MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001
DI
GROUPE SEB ITALIA S.P.A.

*****

PARTE SPECIALE D

I DELITTI INFORMATICI
I DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO
I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

Premessa. Funzione della Parte Speciale D

La presente Parte Speciale D ha l'obiettivo di illustrare i criteri e di regolamentare ruoli, responsabilità e norme comportamentali cui i Destinatari, come definiti nella Parte Generale, nonché gli altri soggetti tenuti al rispetto delle medesime regole, devono attenersi nell'ambito della gestione delle attività a rischio connesse con le seguenti fattispecie di reato:

(i) **Delitti informatici, richiamati dall'art. 24-*bis* d.lgs. 231/2001** (*cfr.* il successivo par. 2, §§ 2.1, 2.2, 2.3);

(ii) **Delitti contro l'industria ed il commercio, richiamati dall'art. 25-*bis.1* d.lgs. 231/2001** (*cfr.* il successivo par. 3, §§ 3.1, 3.2, 3.3);

(iii) **Delitti in materia di violazione del diritto d'autore, richiamati dall'art. 25-*novies* d.lgs. 231/2001** (*cfr.* il successivo par. 4, §§ 4.1, 4.2, 4.3).

Nello specifico, la presente Parte Speciale D ha lo scopo di:

- definire i protocolli e le procedure che i dipendenti ed i collaboratori della Società devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- supportare l'OdV ed i responsabili delle altre funzioni aziendali nell'espletamento delle attività di controllo, monitoraggio e verifica.

I contenuti della presente Parte Speciale D vanno messi in relazione con i principi comportamentali contenuti nelle *policy* aziendali e di gruppo e nei documenti di *compliance* specifici che indirizzano i comportamenti dei Destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive della Società e del Gruppo SEB.

2. Le fattispecie dei delitti informatici (art. 24-*bis* del d.lgs. 231/2001)

La prima categoria di reati trattata nella presente Parte Speciale D si riferisce alle fattispecie previste dall'art. 24-*bis* d.lgs. 231/2001, che vengono integralmente riportate qui di seguito:

Art. 491-*bis* c.p. – Documenti informatici
Testo dell'articolo: 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.

Art. 476 c.p. – Falsità materiale commessa dal pubblico ufficiale in atti pubblici
Testo dell'articolo: Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.
Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

Art. 477 c.p. – Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative

Testo dell'articolo: Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

Art. 478 c.p. – Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti

Testo dell'articolo: Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.
Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.
Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

Art. 479 c.p. – Falsità ideologica commessa dal pubblico ufficiale in atti pubblici

Testo dell'articolo: Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

Art. 480 c.p. – Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative

Testo dell'articolo: Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Art. 481 c.p. – Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità

Testo dell'articolo: Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00.
Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Art. 482 c.p. – Falsità materiale commessa dal privato

Testo dell'articolo: Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

Art. 483 c.p. – Falsità ideologica commessa dal privato in atto pubblico

Testo dell'articolo: Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.

Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

Art. 484 c.p. – Falsità in registri e notificazioni
Testo dell'articolo: Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

Art. 485 c.p. – Falsità in scrittura privata
Testo dell'articolo: Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

Art. 486 c.p. – Falsità in foglio firmato in bianco. Atto privato
Testo dell'articolo: Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.

Art. 487 c.p. – Falsità in foglio firmato in bianco. Atto pubblico
Testo dell'articolo: Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

Art. 488 c.p. – Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali
Testo dell'articolo: Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private.

Art. 489 c.p. – Uso di atto falso
Testo dell'articolo: Chiunque, senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.
Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.

Art. 490 c.p. – Soppressione, distruzione e occultamento di atti veri
Testo dell'articolo: Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute.
Si applica la disposizione del capoverso dell'articolo precedente.

Art. 492 c.p. – Copie autentiche che tengono luogo degli originali mancanti

Testo dell'articolo: Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

Art. 493 c.p. – Falsità commesse da pubblici impiegati incaricati di un servizio pubblico

Testo dell'articolo: Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

- ***Esempi di possibili modalità di commissione (con riferimento alle fattispecie appena elencate)***

- in generale, commissione da parte di dipendenti o collaboratori di GSI di azioni integranti una delle fattispecie di falso al fine di modificare un documento informatico avente efficacia probatoria;
- inserimento su memorie elettroniche, che comprovano operazioni economiche, di dati non conformi al vero;
- commissione, nel corso di rapporti privati con controparti contrattuali della Società (agenti commerciali, clienti, rivenditori, fornitori) condotti mediante strumenti espressivi informatici, di comportamenti finalizzati a comprometterne la genuinità;
- contraffazione del programma informatico, intesa come riproduzione senza autorizzazione dell'originale del programma, attraverso la realizzazione di: (i) copie servili (utilizzazione di un programma eseguibile, cui non si ha diritto di accedere, al fine di ottenere copie identiche all'originale); (ii) copie derivate (effettuate partendo da un programma sorgente, cui attingere per realizzare un nuovo programma con funzioni complementari all'originale).

Art. 615-*ter* c.p. – Accesso abusivo ad un sistema informatico o telematico

Testo dell'articolo:

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.

