PARTE SPECIALE

I. PREMESSA

1.1 Categorie di reati rilevanti

Al fine di dare attuazione al Decreto, si è reso necessario esaminare le singole fattispecie di reato dallo stesso richiamate e verificare quali di esse risultino applicabili alla Società e alle sue società di gruppo collegate.

Le fattispecie di reato per le quali, ai sensi degli artt. da 24 a 25 del Decreto, è prevista la responsabilità amministrativa sono state classificate nelle seguenti categorie (in relazione alle quali sono previste norme speciali in caso di delitti tentati, ai sensi dell'art. 26):

- **reati nei rapporti con la pubblica amministrazione** (in particolare, reati contro il patrimonio commessi in danno dello Stato o di altro ente pubblico e reati dei pubblici ufficiali contro la pubblica amministrazione) (artt. 24 e 25);
- **reati in falsità di monete, carte di pubblico credito e valori di bollo e in strumenti e segni di riconoscimento; (**art. 25-bis**);**
- **reati societari** (art. 25-*ter*);
- **reati con finalità di terrorismo ed eversione dell'ordine democratico** (art. 25-*quater*);
- **reati contro la personalità individuale** (in particolare, in materia di tratta delle persone) (art. 25-*quinquies*);
- **reati in materia di abusi di mercato** (art. 25-sexies);
- **reati transnazionali** (art. 10 della l. 146 del 2006);
- **reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (**articolo 9 della legge 3 agosto 2007, n. 123) (art. 25-septies);
- **reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio** (art. 25- octies);
- **reati in materia di crimini informatici e trattamento illecito dei dati** (artt. 24 bis);**.**
- **reati in tema di criminalità organizzata** (art. 24 ter);
- **reati in tema di violazione del diritto d'autore** (art. 25- novies);
- **reati in tema di delitti contro l'industria e il commercio (**art. 25-bis 1**);**
- **reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**(art. 25- decies)
- **reati ambientali**(art. 25- undecies)
- **reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25-duodecies)
- **reati di razzismo e xenofobia (**art 25- terdecies**)**
-

L'analisi delle fattispecie di reato è stata seguita dall'individuazione delle occasioni di reato nell'ambito dell'attività della Società e, conseguentemente delle aree e relative funzioni aziendali della Società a rischio, cioè di quelle nell'ambito delle quali gli illeciti possano essere commessi, allo scopo di effettuare una concreta valutazione del rischio-reato presente all'interno della Società.

In tale fase è stata esaminata sia l'attività della gestione caratteristica che le altre attività della Società e sono state determinate le seguenti possibili fattispecie di reato :

- **A -reati nei rapporti con la pubblica amministrazione** (artt. 24 e 25);
- **B -reati societari** (art. 25-*ter*);
- **C-reati in falsità di monete, carte di pubblico credito e valori di bollo e in strumenti e segni di riconoscimento; (**art. 25-bis**);**
- **D -reati in tema di delitti contro l'industria e il commercio (**art. 25-bis 1**).**
- **E -reati in materia di crimini informatici e trattamento illecito dei dati** (art. 24 bis);

- **F -reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** (art. 25-septies);
- **G -reati in tema di violazione del diritto d'autore** (art. 25- novies);
- **H - reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio** (art. 25- octies) (La sopravvenienza dei reati di autoriciclaggio con la Legge 186 del 15.12.2014 all'art. 3 comma 5 hanno suggerito l'opportunità di considerare la fattispecie possibile anche se remota per l'azienda.)

- **I - reati contro la personalità individuale (art. 25-*quinquies*);**

Non sono emerse fattispecie, neanche remote che potessero ricondurre a **reati con finalità di terrorismo ed eversione dell'ordine democratico** (art. 25-*quater*); **reati in materia di abusi di mercato** (art. 25-sexies); **reati transnazionali** (art. 10 della l. 146 del 2006); **reati in tema di criminalità organizzata** (art. 24 ter); **reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**(art. 25- decies) **reati ambientali** (art. 25- undecies) **reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25- duodecies) **reati di razzismo e xenofobia** (art 25 tredecies. Queste ultime fattispecie non sono trattate.

Infine, sono stati stabiliti i controlli da cui si evincono i protocolli, cioè gli obblighi e le procedure da osservare al fine di prevenire la commissione dei reati di cui trattasi.

La presente Parte Speciale si applica ai Destinatari operanti nelle aree di attività e relative funzioni aziendali a rischio, come di seguito individuate in relazione a ciascuna fattispecie ed occasione di reato di seguito illustrata.

I Destinatari hanno l'obbligo di adottare una condotta conforme alla presente Parte Speciale e comunque idonea ad impedire il verificarsi dei reati previsti nel Decreto.

In particolare, i Destinatari hanno il divieto di:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

1.2 Procedure aziendali

La Società si dota di un repertorio di procedure interne. Il repertorio include i seguenti documenti, nelle versioni di volta in volta vigenti, disponibili agli atti della Società ed accessibili da qualunque Destinatario che abbia legittimo interesse:

rapporti con il personale:

- procedura per la gestione dei viaggi aziendali e delle relative spese di rappresentanza;
- procedura relativa all'utilizzo della telefonia aziendale;
- procedura relativa all'assegnazione delle auto aziendali ai dipendenti;

rapporti con i clienti

- procedura per la gestione anagrafica dei clienti;
- procedura per la gestione del fido ai clienti:
- procedura relativa all'emissione di note di credito;
- procedura per lo sblocco degli ordini in sospeso;
- procedura di invito dei clienti ai congressi;
- procedura di incarico dei relatori a workshop scientifici;
- procedura di sponsorizzazione congressuale;

- procedura di installazione;
- procedura per la gestione dei reclami da parte dei clienti;
- procedura di gruppo per la gestione degli strumenti e delle parti di ricambio.

Per quanto riguarda la sicurezza informatica, la Società ha adottato

(i) la procedura generale per la gestione degli adempimenti normativi e quindi le misure di sicurezza per il trattamento informatico dei dati previste dal D.Lgs. 196/03, (ii) la procedura per la gestione della nomina del responsabile del trattamento ai sensi del D.Lgs. 196/2003;

(iii) la procedura per la gestione della nomina ad incaricato del trattamento ai sensi del D.Lgs. 196/2003;

(iv) la procedura per la gestione dell'informativa e del consenso ai sensi del D.Lgs. 196/2003; procedura per la gestione della vigilanza e controllo;

(v) la procedura per la gestione dei diritti dell'interessato ai sensi del D.Lgs. 196/2003;

(vi) le linee guida per l'utilizzo dei sistemi informatici aziendali;

(vii) la procedura per la gestione degli archivi cartacei ai fini del D.Lgs. 196/2003;

(viii) la procedura per la gestione dei supporti elettronici ai fini del D.Lgs. 196/2003;

(ix) la procedura generale per la gestione degli archivi cartacei e dei supporti elettronici ai fini del D.Lgs. 196/2003;

Le procedure interne sono caratterizzate dalla separazione delle funzioni di decisione, attuazione e controllo, con adeguata formalizzazione e documentazione delle fasi dei relativi processi funzionali.

La società per la propria organizzazione della qualità interna ha disposto le seguenti procedure

PR.01	Gestione delle Non Conformità, delle Azioni Correttive e Preventive
PR.02	Controllo dei Documenti e delle Registrazioni
PR.03	Conduzione di audit
PR.04	Analisi dei dati
PR.05	Monitoraggio della soddisfazione del cliente
PR.06	Formazione ed addestramento
PR.07	Offerte e Ordini o Contratti
PR.09	Evasione dell'Ordine
PR.10	Controllo degli strumenti di misura
PR.11	Approvvigionamento, valutazione dei fornitori e ricezione dei materiali
PR 13	Assistenza
PR 14	Assistenza Siemens
PR 15	Gestione macchine LAB.E.L.

