CONSORZIO SERVIZI BANCARI

PARTE SPECIALE

REATI INFORMATICI

ART. 24-*BIS*

INDICE

Paragrafo **Pagina**

1. FINALITA' DELLA PRESENTE PARTE SPECIALE

La presente Parte Speciale si riferisce alle fattispecie di reato espressamente richiamate dall'art. 24-*bis*, introdotto dall'art. 7 della Legge 18 marzo 2008 n. 48, recante la ratifica e l'esecuzione della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica (d'ora innanzi, per brevità, i "**Reati Informatici**") ed, in particolare, i comportamenti che devono essere tenuti dai soggetti che utilizzano gli strumenti informatici della Società.

Obiettivo della presente Parte Speciale è che, al fine di limitare il rischio circa il verificarsi dei Reati Informatici, i Soggetti Apicali e/o Sottoposti – nonché, più in generale, i Destinatari – adottino regole di condotta conformi a quanto prescritto, nonché a quanto previsto nel Modello contenente l'insieme dei diritti, doveri e responsabilità che devono essere rispettati da parte dei destinatari della presente Parte Speciale, al fine di agire in modo professionale e corretto e nel pieno rispetto della legge.

In particolare, nel prosieguo della presente Parte Speciale, si procederà a:

a) fornire i principi generali che i Soggetti Apicali e/o i Soggetti Sottoposti – nonché, più in generale, i Destinatari – sono tenuti ad osservare ai fini della corretta applicazione del presente Modello;

b) fornire all'OdV ed ai responsabili delle altre unità operative che con lo stesso interagiscono gli strumenti per effettuare le attività di controllo, monitoraggio e verifica previste.

2. LE FATTISPECIE DI REATO PREVISTE DALL'ART. 24-*BIS*, D. LGS. N. 231/01

Di seguito, il testo delle disposizioni del Codice Penale richiamate dall'art. 24-*bis* del Decreto, ritenute rilevanti per la Società, unitamente ad un breve commento delle singole fattispecie e all'esemplificazione delle possibili modalità di commissione di tali reati.

(i) 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 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".

L'art. 615-*ter* c.p., nel prevedere come reato l'accesso abusivo ad un sistema informatico o telematico, intende tutelare il c.d. "domicilio informatico", da intendersi come spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici di pertinenza della persona, il quale deve essere salvaguardato al fine di impedire non solo la violazione della riservatezza della vita privata, ma qualsiasi tipo di intrusione anche se relativa a profili economico-patrimoniali dei dati.

Il reato in questione è un reato comune, realizzabile ad opera di chiunque; la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato, operatore del sistema) integra la circostanza aggravante di cui al 2° comma, n. 1.

Quanto alla condotta penalmente rilevante, da un lato è punito colui che si introduce abusivamente, e cioè senza il consenso del titolare dello *ius excludendi*, in un sistema informatico o telematico munito di sistemi di sicurezza; dall'altro, è punito chi permanga in collegamento con il sistema stesso, nonostante il titolare abbia esercitato, sia pur tacitamente, lo *ius excludendi*.

L'accesso abusivo ad un sistema informatico o telematico può avvenire per acquisire informazioni o dati ovvero per manipolare i dati presenti nell'archivio elettronico, al

fine di conseguire un vantaggio o per fini meramente distruttivi. In ogni caso, il reato si consuma con il semplice accesso al sistema informatico o telematico.

La Suprema Corte ha affermato che la condotta integra gli estremi del reato in oggetto anche nel caso in cui l'agente acceda senza titolo ad una banca dati privata che non presenta meccanismi di protezione informatica: quello che rileva, infatti, è la volontà inequivocabile dell'avente diritto di escludere gli estranei dalla conoscenza dei dati ivi contenuti.

La disposizione contenuta nell'ultimo comma appresta una tutela più intensa, attraverso l'inasprimento della pena, a taluni sistemi informatici, che, per la funzione svolta e per il rilevante interesse pubblico, si appalesano come beni di primaria importanza.

(ii) Detenzione e diffusione abusiva di codici di accesso a sistema 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 a un anno e con la multa sino a € 5.164.*

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

La norma in esame completa la tutela prevista dalla disposizione precedente e punisce l'abusiva acquisizione in qualunque modo dei mezzi o codici di accesso, che consente a soggetti non legittimati di inserirsi nel sistema informatico o telematico altrui, vanificando l'ostacolo costituito dalle misure di protezione. Si tratta di un reato di pericolo, essendo la condotta prodromica rispetto ad altre condotte delittuose che possono consumarsi una volta superato l'ostacolo rappresentato dalle misure di protezione; il legislatore, infatti, ha agito nell'ottica di anticipare la soglia della punibilità rispetto all'effettivo conseguimento di un profitto.