➢ *Esempi di possibili modalità di commissione*

- accesso abusivo nel sistema informatico di un concorrente di GSI al fine di conoscere l'offerta economica presentata per la partecipazione ad una selezione da parte di potenziali clienti pubblici o privati;
- accesso abusivo nel sistema informatico di un concorrente/cliente, al fine di conoscere informazioni riservate e/o sottrarre dati contenuti in tale sistema (anche se la sottrazione non sia materialmente avvenuta);
- accesso da parte di un dipendente ad aree del *server* aziendale, alle quali non potrebbe accedere attraverso il suo *username* e la sua *password*;
- riproduzione non autorizzata, in copia, di programmi aziendali e notizie riservate compiuto mediante accesso al sistema operativo aziendale di un concorrente/cliente;
- accesso senza titolo ad una banca dati privata contenente le notizie / informazioni contabili di un'azienda terza, anche se priva di chiavi di accesso o altre protezioni interne (essendo consuetamente indubitabile, pur in assenza di tali meccanismi di protezione, la volontà dell'avente diritto di escludere gli estranei).

Art. 615-*quater* c.p. – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
Testo dell'articolo: 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 € 5.164,00.
La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-*quater*.

Art. 615-*quinques* c.p. – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
Testo dell'articolo: 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 € 10.329,00.

➢ *Esempi di possibili modalità di commissione (con riferimento alle fattispecie appena elencate)*

- produzione, importazione, riproduzione e diffusione di apparecchiature, dispositivi o programmi finalizzati a danneggiare un sistema informatico o ad alterarne il funzionamento: condotte particolarmente insidiose in quanto vanno ad alimentare il mercato illecito attraverso l'introduzione dei dispositivi;
- un dipendente di GSI, venuto a conoscenza dei codici di accesso ad un sistema informatico di un cliente cui ha fornito dei servizi, li detiene o li diffonde abusivamente;
- un dipendente di GSI danneggia il sistema informatico della Società, al fine di distruggere i dati ivi contenuti e costituenti prove di illeciti ipoteticamente commessi da GSI;
- un dipendente/collaboratore si procura codici di accesso a sistemi informatici al fine di accedere al sistema interno o a sistemi di pertinenza di clienti per effettuare operazioni che portino vantaggi alla Società.

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

Testo dell'articolo: 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.

Art. 617-*quinquies* c.p. – Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche

Testo dell'articolo: 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*.

- ***Esempi di possibili modalità di commissione (con riferimento alle fattispecie appena elencate)***

- istallazione abusiva di c.d. *spyware*, vale a dire di *software* che permetta di acquisire le più svariate informazioni relative al sistema informatico attaccato;
- invio ad un *server* di posta elettronica di migliaia di messaggi fino a causarne il blocco o comunque un rallentamento che ne impedisca l'utilizzo;

- attacco ad un *server web* con sostituzione della pagina iniziale del concorrente / cliente con un'altra (c.d. *denial of service*);
- installazione abusiva di apparecchiature idonee ad interrompere le comunicazioni relative ad un sistema informatico, al fine di impedire la partecipazione di un concorrente ad una gara.

Art. 635 c.p. – Danneggiamento
Testo dell'articolo: Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa, con la reclusione fino a un anno o con la multa fino a € 309,00.
La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso:
1) con violenza alla persona o con minaccia;
(*omissis*)

Art. 635-*bis* c.p. – Danneggiamento di informazioni, dati e programmi informatici
Testo dell'articolo: 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.

Art. 635-*ter* c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
Testo dell'articolo: 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.

Art. 635-*quater* c.p. – Danneggiamento di sistemi informatici o telematici
Testo dell'articolo: 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.

Art. 635-*quinquies* c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità

Testo dell'articolo: 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.

➢ *Esempi di possibili modalità di commissione (con riferimento alle fattispecie appena elencate)*

- un dipendente della Società diffonde *virus* nel sistema informatico di una società concorrente al fine di danneggiarlo/renderlo inservibile;
- vengono installati abusivamente programmi la cui specifica finalità è quella del danneggiamento ovvero dell'alterazione di funzionamento di un sistema informatico altrui.

2.1 Attività sensibili nell'ambito dei delitti informatici

La principale area sensibile al rischio di commissione di delitti informatici rilevata presso la Società consiste nella gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricompresi i processi relativi a:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno;
- gestione e protezione delle reti;
- gestione degli *output* di sistema e dei dispositivi di memorizzazione;
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);

2.2 Principi procedurali per la prevenzione dei rischi di commissione dei delitti informatici in relazione alla realtà aziendale della Società

Con specifico riguardo alle problematiche connesse al rischio informatico, la Società, consapevole della continua evoluzione delle tecnologie applicabili e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si pone come obiettivo l'adozione di efficaci politiche di sicurezza informatica. In particolare, tale sicurezza viene perseguita attraverso: (i) la protezione dei sistemi e delle informazioni da potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire

e a reagire a fronte delle diverse tipologie di attacchi); (ii) la garanzia della massima continuità del servizio.

Di seguito sono elencati alcuni dei principi operativi da considerarsi applicabili sia ai collaboratori di GSI che a tutti i soggetti terzi che operano per conto della Società (consulenti esterni, *outsourcer,* fornitori di servizi di gestione e sviluppo di applicazioni *software* e di *data base* per la amministrazione delle forze vendita, ecc.).