1.3 Sistema delle deleghe e dei poteri di firma, regolamento di spesa

1.3.1 In generale

La Società si è dotata del sistema di poteri interni (cd. deleghe) ed esterni (cd. poteri di firma) illustrato nei documenti qui di seguito indicati, nelle versioni di volta in volta vigenti, disponibili agli atti della società ed accessibili da chiunque abbia legittimo interesse:

(i) Statuto

(ii) Organigramma con descrizione delle relative responsabilità funzionali (quello vigente alla data di adozione del presente Modello è riportato al paragrafo 2.0.3 della parte generale del Modello).

(iii) Poteri di firma (ad efficacia esterna)

1.3.2 Deleghe

Il sistema delle deleghe adottato dalla Società alla data di adozione del presente Modello è riportato nei documenti che si allegano sub **Allegato 1**. Tale allegato è aggiornato a cura dell'Organismo in caso di successive modifiche. Il sistema delle deleghe è caratterizzato dalla allocazione di ciascuna delega al soggetto dotato delle necessarie competenze.

1.3.3 Poteri di firma

Il sistema dei poteri di firma è in ogni momento caratterizzato dal conferimento di poteri di firma ai soggetti dotati delle necessarie competenze.

1.3.3.1 Poteri di firma operativi

La documentazione che riporta i poteri di firma operativi (per tali intendendosi tutti i poteri ad esclusione di quelli bancari) vigente alla data di adozione del presente Modello è allegata sub **Allegato 2**. Tale allegato è aggiornato a cura dell'Organismo in caso di successive modifiche.

1.3.3.2 Poteri di firma bancari

La documentazione che riporta i poteri di firma bancari vigente alla data di adozione del presente Modello è allegata sub **Allegato 3**. Tale allegato è aggiornato a cura dell'Organismo in caso di successive modifiche.

1.3.4 Gestione delle risorse finanziarie: regolamento di spesa

La Società si dota di un regolamento che disciplina le procedure per autorizzare l'esecuzione di qualsiasi pagamento da parte della Società e società del gruppo, in relazione ad operazioni a rischio per i fini del presente Modello, ispirato al principio generale che la funzione che autorizza l'esecuzione del pagamento o dell'incasso, previa verifica della sussistenza di adeguata causa ed evidenza documentale, sia diversa da quella che decide la relativa operazione.

II. A - REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

2.1 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

Il presente capitolo contiene il risultato delle analisi condotte dalla Società allo scopo di individuare le aree (processi) e funzioni aziendali sensibili, in quanto esposte al rischio di commissione di reati rilevanti ai fini del Decreto.

Per quanto riguarda l'identificazione delle aree a rischio, l'analisi è stata condotta mediante compilazione di apposito repertorio dei reati rilevanti ed identificazione delle relative aree (processi) e funzioni a rischio per ciascun reato rilevante.

Qualsiasi riferimento alla pubblica amministrazione include, oltre allo Stato ed alle sue amministrazioni, anche enti pubblici economici o non, organismi di diritto pubblico (imprese a partecipazione pubblica o controllate dallo Stato o comunque esercenti attività di interesse pubblico o di pubblica utilità) o altri soggetti privati i cui rappresentanti, esponenti aziendali o dipendenti possano essere qualificati pubblici ufficiali o incaricati di pubblico servizio ai sensi della normativa vigente.

I reati presupposto potenziali riscontrati in azienda ex art 24 sono:

- art 316 bis - Malversazione a danno dello Stato

- art 316 ter - Indebita percezione di erogazioni a danno dello Stato
- art. 640 comma 2 n° 1 - Truffa

2.1.1 Art. 316-bis c.p.
Malversazione in danno dello Stato

"Chiunque, estraneo alla P.A., avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee, contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni".

Fattispecie

Presupposto della condotta è l'avvenuta erogazione ad un determinato soggetto, da parte di un ente pubblico, di sovvenzioni, contributi o finanziamenti:

- a condizioni più favorevoli di quelle di mercato;
- in vista di un fine di pubblica utilità.

La condotta criminosa si sostanzia nella mancata destinazione delle risorse ottenute alle attività di pubblico interesse per le quali sono state concesse. La sussistenza del reato va esclusa nei casi in cui il finanziamento sia stato utilizzato per finalità diverse ma comunque di interesse collettivo.

Considerazioni applicative

Allo stato la Società ricorre a tali forme di erogazioni pubbliche e, conseguentemente, l' esposizione a tali aree di rischio è astrattamente ipotizzabile. Per completezza, esponiamo qui di seguito le occasioni di reato, i processi aziendali a rischio e le funzioni / aree aziendali a rischio.

Occasioni di reato

- indebito utilizzo o destinazione a scopi diversi di erogazioni pubbliche (nazionali e comunitarie, in forma di contributi, finanziamenti, mutui agevolati, altre erogazioni) ricevute dalla Società, ad esempio, per assunzioni di personale, per attività di formazione, per investimenti ambientali, per ricerca ed innovazione tecnologica, per adeguamento della sicurezza.

Processi aziendali a rischio:

Gestione ed utilizzo di aiuti pubblici previsti dalla normativa sul lavoro;

Gestione ed utilizzo di aiuti pubblici previsti dalla normativa fiscale;

Gestione ed utilizzo di aiuti pubblici previsti da specifici bandi;

Gestione ed utilizzo di aiuti pubblici previsti per lo sviluppo di progetti di ricerca.

Funzioni / Aree aziendali a rischio:

Consiglio di Amministrazione

Personale e Amministrazione e Finanza

2.1.2 Art. 316- ter c.p

Indebita percezione di erogazioni pubbliche in danno dello Stato o dell'Unione Europea

Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a e 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da e 5.164,00 a e 25.822,00. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Fattispecie

Per la commissione del reato si richiede che le somme ricevute a titolo di contributo, finanziamento o sovvenzione non siano dovute, in quanto manchino gli estremi per poter aspirare o pretendere di ottenerle e quindi manchi la giustificazione di un pubblico interesse.

Quanto all'elemento soggettivo, il dolo è generico e consiste nella coscienza e volontà di ottenere somme destinate a soddisfare un pubblico interesse pur non avendo titolo a richiederle e ad ottenerle.

Il reato avviene all'atto dell'ottenimento di erogazioni pubbliche non dovute.

Considerazioni applicative

Vale quanto detto per l'art. 316-bis cod. pen

Allo stato la Società ricorre a tali forme di erogazioni pubbliche e, conseguentemente, la esposizione a tali aree di rischio è concretamente ipotizzabile. Per completezza, esponiamo qui di seguito le occasioni di reato, i processi aziendali a rischio e le funzioni / aree aziendali a rischio

Occasioni di reato:

indebita percezione di erogazioni pubbliche (nazionali e comunitarie, in forma di contributi, finanziamenti, mutui agevolati, sovvenzioni, altre erogazioni) ricevute per qualsiasi fine e in particolare a scopo di ricerca per l'insediamento di attività produttive (ad es. per ristrutturazioni di immobili o per adeguamento della sicurezza) o per la assunzione o formazione del personale, ad es. mediante presentazione di documenti o dichiarazioni non veritiere od omissive.