La prima parte della disposizione descrive varie condotte atte ad integrare la fattispecie:

- "**procurarsi**" i mezzi di accesso ad un sistema, ovvero appropriarsi fisicamente della chiave meccanica o della scheda magnetica, oppure individuare i codici di accesso attraverso procedimenti logici tipici del computer, soprattutto quando la combinazione alfa-numerica è di semplice decodificazione;

- "**riprodurre**", nel senso di realizzare una copia abusiva di un codice di accesso, idonea all'uso;

[1] Le circostanze aggravanti previste dai numeri 1) e 2) del 4° comma dell'art. 617-quater c.p. ricorrono qualora 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*".

- "**divulgare**" a terzi del codice o della parola-chiave, mediante la diffusione, la comunicazione, la consegna, condotte che possono concorrere con il mero procacciamento.

Il reato in questione è un reato comune, realizzabile ad opera di chiunque; la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato, operatore del sistema) integra la circostanza aggravante di cui al 2° comma.

La fattispecie si configura in presenza del doloso conseguimento della disponibilità del dato utile all'ingresso abusivo nel sistema informatico e/ o telematico e dalla coscienza e volontà di entrarvi allo scopo di procurare a sé o ad altri un profitto.

(iii) 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 fino a € 10.329*".

La condotta criminosa si realizza attraverso comportamenti, quali il procacciamento, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione, la consegna o la messa a disposizione di terzi di programmi informatici virali, al fine di danneggiare illecitamente, o interrompere totalmente o parzialmente, o alterare, un programma informatico o telematico o i dati e le informazioni in esso contenute o ad esso pertinenti.

Trattasi di reato comune. Il momento consumativo del reato si verifica con la messa in atto delle condotte di diffusione, comunicazione o consegna: la mera realizzazione di un virus informatico, infatti, di per sé non ha rilevanza penale.

L'elemento soggettivo richiesto è il dolo generico.

(iv) 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*".

La norma prevede due distinte ipotesi criminose. La prima, prevista al 1° comma, consiste nell'intercettare, impedire o interrompere comunicazioni con e tra mezzi informatici o telematici. Per intercettazione si intende la presa di cognizione totale o parziale della comunicazione consistente nell'intromissione nel corso della comunicazione. L'interruzione si verifica quando la comunicazione sia iniziata e, successivamente, sia fatta cessare. L'impedimento, invece, esclude anche il mero inizio della comunicazione, rendendola impossibile.

La seconda ipotesi criminosa, prevista al 2° comma, consiste nella rivelazione di notizie illegittimamente apprese e deve essere rivolta al pubblico, per cui non costituiscono reato le comunicazioni personali e riservate.

La norma in esame intende proteggere la riservatezza delle comunicazioni effettuate tramite tutti i mezzi a distanza ed aventi ad oggetto suoni, immagini ed altri dati.

Il reato in questione è un reato comune, realizzabile ad opera di chiunque. Il 4° comma, tuttavia, prevede una serie di circostanze aggravanti, in presenza delle quali il delitto, perseguibile a querela delle persone offese nelle ipotesi contemplate dai primi due commi, diviene perseguibile d'ufficio con contestuale aumento della pena. Tali aggravanti riguardano la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato, operatore del sistema) o la qualità oggettiva del sistema informatico o telematico in danno del quale si agisce ("*utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità*").

Per quanto concerne il momento consumativo rilevano il tempo e il luogo in cui è avvenuta la captazione.

Per integrare la fattispecie prevista all'art. 617-*quater*, comma 1 c.p., è richiesto il requisito della fraudolenza ovvero una particolare intensità del dolo (generico) o l'uso di artifici o mezzi particolari, con l'obiettivo di rivelare il contenuto delle comunicazioni o conversazioni con qualsiasi mezzo di informazione al pubblico.

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

"*Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire od 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".

Il legislatore, con l'articolo in esame, ha inteso tutelare la sicurezza delle comunicazioni informatiche e telematiche.

Si tratta di un reato comune, di cui può rendersi responsabile chiunque.

