri in ingresso e uscita volti ad escludere l'accesso a determinati siti internet (contenuti sessuali, pedo-pornografici, siti di istigazione alla violenza, ecc...).
- Le password non sono conosciute esclusivamente dall'utente cui vengono attribuite, ma anche dal responsabile informatico.
- Non vi è la possibilità di monitorare eventuali tentativi di accesso a siti della pubblica amministrazione.
- Non è prevista un'adeguata e specifica formazione per illustrare i rischi di commissione dei reati informatici.
- Non vengono effettuate verifiche periodiche e/o a campione in merito al corretto utilizzo degli strumenti informatici e telematici da parte del personale interno/esterno all'ente.
- Non è prevista l'adozione di un regolamento informatico; tuttavia, dato l'esiguo numero di utenti, i programmi di firewall, gli antivirus e i filtri di protezione, è possibile risalire ai tracciati numerati per utente.

Alla luce di quanto esposto sinora, si ritiene opportuna la formalizzazione, sia delle procedure non adeguatamente formalizzate, sia delle prassi sopra indicate, oltre che l'attuazione - tramite l'utilizzo di apposite schede di evidenza - delle cautele e dei controlli di seguito indicati:

- adozione di adeguati programmi di formazione del personale, in merito al rischio di commissione dei reati informatici e alle conseguenze della loro commissione;

- previsione di verifiche periodiche e/o a campione sul corretto utilizzo degli strumenti informatici e telematici da parte del personale interno e dei collaboratori;
- monitoraggio dell'eventuale utilizzo di sistemi informatici di proprietà dell'azienda dati in utilizzo ai dipendenti o di sistemi di *cloud computing,* per i quali, comunque, deve essere effettuata specifica formazione;
- implementazione di un sistema di *filtering* in grado di limitare l'accesso a determinati siti catalogati come "*Black List*" (con particolare attenzione a siti contenenti materiale pornografico, di istigazione alla violenza, di istigazione all'uso di droghe, alcool e simili);
- definizione di un Regolamento Informatico da consegnare a tutti i dipendenti in cui siano esplicitati tutti i contenuti e i principi procedurali di cui alla presente Parte Speciale.