Processi aziendali a rischio:

Gestione ed utilizzo di aiuti pubblici previsti dalla normativa sul lavoro;

Gestione ed utilizzo di aiuti pubblici previsti dalla normativa fiscale;

Gestione ed utilizzo di aiuti pubblici previsti da specifici bandi;

Gestione ed utilizzo di aiuti pubblici previsti per lo sviluppo di progetti di ricerca.

Funzioni / Aree aziendali a rischio: Amministratore Delegato

Consiglio di Amministrazione

Personale e Amministrazione e Finanza

2.1.3 Art. 640 c.p comma 2 n.1

Truffa ai danni dello Stato

"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un

ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da £ 51,00 a £ 1.032,00.

La pena è della reclusione da uno a cinque anni e della multa da £ 309,00 a £ 1.549,00:

1) ***se il fatto è commesso a danno dello stato o di altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;***
2) ***se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità.***

2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o altra circostanza aggravante*".*

Fattispecie

L'ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea). Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Considerazioni applicative

I reati sopra indicati appaiono astrattamente ipotizzabili per la Società.

Occasioni di reato

a) truffa in gare pubbliche o affidamenti diretti da parte di enti pubblici (es. ospedali, aziende sanitarie regionali, unità sanitarie locali) o, segnatamente, soggetti privati qualificabili come Organismi di Diritto Pubblico*)*, ad es. mediante produzione o predisposizione agli enti pubblici o agli Organismi di Diritto Pubblico di documenti o dati informazioni non veritiere (ad esempio supportate da documentazione artefatta) per la partecipazione a procedure di gara, al fine di ottenere l'aggiudicazione della gara stessa o al fine di evitare l'esperimento di gare pubbliche con conseguente affidamento diretto;
b) truffa nell'attività di negoziazione, stipulazione o esecuzione di contratti con incaricati di pubblico servizio (es. medici, etc.) ad esempio mediante produzione o predisposizione a tali soggetti di documenti o dati o informazioni non veritiere al fine di stipulare contratti di fornitura.
c) truffa nell'ottenimento di permessi per installare le macchine presso i laboratori degli ospedali e delle richieste di autorizzazione alla pubblica amministrazione in caso di collegamento on line della sede per la fornitura di assistenza tecnica remota.
d) truffa con consapevole omissione o alterazione negli adempimenti contributivi, previdenziali;
e) truffa nella trasmissione ad una struttura sanitaria di documentazione informativa concernente un prodotto della società che assicura determinate caratteristiche nel caso in cui l'ente viene indotto ad acquistare un notevole quantitativo di tale prodotto ma le caratteristiche si rivelano inesistenti;
f) Sovrafatturazione agli enti pubblici o agli incaricati di pubblico servizio sopra menzionati.

Processi aziendali a rischio:

Adempimenti Fiscali

Adempimenti Contributivi e Previdenziali

Partecipazione a procedure di gara d'appalto di enti pubblici (es. ospedali, aziende sanitarie regionali o locali) e di Organismi di Diritto Pubblico

Richiesta di permessi, licenze ed autorizzazioni alla PA

Fatturazione attiva agli Organismi di Diritto Pubblico

Funzioni/Aree a rischio:

Consiglio di Amministrazione

Personale e Amministrazione e Finanza

Marketing

Vendite

Sono ipotizzabili peraltro i seguenti altri due articoli tra quelli potenzialmente commettibili anche se non ipotizzati:

- Art. 640-bis Truffa aggravata per il conseguimento di erogazioni pubbliche
- Art. 640-ter Frode informatica

2.1.4 Art. 640-bis
Truffa aggravata per il conseguimento di erogazioni pubbliche

"La pena è della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'Art. 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità Europee".

Fattispecie

Per quanto concerne la fattispecie prevista dall'Art. 640-bis, si tratta di una truffa avente ad oggetto erogazioni pubbliche finalizzate alla realizzazione di opere o allo svolgimento di attività di interesse pubblico.

L'elemento di distinzione fra tale reato e quello, già esaminato, di malversazione in danno dello Stato, è stato individuato dalla Giurisprudenza nel fatto che nella malversazione la condotta punibile si sostanzia nel non aver destinato i fondi ottenuti alle finalità per le quali sono stati erogati, mentre in caso di truffa l'azione delittuosa consiste nell'essersi procurato con frode (mediante artifizi o raggiri) prestazioni alle quali non si avrebbe avuto diritto, non rilevando la differente destinazione dei fondi a scopi diversi da quelli per i quali sono stati concessi. *(v. Cass. Pen., Sez. I 98/ 211494).*

Considerazioni applicative

Il reato (delitto) è ipotizzabile per la Società. Vale, in via di principio, quanto detto sub art 640 cod. pen.

2.1.5 Art. 640-ter
Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da e 51,00 a e 1.032,00.

La pena è della reclusione da uno a cinque anni e della multa da euro 309,00 a e 1.549,00 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti
Il ***delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma*** e terzo o ***un'altra circostanza aggravante.***

Fattispecie

La condotta punibile può consistere sia in un intervento volto ad adibire il sistema informatico a scopi diversi da quelli per i quali esso è stato destinato (alterazione del funzionamento), sia nel manipolarne arbitrariamente i contenuti (intervento su dati, informazioni e programmi.

Ai fini della responsabilità ex Decreto n. 231, peraltro, il fatto deve essere commesso in danno dello Stato o di altro ente pubblico o di terzo.

Quanto all'elemento soggettivo, il dolo è specifico e consiste nella volontà di alterare il funzionamento dei sistemi o di intervenire su dati, programmi, informazioni, modifica dell'identità digitale con la previsione del profitto ingiusto e dell'altrui danno, senza che sia necessaria alcuna volontà di indurre altri in errore o di ingannare.

Considerazioni applicative

Il reato (delitto) interessa solo per la fattispecie di cui al secondo e terzo comma dell'art. 640-*ter* ed è astrattamente ipotizzabile per la Società, anche in relazione all'eventuale alterazione di flussi di informazioni e dati destinati agli Organismi di Diritto Pubblico ovvero alle Pubbliche Amministrazioni nell'ambito dei rapporti con esse ovvero nella manomissione della identità digitale di qualcuno .

Occasioni di reato

a) Frode realizzata attraverso collegamenti telematici o trasmissione di dati su supporti informatici a pubbliche Amministrazioni o ad enti pubblici, o ad Autorità di vigilanza (ad es. invio di materiale per gare in forma elettronica difforme dalle informazioni ufficiali trasmesse in forma cartacea);
b) Alterazione di registri informatici della P.A. per far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.) ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora per modificare dati fiscali / previdenziali di interesse dell'azienda (es. mod. 770), già trasmessi all'Amministrazione.
c) Alterazione di identità digitale di qualcuno sottraendo codici personali

Processi aziendali a rischio:

collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a Pubbliche Amministrazioni o ad enti pubblici o ad autorità di vigilanza per adempimenti fiscali o societari.

Funzioni / aree a rischio:

Personale e Amministrazione e Finanza
Vendite

I reati presupposto potenziali riscontrati in azienda ex art 25 sono:

- art 318 - Corruzione per l'esercizio della funzione
- art 319 - Corruzione per un atto contrario ai doveri d'ufficio
- art 319 quater - Induzione indebita a dare o promettere utilità
- art 320 - Corruzione di persona incaricata di pubblico servizio
- art 322 - Istigazione alla corruzione

Si applica ovviamente l'art 321 Pene per il corruttore

2.1.6 Art. 318 c.p.
Corruzione per l'esercizio della funzione

"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa, è punito con la reclusione da uno a sei anni.