A tutti i Destinatari del presente Modello (limitatamente agli obblighi contemplati, rispettivamente, nelle procedure aziendali e nelle specifiche clausole contrattuali) è fatto divieto di porre in essere comportamenti, collaborare o dare causa alla loro realizzazione, che possano rientrare nelle fattispecie di reato considerate ai fini dell'articolo 24-*bis* d.lgs. 231/2001.

Ai Destinatari è fatto, in particolare, divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici e privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di aziende concorrenti o di clienti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare un sistema informatico o telematico, di soggetti pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- modificare e/o cancellare dati, informazioni o programmi di soggetti privati o di soggetti pubblici o comunque di pubblica utilità;
- danneggiare informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i Destinatari sono tenuti a:

1. attenersi a quanto disposto dalla Procedura gestionale Autorizzazione accesso rete (GSI X04), nonché dalle *policy* e procedure aziendali del Gruppo SEB in materia di:
    - utilizzo del personal computer;
    - utilizzo della rete aziendale;
    - gestione delle *password*;
    - utilizzo dei supporti magnetici;
    - utilizzo dei PC portatili;
    - uso della posta elettronica, della rete internet e dei relativi servizi;
    - accesso ai sistemi IT finalizzato alla verifica di infrazioni procedurali o disciplinari del personale;
    - protezione dei dati personali e riservatezza del *know-how*;
2. attenersi rigorosamente alle prescrizioni in materia di acquisizione delle necessarie autorizzazioni interne e di gruppo ai fini dell'installazione di nuovi applicativi, in linea con le disposizioni e le indicazioni fornite dalla Direzione IT;
3. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di lavoro/ufficio;
4. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della Direzione IT;
5. in caso di smarrimento o furto, informare tempestivamente il responsabile della Direzione IT e presentare denuncia all'autorità giudiziaria;
6. accedere a messaggi o archivi presenti sui sistemi utilizzati dai propri collaboratori soltanto in caso di assenza o indisponibilità del collaboratore ed esclusivamente previa richiesta scritta da indirizzare al responsabile della Direzione IT;
7. in caso di necessità di accesso finalizzato alla verifica di infrazioni procedurali o disciplinari, procedere soltanto previa esplicita approvazione della Direzione Risorse Umane;
8. accedere a materiale presente in archivi non attivi (elettronici o cartacei) dei dipendenti esclusivamente previa esplicita approvazione della Direzione Risorse Umane;
9. procedere all'eventuale esame delle registrazioni degli accessi ai siti internet utilizzati dai dipendenti esclusivamente previa esplicita approvazione in forma scritta da parte della Direzione Risorse Umane;
10. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo nel caso in cui siano stati acquisiti con l'espresso consenso di questi ultimi, nonché applicazioni/*software* che non siano state

preventivamente approvate dal responsabile della Direzione IT o la cui provenienza sia dubbia;

11. evitare di trasferire all'esterno dell'azienda e/o di trasmettere *file*, documenti, o qualsiasi altra documentazione riservata di proprietà della Società o di altra società del Gruppo SEB, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio superiore gerarchico;
12. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.);
13. evitare l'utilizzo della *password* di altro utente aziendale, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile della Direzione IT. Qualora un utente venga a conoscenza della *password* di un altro utente, è tenuto a darne immediata notizia alla Direzione IT;
14. evitare l'utilizzo di strumenti *software* e/o *hardware* atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
15. utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
16. rispettare le procedure e gli *standard* previsti in materia di utilizzazione delle risorse (piattaforma SAP, altri applicativi) e delle infrastrutture (*server*, reti di dati, *security*) informatiche, segnalando senza ritardo eventuali utilizzi e/o funzionamenti anomali alle funzioni competenti per i servizi manutenzione degli applicativi e delle infrastrutture informatiche;
17. in ogni caso, attenersi scrupolosamente alle procedure applicabili in materia di richiesta di autorizzazione all'accesso ai sistemi informativi in base alla necessità aziendale, anche con riferimento al rispetto delle autorizzazioni da rilasciarsi da parte dei clienti per i servizi che necessitano l'accesso ai sistemi informatici di pertinenza di questi ultimi;
18. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
19. utilizzare l'apposito *software* di protezione fornito dalla Società, per l'accesso ad internet con *laptop* aziendali da remoto (tramite reti non GSI);
20. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

Nel Documento Programmatico sulla Sicurezza della Società, predisposto ai sensi del d.lgs. n. 196 del 30 Giugno 2003 (*Codice in materia di protezione dei dati personali*) sono analizzate le situazioni aziendali ed organizzati i protocolli a garanzia della sicurezza nell'ambito del trattamento dei dati personali da parte della Società.

In particolare, per quanto riguarda il rischio di commissione dei reati di cui alla presente Parte Speciale, rileva l'analisi di:

- *server* aziendali;
- misure di sicurezza per i trattamenti informatici;
- strumenti *antivirus*;
- sistemi anti-intrusione;
- *firewall*;
- piani di *Disaster Recovery*.