La condotta consiste nell'installazione di strumenti idonei ad intercettare, impedire o interrompere le comunicazioni; non è necessario che questi strumenti vengano effettivamente utilizzati, essendo sufficiente la loro posa in opera e la loro attitudine agli scopi per i quali essi sono stati installati. La norma in esame richiede la concreta idoneità dell'apparecchiatura installata a realizzare le condotte delittuose sanzionate al presente articolo.

Il reato si consuma con il solo fatto di aver collocato gli apparati idonei agli scopi sopra indicati e, quindi, nel momento dell'installazione di detti sistemi.

(vi) 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[2] *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*".

La disposizione in commento punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime informazioni, dati o programmi informatici altrui.

E' reato comune ed è configurabile il tentativo.

L'elemento soggettivo richiesto è il dolo generico, consistente nella consapevolezza e volontà di distruggere, deteriorare, disperdere o rende inservibile (in tutto o in parte) i sistemi informatici e telematici altrui.

Il reato prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema. Al ricorrere di una delle aggravanti previste, il reato è perseguibile d'ufficio, altrimenti a querela.

(vii) 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.)

[2] L'art. 635, 2° comma, n. 1, c.p. prevede l'aumento della pena nel caso in cui il danneggiamento è commesso "*con violenza alla persona o con minaccia*".

"*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 il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti all'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante ai fini della pena. Deve però trattarsi di condotte 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.

Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

(viii) 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 il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma in esame punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-*bis* c.p., 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. Per dirsi consumato il reato in oggetto, il sistema su cui è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

(ix) 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 il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La norma in esame punisce le medesime condotte descritte nell'articolo che precede, ma che siano perpetrate su sistemi informatici o telematici di pubblica utilità. A tal proposito, si rileva che, a differenza del testo letterale dell'art. 635-*ter* c.p., questa norma non fa più alcun riferimento all'utilizzo dei sistemi informatici o telematici da parte di enti pubblici. Per la configurazione del reato in oggetto parrebbe, quindi, che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità". Non sarebbe, cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, dall'altro lato, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Il reato è perseguibile d'ufficio e prevede aggravanti di pena se i fatti sono commessi con violenza alle persone, minaccia o con abuso della qualità di operatore di sistema.

(x) Falsità di un documento informatico pubblico o privato avente efficacia probatoria (art. 491-*bis* c.p.)

"*Se alcune delle falsità previste da 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*".

L'articolo in esame 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, previste e punite dagli articoli da 476 a 493 c.p..

La Cassazione, infatti, ha ritenuto ininfluente la circostanza che i dati archiviati, oggetto di alterazione, siano anche presenti su supporti cartacei, valorizzando la definizione di "documenti informatici" racchiusa nell'articolo in oggetto.

Si citano, tra gli altri, 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.

Il reato è punibile a querela della persona offesa.

Il reato richiede, per la sua realizzazione, il dolo generico e deve riferirsi sia alle modalità della condotta (cosciente e volontaria manipolazione del sistema), che al perseguimento dell'oggetto materiale (coscienza e volontà di perseguire un profitto ingiusto con altrui danno).

3. LE SANZIONI PREVISTE IN RELAZIONE AGLI ART. 24-*BIS* D. LGS. N. 231/01

Con riferimento ai Reati Informatici descritti al precedente paragrafo 2, si riporta, di seguito, una tabella riepilogativa delle relative sanzioni previste a carico della Società qualora, per effetto della loro commissione da parte dei Soggetti Apicali e/o Sottoposti – nonché, più in generale, dei Destinatari – derivi alla Società un interesse o un vantaggio.

Reato	**Sanzione Pecuniaria**	**Sanzione Interdittiva**
- Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.) - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.) - Installazione di apparecchiature atte a 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.)	Da 100 a 500 quote	art. 9, comma 2, lett. a), b), e) - interdizione dall'esercizio dell'attività; - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; - divieto di pubblicizzare beni o servizi

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quate*r c.p.) - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.)	Fino a 300 quote	art. 9, comma 2, lett. b), e) - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; - divieto di pubblicizzare beni o servizi
- Documenti informatici (art. 491-*bis* c.p.)	Fino a 400 quote	art. 9, comma 2, lett. c), d), e) - divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; - esclusione da agevolazioni, finanziamenti, contributi o sussidi o eventuale revoca di quelli già concessi; - divieto di pubblicizzare beni o servizi

4. LE AREE A POTENZIALE RISCHIO REATO

Con riferimento alle fattispecie richiamate dall'art. 24-*bis* del D. Lgs. n. 231/2001 considerate applicabili alla Società (come sopra individuate), in considerazione della specifica attività svolta dalla stessa, sono individuate le principali attività sensibili, le funzioni aziendali coinvolte e le principali modalità di commissione dei medesimi reati.