Fattispecie

L'elemento determinante, e che distingue tra la concussione e la corruzione, è costituito dall'atteggiamento delle volontà rispettive del pubblico ufficiale e del privato e di conseguenza dal tipo di rapporto che si instaura tra i due soggetti: si ha infatti concussione quando il pubblico ufficiale strumentalizza la propria autorità e il proprio potere per coartare la volontà del soggetto, facendogli comprendere che non ha alternative rispetto alla richiesta, mentre si ha corruzione quando l'iniziativa è del privato, che si sforza di convincere il pubblico ufficiale a soddisfare le sue richieste.

Il reato si consuma nel momento in cui il pubblico ufficiale accetta la promessa o riceve la retribuzione indebita.

Considerazioni applicative

Il reato (delitto) è ipotizzabile per la Società, con la possibile seguente casistica.

Occasioni di reato

1. Nel caso della Società in veste di corruttore:
    a) Pressioni, sollecitazioni in ogni tipo di rapporto, anche per via mediata, con Pubbliche Amministrazioni e Organismi di diritto Pubblico, titolari del potere di assumere determinazioni favorevoli o sfavorevoli alla Società in relazione a:
        i. adempimenti INPS, INAIL, Ispettorato del lavoro
        ii. gare pubbliche per appalti o forniture, affidamenti diretti;
        iii. attività di negoziazione, stipulazione o esecuzione di contratti con enti pubblici (es. ospedali o strutture sanitarie pubbliche) o con Organismi di Diritto Pubblico
        iv. ottenimento di concessioni, licenze, autorizzazioni, accreditamenti;
        v. conciliazioni amministrative;
    b) Offerta di denaro o riconoscimento di altri vantaggi in favore di operatori sanitari, di professionisti o di medici che operano alle dipendenze di strutture sanitarie pubbliche in relazione ai rapporti di fornitura di beni e servizi;

c) Offerta ad un dipendente della Pubblica Amministrazione o ad un incaricato di pubblico servizio (es. medico) di partecipare a congressi fittizi o dazione di regali preziosi in cambio dell'adozione presso la struttura sanitaria di appartenenza, di un determinato prodotto della società;
d) Stipulazione di un contratto di ricerca fittizio con il primario di una struttura ospedaliera come corrispettivo per ottenere la dazione presso la struttura ospedaliera di un determinato prodotto della società;
e) Offerta di denaro o altre utilità ad autorità giudiziarie per il tramite di propri legali interni o di consulenti legali esterni.

In tutte le sopraindicate ipotesi, si precisa che dovrà comunque essere sotteso un differente interesse della Società, quale, ad esempio, accrescere i rapporti contrattuali con un cliente o, ottenere consulenze favorevoli alla conclusione di operazioni e dunque ad un incremento dell'attività della Società.

Processi aziendali a rischio:

Partecipazione a procedure di gara o affidamento diretto con enti pubblici (es. ospedali o strutture sanitarie pubbliche) o con Organismi di Diritto Pubblico

Attività di negoziazione, stipulazione ed esecuzione di contratti con enti pubblici (es. ospedali o strutture sanitarie pubbliche) o con Organismi di Diritto Pubblico

Attività di scelta dei consulenti e gestione dei rapporti con gli stessi in relazione ai rapporti con le pubbliche amministrazioni, enti pubblici o Organismi di Diritto Pubblico;

Presidio dei procedimenti giudiziari;

Richiesta di permessi, licenze ed autorizzazioni alla PA

Gestione di liberalità destinate alla Pubblica Amministrazione (es. a favore delle strutture sanitarie pubbliche)

Omaggi

Gestione di congressi e convegni

Funzioni aziendali a rischio:

Consiglio di Amministrazione

Amministrazione e Finanza

Vendite

Marketing

2.1.7 Art. 319 c.p.
Corruzione per un atto contrario ai doveri d'ufficio

"Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni."

Fattispecie

Il dolo è specifico e consiste nella coscienza e volontà di ricevere, per sé o per un terzo, una dazione o promessa di denaro o altra utilità per omettere o ritardare un atto di ufficio o per compiere un atto contrario ai doveri di ufficio.

Considerazioni applicative

Il reato (delitto) è ampiamente ipotizzabile per La Società.
Vale quanto detto sub art. 318 cod. pen..

2.1.8 Art. 319-quater c.p.
Induzione indebita a dare o promettere utilità

"Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi.

Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni.

Fattispecie

L'induzione è intesa come attività di persuasione, convinzione o suggestione o atteggiamento - e secondo alcuni anche inganno o frode - comunque atti ad influire sulla vittima. La dazione o promessa di denaro o altra utilità - anche non di natura economica (fino alle "prestazioni sessuali") - devono essere in rapporto causale con la condotta abusiva del funzionario e quindi rispondere ad una pretesa indebita di questo. Quanto all'elemento soggettivo, il dolo è generico e consiste nella coscienza e volontà di abusare della qualità o dei poteri connessi con la pubblica funzione, costringendo o inducendo altri all'indebito.

Il reato si consuma nel momento della effettuazione della promessa o, solo qualora sia immediata, della dazione.

Considerazioni applicative

Il reato appare ipotizzabile per la Società.

2.1.9 Art. 320 c.p.
Corruzione di persona incaricata di pubblico servizio

"Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

In ogni caso le pene sono ridotte in misura non superiore a un terzo".

Fattispecie

La norma prevede un reato autonomo il cui soggetto attivo può essere, per la corruzione impropria, di cui all'art. 319 cod. pen., solo l'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato e, per la corruzione propria, di cui all'art. 318 cod. pen, ogni incaricato di un pubblico servizio.

Considerazioni applicative

Il reato è ipotizzabile per la Società. Vale quanto detto sub artt. 318 e 319 cod. pen..

2.1.10 Art. 321 c.p.
Pene per il corruttore

"Le pene stabilite nel primo comma dell'Art. 318, nell'Art. 319, nell'Art. 319 bis, nell'art. 319 ter e nell'Art. 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità".

Fattispecie

Il privato deve dare o promettere denaro o altra utilità al pubblico ufficiale o all'incaricato di pubblico servizio affinché questi compia un atto del suo ufficio o un atto contrario ai doveri di ufficio ovvero al fine di compensarlo per il compimento dell'atto contrario ai doveri di ufficio.

Il dolo è specifico e consiste nella coscienza e volontà di compensare il pubblico ufficiale o l'incaricato di pubblico servizio con doni o promesse per il compimento dell'atto di ufficio o contrario ai doveri di ufficio. Le responsabilità del corrotto e del corruttore sono indipendenti.

Considerazioni applicative

Il reato (delitto) è ipotizzabile per la Società. Vale quanto detto sub artt. 318, 319, 319-bis, 319-ter e 320 cod. pen..

2.1.11 Art. 322 c.p.
Istigazione alla corruzione

*"**Chiunque offre o promette denaro o altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'Art.318, ridotta ad un terzo.***

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di pubblico servizio ad omettere o ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'art. 319 ridotta ad un terzo.

La pena di cui al primo comma si applica a pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.

La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità da parte di un privato per le finalità indicate dall'Art. 319".

Fattispecie

La condotta consiste nell'offrire o promettere a un pubblico ufficiale o ad un incaricato di pubblico servizio denaro o altra utilità per indurlo a compiere un atto di ufficio o contrario ai doveri dell'ufficio, qualora l'offerta o la promessa non venga accettata

Quanto all'elemento soggettivo, il dolo è specifico e consiste nella coscienza e volontà, rispettivamente, di indurre il pubblico funzionario al compimento dell'atto conforme o contrario ai doveri di ufficio ovvero di sollecitare la dazione o promessa di denaro o dell'utilità per il compimento dell'atto conforme o contrario ai doveri di ufficio.