2.3 Ruolo dell'Organismo di Vigilanza

L'attività dell'Organismo di Vigilanza è svolta in stretta collaborazione con il responsabile della Direzione IT di GSI, nonché coordinandosi - per gli aspetti di competenza - con la Direzione Risorse Umane. In tal senso dovrà essere previsto un flusso informativo completo tra dette unità organizzative e l'Organismo di Vigilanza, al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

A titolo esemplificativo e non esaustivo, l'Organismo di Vigilanza:

- monitora l'adeguamento e l'aggiornamento costante delle suddette procedure alla luce dei principi di controllo espressi dalla presente Parte Speciale, con specifico riferimento al Documento Programmatico sulla Sicurezza *ex* d.lgs. n. 196 del 30 Giugno 2003 della Società;
- assicura che le misure attuate dalla Società ai fini della sicurezza dei dati trattati e della prevenzione di potenziali violazioni di diritti di terzi siano applicate adeguatamente presso la Società;
- promuove la corretta formalizzazione di adeguate procedure interne per la gestione degli accessi ai sistemi informatici e telematici, affinché le mansioni svolte da ciascun dipendente di GSI siano correlate in modo coerente ed obiettivo con le rispettive necessità di accesso ai suddetti sistemi e le richieste di accesso siano conseguentemente sottoposte ad autorizzazione da rilasciarsi sulla base di tali esigenze;

A tal fine, all'Organismo di Vigilanza deve essere garantito libero accesso a tutta la documentazione aziendale rilevante con riferimento alle attività sensibili qui considerate.

Tabella *Flussi informativi specifici a favore dell'OdV*

Ref	*Descrizione Flusso*	*Evidenza*	*Responsabile*	*Frequenza*

F1	Invio della lista completa degli applicativi IT installati nel periodo di riferimento	Testo e-mail con notifica di ricevimento	*Direzione IT*	Annuale
F2	Invio della lista completa delle eventuali richieste di accesso ai sistemi informatici e telematici in uso al personale, ai sensi delle procedure aziendali in vigore	Testo e-mail con notifica di ricevimento, con dettaglio delle motivazioni alla base di ciascuna richiesta	*Direzione Risorse Umane*	Annuale
F3	Trasmissione di segnalazioni relative ad abusi di qualunque tipo dei sistemi informativi interni in violazione della Procedura gestionale Autorizzazione accesso rete (GSI X04) e delle *IT policies* di gruppo, nonché a qualunque minaccia all'integrità ed alla sicurezza dei sistemi stessi	Testo e-mail con notifica di ricevimento	*Direzione IT*	Ad evento
F4	Rapporto sintetico sugli incidenti più significativi e/o anomali che abbiano interessato gli applicativi o le infrastrutture informatiche della Società nel periodo di riferimento	Testo e-mail con notifica di ricevimento	*Direzione IT*	Annuale

3. Le fattispecie dei delitti contro l'industria ed il commercio (art. 25-*bis.1* d.lgs. 231/2001)

La legge 23 luglio, n. 99 recante "*Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*" ha introdotto all'interno del d.lgs. 231/2001 - *inter alia* - l'art. 25-*bis.1*, rubricato "*Delitti verso l'industria e il commercio*", che punisce una serie di fattispecie, tra cui la frode nell'esercizio del commercio, la "frode alimentare", la contraffazione di indicazioni geografiche o denominazioni di origine.

Si riportano, qui di seguito, i reati richiamati dall'art. 25-*bis.1* che appaiono rilevanti nell'ambito della realtà aziendale specifica di GSI:

<u>Turbata libertà dell'industria o del commercio (art. 513 c.p.)</u>
La fattispecie di reato punisce chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio. La fattispecie tutela il normale esercizio dell'attività industriale o commerciale svolta dai soggetti privati.
Per "*violenza sulle cose*" si fa riferimento alla nozione contenuta nell'art. 392, secondo comma, c. p. secondo cui "agli effetti della legge penale, si ha violenza sulle

cose allorché la cosa viene danneggiata o trasformata o ne è mutata la destinazione".
Pertanto, si deve far riferimento a qualsiasi atto di modifica dello stato fisico delle cose, con o senza danneggiamento delle stesse.
In particolare, la cosa viene danneggiata quando è distrutta, dispersa o deteriorata; è trasformata quando è materialmente modificata anche se in senso migliorativo; ne è mutata la destinazione quando vi è un mutamento di destinazione soggettiva nei confronti di chi ne aveva la disponibilità o l'utilizzabilità.
Per "*mezzi fraudolenti*" devono intendersi quei mezzi idonei a trarre in inganno, quali artifici, raggiri, simulazioni, menzogne. Pertanto, la frequente realizzabilità del fatto tipico in funzione di atto di concorrenza ha indotto parte della dottrina a identificare i mezzi fraudolenti con i fatti descritti dall'art. 2598 c.c. e, dunque, per esempio nell'uso di altri marchi registrati, nella diffusione di notizie false e tendenziose, e in generale nella pubblicità menzognera e nella concorrenza parassitaria, vale a dire imitazione delle iniziative del concorrente in modo da ingenerare confusione.
La fattispecie delittuosa può rilevare anche in materia di concorrenza sleale, allorché il turbamento dell'altrui attività economica derivi da comportamenti posti in essere con inganno e illeciti artifici al fine di danneggiare l'attività stessa e sempre che l'uso dei mezzi fraudolenti non sia diretto ad assicurare un utile economico.
La condotta deve essere orientata all'impedimento o al turbamento dell'industria o del commercio.
Per "*impedimento*" si intende il non lasciar svolgere l'attività, sia ostacolandone l'inizio, sia paralizzandone il funzionamento ove sia già in corso.
Per "*turbamento*" si intende un'alterazione del regolare svolgimento dell'attività che può intervenire nel momento genetico o in fase funzionale.