--- OMISSIS ---

--- OMISSIS ---

--- OMISSIS ---

--- OMISSIS ---

5. NORME DI COMPORTAMENTO GENERALE NELLE AREE A RISCHIO REATO

Al fine di prevenire ed impedire il verificarsi dei Reati Informatici individuati al precedente paragrafo 2, i Soggetti Apicali e Sottoposti – nonché, più in generale, i Destinatari – che svolgono la propria attività nell'ambito delle Aree a Rischio Reato individuate al precedente paragrafo 4, sono tenuti al rispetto delle seguenti norme di comportamento generale, fermo restando quanto indicato nei successivi paragrafi 6 e 7:

1 astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato riportate nella presente Parte Speciale;
2 astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati indicati nella presente Parte Speciale, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

(i) introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;
(ii) accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
(iii) intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
(iv) utilizzare dispositivi tecnici o strumenti software (ad esempio, *virus*, *worm*, *troian*, *spyware*, *dialer*, *keylogger*, *rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
(v) distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
(vi) introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
(vii) detenere, procurarsi, riprodurre, o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
(viii) procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
(ix) alterare, mediante l'utilizzo di firma elettronica o comunque in qualsiasi modo, documenti informatici;
(x) produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o alterati.

6. I CONTROLLI AZIENDALI

Il sistema dei controlli aziendali identificato dalla Società con riferimento alle Aree a Rischio Reati Informatici, si fonda:

- sulle Norme di Comportamento Generale, di cui al precedente paragrafo 5;
- sui principi generali di controllo elencati nel seguito, con particolare riferimento alle disposizioni contenute nei protocolli elencati *sub* "Regolamentazione".

6.1 PRINCIPI GENERALI DI CONTROLLO

Tracciabilità

Al fine di assicurare l'adeguata tracciabilità dei processi operativi e decisionali nell'ambito delle Aree a Rischio Reato precedentemente indicate, tutti i Soggetti Apicali e/o Sottoposti, sono tenuti ad assicurare un'adeguata ricostruibilità ex post di ogni operazione effettuata.

Definizione dei poteri autorizzativi e di firma

Tutti i Soggetti Apicali, i Soggetti Sottoposti sono tenuti ad agire nel pieno rispetto del sistema di deleghe e poteri adottato dalla Società.

Segregazione dei compiti

Il sistema di attribuzione dei compiti della Società deve essere improntato al principio di segregazione dei poteri, in forza del quale ogni processo operativo o decisionale nell'ambito di ciascuna delle Aree a Rischio Reato precedentemente indicate è posto in essere mediante la condivisione delle specifiche attività tra più soggetti, secondo le rispettive competenze.

Informazione e Formazione

Le comunicazioni aziendali devono avvenire secondo un efficiente sistema di flussi informativi a tutti i livelli gerarchico-funzionali. I soggetti operanti per la Società devono essere messi in grado di conoscere e comprendere, attraverso adeguate e pertinenti attività di formazione, le disposizioni aziendali finalizzate a prevenire i rischi di commissione dei Reati Informatici.

Regolamentazione

Con riferimento alle Aree a Rischio Reato descritte al precedente paragrafo 4, e sulla base delle Norme di Comportamento Generale di cui al paragrafo 5, la Società ha adottato una serie di regole e procedure, alle cui prescrizioni devono attenersi tutti i Soggetti Apicali e/o Sottoposti, che operano nell'ambito delle Aree a Rischio precedentemente indicate.

--- OMISSIS ---

--- OMISSIS ---

--- OMISSIS ---

7. COMPITI DELL'ODV

Fermi restando i compiti e le funzioni dell'OdV statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati Informatici, lo stesso è tenuto ad effettuare specifici controlli e, periodicamente, controlli a campione sulle attività connesse ai processi sensibili descritti ai precedenti paragrafi di questa Parte Speciale, diretti a verificare la corretta implementazione delle stesse in relazione alle regole di cui al presente Modello.

A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.