Si tratta di un reato di mera condotta, che si consuma, rispettivamente, con l'offerta o promessa dell'utilità ovvero con la sollecitazione della promessa o dazione, che ovviamente non devono essere accettate.

Considerazioni applicative

Il reato (delitto) è ampiamente ipotizzabile per la Società. Vale quanto detto sub artt. 318, 319, 319-ter e 320 cod. pen..

2.1.12 Art. 346 bis c.p. Traffico di influenze illecite

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319 ter c.p., sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente fa dare o promettere a sé o ad altri denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio, è punito con la reclusione da uno a tre anni
La stessa pena si applica a chi indebitamente dà o promette denaro o altro vantaggio patrimoniale.
La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sè o ad altri, denaro o altro vantaggio patrimoniale riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio.
Le pene sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie.
Se i fatti sono di particolare tenuità, la pena è diminuita.

Fattispecie

La condotta di privati che, non riuscendo ad avere un contatto diretto con il funzionario pubblico, si rivolgono a qualcuno in grado di intercedere, trovandosi poi nella condizione di remunerarlo per la prestazione resa in loro favore. Gli esempi che ritroviamo riguardano spesso faccendieri che interferiscono per l'aggiudicazione di lavori pubblici, o per l'erogazione di sovvenzioni o contributi pubblici, ovvero per la ricerca di un posto di lavoro, o comunque per "aprire determinate porte" in cambio di una retribuzione.

La nuova norma punisce con la reclusione da uno a tre anni «chiunque, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319-ter c.p., sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente fa dare o promettere, a sé o ad altri, denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio, ovvero per remunerarlo, in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio».

La stessa pena si applica, in base al secondo comma della disposizione, «a chi indebitamente dà o promette denaro o altro vantaggio patrimoniale», mentre la pena è aumentata nell'ipotesi prevista dal terzo comma, ossia «se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altro vantaggio patrimoniale riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio». Il comma quarto prevede che le pene «sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie», mentre il quinto stabilisce una diminuzione di pena «se i fatti sono di particolare tenuità».

Considerazioni applicative

Il reato (delitto) è ipotizzabile per la Società. Vale quanto detto sub artt. 318, 319, 319-ter e 320 ,322 cod. pen..

2.2. Sintesi delle attività sensibili nella Società

L'analisi dei processi aziendali della Società, svolta nel corso dell'elaborazione del Modello, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dagli articoli 24 e 25 del d.lgs. 231/2001. Qui di seguito sono elencate le operazioni di maggiore rilievo, rientranti nelle attività sensibili identificate con riferimento ai reati nei confronti della pubblica amministrazione:

1. redazione e/o presentazione delle domande volte all'ottenimento da parte della Società di erogazioni pubbliche (nazionali e/o comunitarie, in forma di contributi, finanziamenti, sovvenzioni etc.);

2. gestione e destinazione di contributi/sovvenzioni/finanziamenti concessi da Enti Pubblici a favore della Società;

3. gestione delle domande e dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze e altri provvedimenti amministrativi per l'esercizio delle attività aziendali;

4. gestione dei flussi finanziari in entrata ed in uscita;

5. gestione dell'attività relativa ad azioni di recupero di crediti insoluti;

6. negoziazione, stipulazione o esecuzione di contratti e/o convenzioni con la Pubblica Amministrazione anche attraverso la partecipazione a procedure ad evidenza pubblica (aperte, negoziate o ristrette);

7. negoziazione, stipulazione ed esecuzione di contratti con la Pubblica Amministrazione o altri enti i cui dipendenti possano qualificarsi con pubblici ufficiali o incaricati di pubblico servizio ;

8. gestione dei rapporti con soggetti pubblici relativi a diritti sugli immobili (es. Conservatoria e Catasto);

9. gestione rapporti con autorità di pubblica sicurezza o altre autorità pubbliche nel normale svolgimento di attività aziendali (es. Enti Pubblici Locali, Ministeri);

10. gestione dei rapporti con Autorità Pubbliche di Vigilanza o Regolamentazione (es. Autorità Garante per la protezione dei dati personali);

11. adempimenti per la sicurezza interna;

12. selezione e gestione dei rapporti con imprese fornitrici di beni e servizi della società;

13. selezione e assunzione di personale dipendente (ivi compreso personale appartenente alle categorie protette o la cui assunzione è agevolata);

14. attività relativa agli adempimenti INPS, INAIL, Ispettorato del lavoro;

15. selezione e gestione di agenti /procacciatori d'affari /intermediari e collaboratori che svolgono ruoli analoghi;

16. gestione di *software* di soggetti pubblici o forniti da terzi per conto di soggetti pubblici e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a soggetti pubblici – in particolare in materia societaria e fiscale.

17. gestione dei rapporti con soggetti appaltanti (es. Consip);

18. utilizzazione e impiego di beni della Società a scopo di pubblicità e sponsorizzazione;

19. gestione degli omaggi e delle spese di rappresentanza / gestione delle erogazioni liberali.

20. campionamenti.

In tutte le attività suddette, le funzioni primariamente coinvolte nelle relative operazioni sono quelle della Amministrazione Risorse Umane, del Marketing e della funzione Vendite, che riportano agli Amministratori.

2.3. Il sistema dei controlli.

Il sistema dei controlli, applicabili alle attività individuate, è stato definito utilizzando come riferimento le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali in tema di rischi di frode e corruzione, ed è stato successivamente adottato dalla Società.

Il Modello, per quanto riguarda i reati nei confronti della pubblica amministrazione, è strutturato su due distinti livelli di controllo:

- ***standard* di controllo fissi:** devono essere sempre presenti in tutte le attività sensibili;
- ***standard* di controllo**

2.3.1 Standard di controllo fissi

Gli ***standard* di controllo fissi** sono:

1. **poteri di firma e poteri autorizzativi - forma:** deve essere adottato da parte della Società un sistema di poteri interni (cd. deleghe) ed esterni (cd. poteri di firma) illustrato e formalizzato in appositi documenti, da tenere aggiornati, disponibili agli atti della Società ed accessibili da chiunque abbia legittimo interesse;
2. **Poteri di firma e poteri autorizzativi - competenza:** il sistema di deleghe e dei poteri di firma deve essere caratterizzato dal principio dell'allocazione di ciascuna delega al soggetto dotato delle necessarie competenze;
3. **Poteri di firma e poteri autorizzativi – doppia firma in materia bancaria:** il sistema dei poteri di firma bancari deve essere caratterizzato da meccanismi di doppia firma per quanto attiene alle operazioni di maggiore rilevanza, secondo quanto di volta in volta definito dai regolamenti interni
4. **segregazione delle attività:** deve esistere segregazione delle attività tra chi autorizza, chi esegue e chi controlla;
5. **tracciabilità:** il soggetto che firma le comunicazioni scritte alla pubblica amministrazione deve assicurare la tracciabilità delle relative fonti e degli elementi informativi;
6. **procedura scritta**: qualsiasi operazione deve essere disciplinata da una procedura interna conforme agli standard di controllo applicabili a tale operazione;
7. **norme/circolari:** devono esistere disposizioni aziendali idonee a fornire i principi di riferimento per la regolamentazione dell'attività, nonché a portare le procedure scritte a conoscenza dei destinatari;
8. **archiviazione:** deve esistere un sistema di individuazione e conservazione di qualsiasi documento scritto

2.3.2 Standard di controllo

Gli ***standard* di controllo** sono:

A **divieto di accesso a risorse finanziarie in autonomia:** il soggetto che intrattiene rapporti con la pubblica amministrazione non può da solo e liberamente accedere alle risorse finanziarie e autorizzare disposizioni di pagamento;

B **divieto di conferimento di contratti di consulenza o similari in autonomia:** il soggetto che intrattiene rapporti con la pubblica amministrazione non può da solo e

liberamente conferire incarichi di consulenza/prestazioni professionali;

C **divieto di concessione di utilità in autonomia:** il soggetto che intrattiene rapporti con la pubblica amministrazione non può da solo e liberamente concedere qualsivoglia utilità;

D **divieto di assunzione di personale in autonomia:** il soggetto che intrattiene rapporti con la pubblica amministrazione non può da solo e liberamente procedere ad assunzioni di personale.