Frode nell'esercizio del commercio (art. 515 c.p.)

La fattispecie di reato punisce chiunque, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.
La frode in commercio presuppone l'esistenza di un contratto: avendo, infatti, la legge fatto riferimento all'acquirente e non al compratore, può trattarsi di un qualsiasi contratto che produce l'obbligo di consegna di una cosa mobile (es. contratto estimatorio, di somministrazione, di permuta) e non solo la compravendita, la quale resta comunque la forma negoziale nel cui ambito più frequentemente si inserisce l'illecito. Tuttavia, la norma in esame, pur operando in un rapporto prettamente bilaterale, non fa riferimento agli interessi patrimoniali delle parti ma piuttosto alla buona fede negli scambi commerciali, a tutela sia del pubblico dei consumatori che dei produttori e commercianti.
Nel singolo atto di scambio disonesto si tutela l'interesse di tutta la comunità a che sia osservato un costume di onestà, lealtà e correttezza nello svolgimento del commercio.
Il delitto si consuma con la consegna della cosa, cioè la ricezione della cosa da parte dell'acquirente. La consegna si verifica non solo quando l'acquirente riceve materialmente la merce ma anche venga accettato un documento equipollente (lettera di vettura, polizza di carico, ecc.).

La cosa consegnata deve essere diversa rispetto a quella dichiarata o pattuita: questa diversità va individuata appunto in relazione al contenuto della dichiarazione ovvero della pattuizione.
La diversità "*per origine*" riguarda il luogo geografico di produzione di cose che ricevono un particolare apprezzamento da parte dei consumatori proprio per essere prodotte in una determinata zona o regione.
La diversità per "*provenienza*" concerne essenzialmente due ipotesi; la prima consiste nel contraddistinguere, con un'indicazione originaria, un prodotto diverso da quello originario mentre la seconda ipotesi consiste nell'utilizzare, nella confezione di un prodotto, l'attività di un'azienda diversa da quella che lo contraddistingue.
La diversità "*per qualità*" si ha quando si consegni una cosa dello stesso genere o della stessa specie di quella dichiarata o pattuita, ma inferiore per prezzo o utilizzabilità a causa di una differente composizione o di una variazione di gusto.
La diversità "*per quantità*" riguarda il peso, la misura o anche il numero.
Il capoverso dell'art. 515 c.p. prevede altresì una circostanza aggravante speciale, che concerne la frode di oggetti preziosi, intendendosi per tali tutte le cose che per la loro rarità, per pregio artistico, storico, per antichità hanno un valore venale superiore rispetto all'ordinario.
Per effetto della disposizione dell'art. 518 c.p., la condanna comporta la pubblicazione della sentenza.

<u>Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)</u>
La norma punisce chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.
L'incriminazione ha natura sussidiaria perché è punita solo se il fatto non è previsto come reato da altra disposizione di legge.
Il bene tutelato dalla disposizione è la buona fede e la correttezza commerciale, la cui violazione è considerata pericolosa per gli interessi della gran parte dei consumatori.
La messa in vendita o in circolazione delle opere dell'ingegno o dei prodotti deve avvenire con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.
Per "*marchi o segni distintivi nazionali o esteri*" si intendono segni emblematici o nominativi usati dall'imprenditore per contraddistinguere un prodotto ovvero una merce.
Non occorre tuttavia che i marchi siano registrati in quanto l'art. 517 c.p., a differenza dell'art. 474 c.p., non prescrive la previa osservanza delle norme sulla proprietà industriale. Il marchio può essere altresì di gruppo, in quanto indicante la provenienza dei prodotti da tutte le imprese collegate.
Per "*nomi*" di intendono le denominazioni che caratterizzano il prodotto all'interno di uno stesso genere.
Tutti i contrassegni italiani e stranieri devono essere idonei a ingannare il compratore: questa attitudine va valutata in rapporto alle abitudini del consumatore medio nell'operare gli acquisti.
L'inganno deve riguardare l'origine, la provenienza o la qualità dell'opera o del prodotto, per i quali si rinvia a quanto già descritto con riferimento all'art. 515 c.p..
La condanna comporta la pubblicazione della sentenza.

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)

La norma incriminatrice condanna, salva l'applicazione degli articoli 473 e 474 c.p., chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso nonché colui che, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni sopra descritti.

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)

La norma punisce chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia. La pena è aumentata se gli atti di concorrenza riguardano un'attività finanziata in tutto o in parte e in qualsiasi modo dallo Stato o da altri enti pubblici.