E **divieto di concedere in autonomia prodotti/servizi a condizioni diverse da quelle *standard*:** il soggetto che intrattiene rapporti con la pubblica amministrazione non può da solo e liberamente concedere prodotti/servizi a condizioni diverse da quelle *standard*.

2.3.3 Altri standard di controllo specifici

Sono inoltre previsti degli *standard* di controllo specifici per (i) la **sicurezza informatica** che prevedono l'esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d.lgs. 196/2003 e nelle *best practice* internazionali (ii) la gestione di **agenti/procacciatori di affari/intermediari e collaboratori che svolgono ruoli analoghi**; (iii) la gestione delle **richieste e la gestione dei contributi /finanziamenti pubblici**; (iv) la gestione dei beni dell'azienda **a scopo di immagine / sponsorizzazione**; (v) la gestione dell'attività di **assunzione del personale** (vi) la gestione dei **trattamenti previdenziali del personale**; (vii) la gestione dei **flussi finanziari**

I controlli *standard* specifici per **la sicurezza informatica** sono quelli di seguito indicati:

- **autenticazione:** è richiesta l'autenticazione individuale degli utenti tramite *log in* e *password* od altro sistema di autenticazione sicura;
- **sistema di autorizzazione alle operazioni eseguibili sui dati:** deve essere previsto un sistema di autorizzazione (profili di utilizzo) per l'esecuzione di operazioni sui dati o per limitare la visibilità ad un sottoinsieme dei dati stessi;
- **liste di controllo:** devono essere disponibili liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti, nel caso in cui sia previsto un sistema di autorizzazione;
- **obblighi degli utenti:** devono esistere procedure che definiscono gli obblighi degli utenti nell'utilizzo dei sistemi informatici;
- **Poteri:** deve essere attribuito esclusivamente al servizio competente la facoltà di cancellare dati, liste di controllo ed archivi. Il servizio deve assicurare la tracciabilità delle relative operazioni.
- **altre misure di protezione:** devono essere documentate le principali misure di protezione adottate (politica di aggiornamento dell'antivirus, misure di *back up*, ecc.).

I controlli *standard* specifici per la gestione di **agenti/procacciatori di affari/intermediari e collaboratori che svolgono ruoli analoghi** sono quelli di seguito indicati:

- Procedura: formalizzazione di una procedura per la selezione e valutazione degli agenti/procacciatori d'affari/intermediari e collaboratori che svolgono ruoli analoghi che preveda: i) criteri oggettivi e trasparenti per l'attività di selezione degli agenti/ procacciatori d'affari (richiesta di preventiva iscrizione e verifica della permanenza nei ruoli degli Agenti istituiti presso le Camere di Commercio, richiesta di requisiti soggettivi relativi alla professionalità e onorabilità dell'agente/ procacciatore d'affari/intermediario e collaboratore che svolge ruoli analoghi, richiesta di documentazione quale certificato del casellario giudiziario/carichi pendenti, certificato

camerale con dicitura antimafia, referenze qualificanti, ecc.), ii) la separazione di funzioni tra coloro che selezionano gli agenti/ procacciatori d'affari/intermediari e collaboratori che svolgono ruoli analoghi e coloro che ne controllano l'operato e (iii) il divieto di instaurare rapporti con agenti/intermediari o collaboratori per specifici affari.

- **Provvigioni**: i) riconoscimento/determinazione di provvigioni e rimborsi spese in favore degli agenti/ procacciatori d'affari/intermediari e collaboratori che svolgono ruoli analoghi ancorati a parametri predefiniti e siano comunque in linea con la prassi del mercato; (ii) le provvigioni, i bonus, i premi e i rimborsi spese siano preventivamente ed espressamente approvati dalla Società e non pagati con meccanismi di corresponsione "automatica" e non sono stabiliti in relazione a specifici affari.
- **Pagamenti**: nessun pagamento in favore di tali soggetti può essere effettuato in contanti o per mezzo di titoli al portatore, comunque per interposta persona e in luogo/stato diverso da quello in cui tale soggetto ha reso i propri servizi
- **Poteri**: agenti/ procacciatori d'affari/intermediari e collaboratori che svolgono ruoli analoghi non devono essere dotati di potere di rappresentanza e gli ordini raccolti dagli agenti/ procacciatori d'affari nell'interesse della Società devono essere comunque soggetti a preventiva approvazione da parte del proponente.
- **Subagenti e divieto di cessione del contratto**: il contratto di agenzia deve prevedere la preventiva autorizzazione, da parte del proponente, per la nomina di subagenti nonché il divieto di cessione del contratto.
- **Richiami al Modello**: il contratto di agenzia deve prevedere specifici richiami al Modello ex d.lgs. 231 del 2001 adottato dalla Società e clausole risolutive espresse volte a sanzionare comportamenti contrari alle previsioni dello stesso da parte dell'agente

I controlli *standard* specifici per la gestione di **richieste e alla gestione dei contributi /finanziamenti pubblici** sono quelli di seguito indicati:

- **Procedura**: formalizzazione di una procedura per la richiesta e la gestione di contributi/finanziamenti pubblici che preveda: i) il coinvolgimento di più funzioni aziendali nella predisposizione di domande inviate a soggetti pubblici, ii) poteri di firma congiunta per le richieste all'ente erogante, iii) modalità di gestione dei contributi/finanziamenti, iv) il coinvolgimento di più funzioni aziendali nella rendicontazione sull'utilizzo del finanziamento, v) modalità di gestione delle eventuali verifiche da parte degli enti erogatori.
- **Autorizzazione e poteri**: solo soggetti dotati di apposita procura sono legittimati ad intrattenere rapporti con gli enti pubblici eroganti. Esclusione esplicita nel sistema delle procure della "richiesta di denaro o altra utilità a terzi".

I controlli standard specifici per la gestione di **beni a scopo di immagine e sponsorizzazione** sono quelli di seguito indicati:

- **Procedura**: formalizzazione di una procedura per l'utilizzazione di beni dell'azienda a scopo di immagine/sponsorizzazione.
- **Lista di fornitori**: deve esistere l'obbligo di selezionare eventuali fornitori scelti all'interno di una lista gestita dalla funzione competente. L'inserimento/eliminazione dei fornitori dalla lista deve essere basato su criteri oggettivi e l'individuazione, all'interno della lista, del fornitore deve essere motivata e documentata.

I controlli standard specifici per la gestione dell'attività di **assunzione del personale** sono quelli di seguito indicati:

- **Procedura**: devono esistere procedure per l'assunzione del personale che prevedano i) criteri di selezione dei candidati oggettivi e trasparenti (es. voto di laurea/diploma, conoscenza di lingue straniere, precedenti esperienze professionali, ecc.), ii) tracciabilità delle fonti di reperimento dei curricula, iii) segregazione delle funzioni coinvolte nel processo, iv) definizione di ruoli e responsabilità dei soggetti coinvolti, v) modalità di archiviazione della documentazione rilevante.
- **Disposizioni Aziendali**: devono esistere disposizioni aziendali in base alle quali gli obiettivi posti ai dipendenti nell'esercizio della loro attività e i meccanismi di incentivazione previsti non siano basati su target di performance palesemente immotivati e così " "sfidanti" da risultare, di fatto, irraggiungibili con mezzi leciti.
- **Documentazione**: deve esistere adeguata documentazione del processo di selezione ed obbligo di conservare la relativa documentazione in apposito archivio, con divieto di cancellare o distruggere i documenti archiviati.

I controlli standard specifici per la gestione dei **trattamenti previdenziali del personale** sono quelli di seguito indicati:

- **Procedura:** formalizzazione di una procedura per la gestione dei trattamenti previdenziali del personale che preveda: i) segregazione delle funzioni coinvolte, ii) definizione di ruoli e responsabilità dei soggetti coinvolti, iii) modalità di archiviazione della documentazione rilevante.
- **Autorizzazione e poteri**: solo soggetti dotati di apposita procura sono legittimati ad intrattenere rapporti con soggetti appartenenti alla Pubblica Amministrazione o, comunque, con soggetti qualificabili come "pubblici"

I controlli standard specifici per la gestione dei **flussi finanziari** sono quelli di seguito indicati:

- **Procedura**: formalizzazione di una procedura per la gestione dei flussi finanziari che definisca, fra l'altro: i) ruoli e responsabilità dei soggetti coinvolti; ii) tipologie di transazioni eseguibili direttamente dalle varie funzioni aziendali; iii) controlli specifici e preventivi da applicarsi in casi, tassativamente previsti, in deroga alla normale procedura (es. pagamenti urgenti); iv) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e discrezionalità; (v) controlli della documentazione aziendale e, in particolare, delle fatture passive (la pratica più diffusa per procurarsi la provvista per corrompere è l'utilizzazione di fatture per operazioni inesistenti).
- **Autorizzazione e poteri**: solo soggetti dotati di apposita procura sono legittimati alla gestione e movimentazione dei flussi finanziari.
- **Documentazione**: devono esistere documenti giustificativi delle risorse finanziarie utilizzate, con motivazione e attestazione di inerenza e congruità approvati da adeguato livello gerarchico ed archiviati.

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi di conseguenza.

III. B - REATI SOCIETARI

3.1 Premessa

Il D. Lgs. 61/2002 ha esteso la responsabilità amministrativa delle persone giuridiche alla commissione di reati societari da parte di amministratori, direttori generali o liquidatori nonché, in taluni casi, anche da loro sottoposti o altri soggetti che intrattengono rapporti qualificati con la Società (ad es. i suoi revisori).

In particolare, come previsto dall'art. 25-ter del Decreto, introdotto dal D. Lgs. 61/2002, la società può essere chiamata a rispondere nei casi di commissione dei reati in materia societaria previsti dal codice civile agli articoli 2621 – 2641. La norma precisa che la responsabilità è estesa alla società ove detti reati siano commessi nell'interesse della società stessa.

In proposito, si ritiene fondato recepire l'orientamento di autorevole dottrina, secondo cui non tutti i reati societari comportano profili di responsabilità per la società: infatti, vi sono alcuni reati la cui commissione risulta in ogni caso dannosa per la società, la cui economia sarà impoverita o comunque danneggiata, *"con l'effetto che, relativamente ad essi, non si potrà configurare il presupposto di fatto della responsabilità amministrativa della società, cioè la loro commissione nell'interesse della società"*:[1] trattasi in particolare dei reati di indebita restituzione dei conferimenti (art. 2626 c.c.), ripartizione illegale degli utili e delle riserve (art. 2627 c.c.) e illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), nonché infedeltà patrimoniale (art. 2634 e 2635 c.c.).

Il presente modello è stato aggiornato alla luce delle modifiche disposte con L 69 del 27 maggio 2015 per cui con l'art 9 ha sostituito l'art. c.c. 2621, con l'art 10 ha introdotto l'art. 2621 bis e 2621 ter, con l'art 11 ha sostituito l'art. 2622 e con l'art 12 ha modificato l'art 25 ter comma 1 del d.lgs 231/2001.

A tale scopo, si è ritenuto opportuno prevedere, nell'ambito dei protocolli generali e speciali relativi a tali reati, obblighi informativi a carico dell'Organismo nei confronti dell'azionista di riferimento della Società.

3.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 25 ter sono:

- art 2621 - False comunicazioni sociali
- **a**rt 2621- bis Fatti di lieve entità
- art 2622 - False comunicazioni sociali delle società quotate
- art 2635 - Corruzione tra privati
- art 2635 bis - Istigazione alla corruzione tra privati

3.2.1 Art. 2621 cod. civ.
False comunicazioni sociali

Fuori dai casi previsti dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione

[1] V. Salafia, "*La responsabilità delle società alla luce del D.M. n. 201/2003 e delle modifiche al D. Lgs. n. 231/01"*, in *Le Società*, n. 11/2003, pag. 1434.

economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.
La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi

Fattispecie

Si tratta di un reato proprio, per la cui commissione è richiesta la qualifica di amministratore, direttore generale, dirigente preposto alla redazione dei documenti contabili sociatari, sindaco o liquidatore

La condotta criminosa è duplice e si concretizza:

1) nella esposizione di fatti materiali non veri. Tali informazioni possono anche essere frutto di valutazioni;
2) nella omissione di informazioni imposte *ex lege*.

La falsità delle comunicazioni deve cadere sui bilanci, relazioni o altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico.

In particolare, vengono in considerazione:

Relazioni:

- relazione degli amministratori al bilancio (artt. 2428 e 2429 c.c.)
- relazione per la distribuzione degli acconti dividendo (art. 2433 bis)
- relazione sulla situazione patrimoniale per la riduzione del capitale a seguito di perdite (artt. 2446 e 2447 c.c.)
- relazione al bilancio in fase di liquidazione e finale di liquidazione (artt. 2490 e 2492 c.c.)

Bilancio:

- di esercizio (art. 2423c.c.)
- finale di liquidazione (artt. 2490 e 2492 c.c.)
- straordinari, redatti in occasione di particolari circostanze

Comunicazioni sociali:

- tutte le comunicazioni (anche verbali) previste dalla legge e genericamente dirette ai soci o ai terzi.

L'esposizione inveritiera o l'omissione di informazioni devono essere relative alla *situazione economica, patrimoniale o finanziaria della società o del gruppo di appartenenza;* inoltre, possono anche avere per oggetto *beni posseduti o amministrati dalla società per conto di terzi*.

Le comunicazioni false assumono rilievo penale solo ove:

- da un lato, contengano falsità od omissioni che incidano sul risultato economico di esercizio (determinando una variazione del risultato economico di esercizio, al lordo delle imposte, superiore al 5%) o sul patrimonio netto (determinando una variazione del patrimonio netto superiore all'1%) ovvero contengano valutazioni estimative che singolarmente considerate differiscono in misura superiore al 10% di quella corretta;
- dall'altro, siano idonee ad indurre in errore i destinatari. Tale caratteristica andrà accertata diversamente, a seconda che i destinatari siano il pubblico ovvero i soci.