La norma citata si riferisce a quei comportamenti che, per essere attuati con violenza o minaccia, configurano una concorrenza sleale che si concretizza in forme di intimidazione, che tendono a controllate le attività commerciali, industriali o produttive, o comunque a condizionarle.

Infatti, la fattispecie delittuosa è stata introdotta dal legislatore per sanzionare la concorrenza attuata con metodi mafiosi; pertanto, è tipizzato il ricorso a forme tipiche di intimidazione proprie della criminalità organizzata che, con metodi violenti o minatori, incide sulla fondamentale legge della concorrenza del mercato, destinata a garantire il buon funzionamento del sistema economico e, di riverbero, la libertà delle persone di determinarsi nel settore.

Il reato può essere commesso da chiunque agisca nell'esercizio di un'attività commerciale, industriale o comunque produttiva.

"Commerciale" è ogni attività di interposizione nella circolazione dei beni, "industriale" è ogni attività diretta a produrre beni o servizi e "produttiva" è ogni attività economicamente orientata alla predisposizione e all'offerta di prodotti o servizi su un certo mercato.

E' previsto un aggravamento di pena qualora gli atti di concorrenza concernono attività finanziate con pubblico denaro. La *ratio* della circostanza aggravante è individuata nell'esigenza di rafforzare la tutela delle attività finanziate con pubblico denaro, le quali presentano una rilevante utilità sociale. Ulteriormente, l'aggravamento si giustifica in ragione del dato criminologico secondo il quale le organizzazioni criminali, quando si inseriscono in attività commerciali o produttive, privilegiano proprio i settori sorretti dal finanziamento pubblico e tendono ad assumere una posizione di monopolio nell'assorbimento del pubblico denaro.

Frodi contro le industrie nazionali (art. 514 c.p.)

La norma incriminatrice punisce la vendita o messa altrimenti in circolazione, sui mercati nazionali o esteri, di prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, tali da cagionare un nocumento all'industria nazionale.

Le condotte di porre in vendita e immettere nei circuiti di distribuzione attengono all'attività di commercializzazione, di produzione e di distribuzione, quale appendice necessaria all'attività di produzione.

Accanto alla previsione dei marchi e segni distintivi, la norma incriminatrice annovera anche i "nomi", identificabili come quelle indicazioni come denominazioni, insegne,

emblemi, firme, ecc., apposte per contrassegnare i prodotti ma non facenti parte del marchio.
Il nocumento all'industria nazionale, elemento costitutivo dell'art. 514, può assumere la forma di qualsiasi pregiudizio recato all'industria nazionale, come ad esempio la diminuzione di affari in Italia o all'estero, il mancato incremento degli affari, l'offuscamento del buon nome della società in relazione al prodotto in questione o alla correttezza commerciale.
Il delitto si considera consumato nel momento e nel luogo in cui si è verificato il nocumento. Pertanto, si colloca in Italia la consumazione, anche se il commercio è realizzato su mercati esteri, purché gli effetti si ripercuotano, pregiudicandolo, sul potenziale economico nazionale.

3.1 Le attività sensibili nell'ambito dei delitti contro l'industria e il commercio

L'analisi dei processi di GSI ha consentito di individuare le seguenti aree di attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-*bis.1* d.lgs. 231/2001:

- Definizione e attuazione delle politiche commerciali;
- Gestione delle attività inerenti alla diffusione di notizie/informazioni e/o alla pubblicità relativa ai prodotti del Gruppo SEB;
- Commercializzazione dei prodotti del Gruppo SEB.

3.2 Principi procedurali per la prevenzione dei rischi di commissione dei delitti informatici in relazione alla realtà aziendale della Società

Di seguito sono elencati alcuni dei principi operativi da considerarsi applicabili sia ai collaboratori della Società che a tutti i soggetti terzi che operano per conto della Società stessa (es., *outsourcer* di qualsiasi tipologia: consulenti del lavoro, gestori dei punti di assistenza specializzati nei servizi di *customer service*, fornitori di servizi di stoccaggio dei prodotti destinati alla vendita, ecc.):

- La Direzione Commerciale assicura la piena identificazione dei ruoli e delle responsabilità dei soggetti/funzioni aziendali di GSI coinvolte nella definizione della politica commerciale relativa alla distribuzione dei prodotti del Gruppo SEB.
- La Società garantisce la puntuale regolamentazione delle modalità operative finalizzate a: (i) la definizione della politica commerciale relativa alla distribuzione dei prodotti del Gruppo SEB; (ii) le attività e i controlli effettuati; (iii) le modalità di autorizzazione della politica commerciale;
- E' assicurata la segregazione delle responsabilità tra chi autorizza, chi esegue e chi controlla le attività relative alla definizione ed attuazione della politica commerciale relativa alla distribuzione dei prodotti del Gruppo SEB;

- E' inoltre assicurata la predisposizione, registrazione e archiviazione di tutta la documentazione alla base della definizione della suddetta politica commerciale, al fine di consentire la ricostruzione di tutte le fasi del processo.
- La gestione delle attività inerenti alla diffusione di notizie e/o alla pubblicità relativa ai prodotti del Gruppo SEB, inclusi i rapporti con i *Mass Media* ed i c.d. rapporti istituzionali, viene effettuata in piena conformità con le *policy* di riferimento e con le prassi generalmente applicabili nell'ambito del Gruppo SEB.
- E' assicurata, anteriormente alla distribuzione dei prodotti del Gruppo SEB sul territorio italiano, la scrupolosa verifica da parte della Direzione Logistica, in coordinamento con la Direzione Marketing, in ordine all'origine, provenienza, qualità dei prodotti importati in Italia e destinati alla distribuzione sul territorio nazionale.
- La Direzione Logistica, in coordinamento con la Direzione Marketing, prevede le modalità ed i controlli di completezza, correttezza ed idoneità della documentazione tecnica di accompagnamento a ciascun prodotto/componente ricevuto presso la sede di GSI, ai fini della successiva messa in vendita sul territorio italiano.
- Ai fini di quanto sopra, all'atto della ricezione dei campioni di prodotti del Gruppo SEB destinati alla commercializzazione in Italia, le funzioni competenti assicurano la compilazione ed accurata archiviazione e conservazione di apposite schede-prodotto, complete di tutte le informazioni relative all'origine, provenienza, e qualità dei prodotti stessi.
- Nel momento in cui la Società viene in contatto con soggetti terzi ai fini della distribuzione in Italia dei prodotti del Gruppo SEB, vengono adottate tutte le misure necessarie ad evitare:

  (i) che vengano commessi atti che, traducendosi in violenza e/o minaccia, possano produrre una lesione degli altrui diritti al libero esercizio dell'industria o del commercio, ed alla libera concorrenza;

  (ii) che possano essere acquisiti, e - soprattutto - che possano essere ceduti a terzi da parte di GSI prodotti non conformi alle caratteristiche indicate o pattuite, contraffatti, contraddistinti da segni mendaci e/o lesivi di altrui diritti di privativa.
- E' fatto, in generale, obbligo di:

  (i) effettuare, nella instaurazione di rapporti commerciali, attivi o passivi, tutte le verifiche richieste da regolamenti, protocolli e procedure che disciplinano l'attività aziendale, o che appaiano comunque opportune in ragione delle caratteristiche soggettive del soggetto terzo con cui la Società venga in contatto, e delle caratteristiche oggettive della prestazione oggetto del rapporto negoziale;

  (ii) astenersi da qualsiasi comportamento nei confronti di clienti, Mass Media e soggetti concorrenti della Società che possa integrare una violenza o una minaccia, ed in genere da comportamenti non conformi alla correttezza professionale idonei a creare indebiti effetti distorsivi della concorrenza;
- A ciascun cliente deve essere attribuita una specifica posizione nel sistema informatico (cd "anagrafica"), previa verifica dei necessari requisiti soggettivi, sotto il profilo della affidabilità ai fini del d.lgs. 231/2001.

Sono requisiti di ordine generale del cliente:

(i) la "*correntezza*", intesa come esistenza e capacità di agire del soggetto fisico o giuridico e l'esistenza a suo carico dello stato di liquidazione, o di procedure concorsuali, di divieti di contrattare con la Pubblica Amministrazione, ovvero di un procedimento volto a determinare l'insorgenza di tali situazioni;

(ii) l'assenza a carico di amministratori ed institori, soci, responsabili tecnici della fornitura, di sentenze di condanna passate in giudicato ovvero di patteggiamento per reati che incidano sulla moralità o sulla condotta professionale, o comunque connessi allo svolgimento di attività di criminalità organizzata o di riciclaggio; si considera sempre incidente sulla moralità e condotta professionale la commissione dei reati contemplati dal d.lgs. 231/2001;

(iii) l'assenza a carico dell'impresa di sanzioni per responsabilità amministrativa da reato ai sensi del d.lgs. 231/2001;

(iv) l'assenza di misure interdittive antimafia;

(v) la sussistenza delle autorizzazioni di legge per la costituzione e/o l'esercizio delle attività;

(vi) lo svolgimento da parte del cliente di attività effettiva corrispondente all'oggetto sociale, e la corrispondenza all'oggetto sociale del contenuto dei rapporti negoziali tra il fornitore e la Società.

3.3 Ruolo dell'Organismo di Vigilanza

Le Direzioni aziendali a qualsiasi titolo coinvolte nei processi commerciali e in quelli relativi all'importazione commercializzazione sul territorio nazionale dei prodotti del Gruppo SEB, nel corso delle attività operative ed in relazione alle responsabilità assegnate, trasmettono all'Organismo di Vigilanza, secondo la periodicità individuata da quest'ultimo, tutte le informazioni necessarie allo svolgimento delle seguenti attività di monitoraggio:

- identificazione dei rischi connessi alle operazioni svolte (violazione di normative aziendali, inefficienze di processo, commissione di reati rilevanti ai fini del d.lgs. 231/2001, ecc.);
- adozione di misure idonee a mitigare i rischi rilevati;
- verifica dell'efficacia dei controlli e del eventuale aggiornamento;
- verifica della presenza di eventuali criticità dei processi per le quali si rendano necessari interventi correttivi che esulano dai poteri assegnati alle funzioni competenti.

4. Le fattispecie dei delitti in materia di violazione del diritto d'autore, richiamati dall'art. 25-*novies* d.lgs. 231/2001. Esemplificazioni di condotte criminose rilevanti in relazione alla realtà aziendale di GSI

L'art. 25-*novies* d.lgs. 231/2001 contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (di seguito, "**L.A.**") e, in particolare, dagli artt. 171, 171-*bis*, 171-*ter*, 171-

septies e 171-*octies* di tale normativa, quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Da un'analisi preliminare è emersa l'immediata inapplicabilità alla Società delle fattispecie di cui agli artt. 171-*ter*, 171-*septies* e 171-*octies* L.A.

Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie richiamate dall'art. 25-*novies* ritenute *prima facie* teoricamente rilevanti per la realtà di GSI, previste dagli artt. 171 e 171-*bis* L.A..

1 ***Art. 171 comma 1 lett. a-bis e comma 3, L.A.*** - In relazione alla fattispecie delittuosa di cui all'art. 171, il d.lgs. 231/2001 ha preso in considerazione esclusivamente due fattispecie, ovvero:

(i) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa;

(ii) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete. Nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, bensì il suo onore e la sua reputazione.

➢ ***Esempio***

Tale reato potrebbe teoricamente essere commesso nell'interesse della Società qualora contenuti coperti dal diritto d'autore (loghi, marchi, *slogan*, ecc.), facenti capo ad operatori commerciali terzi ovvero a soggetti privati, vengano utilizzati illecitamente, direttamente da GSI ovvero da parte o per il tramite di operatori terzi specializzati operanti in regime di *outsourcing*, all'interno di offerte di carattere promozionale connesse ai prodotti della Società, nell'ambito delle comunicazioni e documentazione di varia tipologia dirette alla clientela.

2 ***Art. 171-bis L.A.*** - La norma è volta a tutelare il corretto utilizzo dei *software* e delle banche dati.

Per i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

La condotta rilevante è quella di chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.
Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.
Il secondo comma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.
Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

➢ *Esempio*

Tale reato potrebbe essere commesso nell'interesse della Società qualora vengano utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

4.1 Attività sensibili nell'ambito dei reati in materia di violazione del diritto d'autore

Le principali attività sensibili al rischio di commissione di delitti in materia di violazione del diritto d'autore rilevate presso la Società sono le seguenti:

- attività di predisposizione ed invio di offerte qualsiasi altra comunicazione e documentazione alla clientela (cataloghi dei prodotti, comunicazioni promozionali, ecc.);
- attività di stampa dei materiali promozionali/pubblicitari, svolta in *outsourcing* da agenzie di *Print Management*;
- gestione del sito internet della Società e del materiale promozionale di qualsiasi tipo (immagini, brani musicali, ecc.) caricato sul sito stesso a livello locale;
- gestione del sistema informatico e delle licenze *software*.

4.2 Principi procedurali per la prevenzione dei rischi di commissione dei reati sopra descritti in relazione alla realtà aziendale delle Società

GSI assicura la massima attenzione nell'ambito della gestione di materiale di qualsiasi tipologia protetto da diritto d'autore e/o da privative industriali, nell'ambito de: (i) propria attività promozionale/pubblicitaria; (ii) la gestione delle comunicazioni ai clienti finali; (iii) i rapporti con le proprie controparti commerciali e con i fornitori.

In tale ambito, in particolare:

- La Società assicura il pieno rispetto della normativa in materia di diritto di autore nell'ambito della programmazione, gestione ed esecuzione delle attività di predisposizione ed invio di offerte promozionali e di qualsiasi altra comunicazione e documentazione ai rivenditori e clienti finali.
- Nell'ambito dell'attività di predisposizione del materiale promozionale/ pubblicitario, le funzioni competenti garantiscono, in sede di assemblaggio dei *deliverable* finali, la corretta trasmissione ed applicazione delle specifiche in materia di utilizzo del materiale coperto da eventuali privative industriali e diritto d'autore.
- Nella gestione dei rapporti con le agenzie esterne incaricate dello sviluppo del lavoro creativo sulle campagne promozionali, le funzioni competenti garantiscono un attento monitoraggio (anche attraverso l'impartizione di apposite istruzioni alle agenzie esterne di *Print Management* di volta in volta coinvolte) sul corretto utilizzo di qualsiasi materiale identificativo/distintivo riconducibile a soggetti terzi.
- Analogo monitoraggio è garantito in sede di aggiornamento delle informazioni sul sito internet istituzionale della Società, con particolare riferimento ai messaggi e alle informazioni di carattere commerciale.

4.3 Ruolo dell'Organismo di Vigilanza in materia di monitoraggio sul rispetto della normativa in materia di diritto d'autore

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'OdV effettua periodicamente controlli a campione sulle attività sensibili descritte nel precedente paragrafo 4.1, diretti a verificare la corretta esplicazione delle stesse in relazione ai principi espressi nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante, con particolare riferimento alla gestione del materiale promozionale e pubblicitario e dei rapporti intrattenuti con gli operatori terzi incaricati dalla Società delle attività di stampa del materiale di cui sopra, della gestione dei rapporti con i *Mass Media*, della consulenza in materia di *marketing*, ecc..