Quanto all'elemento soggettivo del reato, la norma richiede "l'intenzione di ingannare i soci o il pubblico" ovvero il "fine di conseguire per sé o per altri un ingiusto profitto", e quindi la presenza di un dolo specifico.

Il reato si consuma nel momento in cui la falsa comunicazione idonea ad ingannare il pubblico giunge a conoscenza dei destinatari; con particolare riferimento al bilancio, tale momento

consumativo va individuato, per quanto riguarda i soci nel relativo deposito per l'approvazione da parte dell'assemblea; per quanto riguarda il pubblico col deposito successivo alla sua approvazione.

La fattispecie è punita con l'arresto da uno a cinque anni.

La sanzione pecuniaria a carico della società varia da duecento a quattrocento quote.

Considerazioni applicative

Il reato è ipotizzabile per la Società.

Occasioni di reato

1) Esposizione di fatti non rispondenti al vero sulle condizioni economiche, patrimoniali e finanziarie della Società:
   a) figurare in bilancio attività inesistenti o nascondere passività esistenti (sopravvalutazioni);
   b) figurare in bilancio passività inesistenti o nascondere attività esistenti (sottovalutazioni);
   c) omissione di informazioni la cui comunicazione è imposta dalla legge;
2) dissimulazione di fatti concernenti le condizioni economiche dell'impresa.

Processi aziendali a rischio

- Adempimenti in materia di Contabilità e Bilancio

Funzioni / Aree aziendali a rischio

- Consiglio di Amministrazione
- Personale e Amministrazione e Finanza

3.2.2 Art 2621- bis Fatti di lieve entità

Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'art 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'art. 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'art 1 del r.d. 16/3/1942 n° 267. In tale caso il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

Fattispecie

Si tratta di un reato che attiene a quanto è stato disposto all'art 2621 per cui è prevista una pena inferiore se i fatti previsti sono di lieve entità tenuto conto di natura, dimensioni e delle modalità o degli effetti della condanna.

Siamo sempre nel campo previsto dall'art 2621 ma di lieve entità. In altri termini fatti materiali irrilevati inveritieri e omissioni di non rilevante entità.

La falsità delle comunicazioni deve cadere sui bilanci, relazioni o altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico.

La fattispecie è punita con l'arresto da sei mesi a tre anni.

La sanzione pecuniaria a carico della società varia da cento a duecento quote.

Considerazioni applicative

Il reato è ipotizzabile per la Società.

Occasioni di reato

1) Esposizione di fatti non rispondenti al vero sulle condizioni economiche, patrimoniali e finanziarie della Società:
   d) figurare in bilancio attività inesistenti o nascondere passività esistenti (sopravvalutazioni);
   e) figurare in bilancio passività inesistenti o nascondere attività esistenti (sottovalutazioni);
   f) omissione di informazioni la cui comunicazione è imposta dalla legge;
2) dissimulazione di fatti concernenti le condizioni economiche dell'impresa.

Processi aziendali a rischio

- Adempimenti in materia di Contabilità e Bilancio
- Gestione contabile all'interno delle singole funzioni

Funzioni / Aree aziendali a rischio

- Consiglio di Amministratore
- Amministrazione e Finanza

3.2.3. Art. 2622 cod. civ.

False comunicazioni sociali delle società quotate

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese della Unione europea, i quali, al fine di conseguire per se o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.

Alle società indicate nel comma precedente sono equiparate:

1 le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro paese dell'unione europea;

2 le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;

3 le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro paese dell'unione europea;

4 le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni

riguardano beni posseduti o amministrati dalla società per conto di terzi.

Fattispecie

La fattispecie é identica a quella di false comunicazioni sociali di cui all'art. 2621; l'unico elemento aggiuntivo é dato dalla fatto che la società è emittente strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o europeo o controllante di una emittente o che fa appello al pubblico risparmio o che comunque lo gestisce.

Per quanto riguarda la condotta di reato valgono quindi le considerazioni sopra riportate sub art. 2621.

La norma prevede l'ipotesi di reato con riferimento al tipo di società nell'ambito della cui gestione è commesso l'illecito per cui in quanto quotata o quotanda o controllante di quotata il delitto è procedibile d'ufficio e sanzionato con la reclusione da tre a otto anni;

Quanto al momento consumativo, il delitto si perfeziona con l'induzione di terzi in errore.

Per quanto riguarda la sanzione pecuniaria a carico della società, essa è compresa tra quattrocento e seicento quote.

Considerazioni applicative

Occasioni di reato

Processi aziendali a rischio

Funzioni / Aree aziendali a rischio

Valgono le medesime considerazioni sub 2621.

3.2.4 Art. 2635 del cod. civ. Corruzione tra privati

Salvo che il fatto costituisca piu' grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto e' commesso da chi e' sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date o promesse o offerte."

La fattispecie fa riferimento al fatto che chi è facoltizzato a spendere induca esponenti di un'azienda a compiere atti di infedeltà o venir meno agli obblighi di ufficio corrompendoli dando loro o a terzi denaro ovvero utilità creando beneficio per sé e per l'azienda di cui sono esponenti.

L'ipotesi virtualmente possibile è quella che per una molteplicità di ragioni che possano essere a beneficio della società chi ha facoltà di spesa dia o prometta denaro per corruzione a amministratori, direttori generali, dirigenti, etc. sindaci, liquidatori di una società inducendoli a comportamenti infedeli.

Possono essere richiesta di emissione di fattura per operazione inesistente per generare costi fittizi alla società sottraendo ricavi all'imposizione fiscale e ricavi fittizi alla controparte colpita poi da imposizione fiscale.

Possono essere richiesta di sottoscrizione di contratto scarsamente conveniente per la società cliente contro pagamento di un premio al singolo facoltizzato a decidere, financo l'imprenditore stesso a cura di ns. agente che per il contratto riceva un premio e lo spartisca con il decisore.

Il reato si consuma nel momento in cui è cagionato un danno alla società dei corrotti.

Il reato è procedibile a querela del danneggiato.

La società è punita con sanzione pecuniaria da duecento a quattrocento quote.

Considerazioni applicative

La fattispecie viene in rilievo solo nel caso in cui esponenti della società corrompono esponenti di società il cui comportamento indotto dalla corruttela crea infedeltà e mancanze d'ufficio.

Pertanto, allo stato si ritiene applicabile alla Società.

3.2.5 Art. 2635 – bis del cod. civ.
Istigazione alla corruzione tra privati

Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per se' o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la

sollecitazione non sia accettata.

Si procede a querela della persona offesa.

Le considerazioni sno le medesime di quanto all'art. 2635 c.c.

Considerazioni applicative

La fattispecie viene in rilievo solo nel caso in cui esponenti della società promettano denaro od altra utilità corrompendo esponenti di società il cui comportamento indotto dalla corruttela crea infedeltà e mancanze d'ufficio.

Pertanto, allo stato si ritiene applicabile alla Società.

3.3 Attività sensibili nella Società

L'analisi dei processi aziendali della Società ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-*ter* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati societari.

1. tenuta della contabilità, redazione del bilancio d'esercizio, del bilancio consolidato, delle situazioni economiche infrannuali, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico;

2. adempimenti relativi all'attività di tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione del consiglio di amministrazione al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione;

3. gestione dei rapporti con soci. Redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo;

4. gestione dei rapporti con le Autorità di Vigilanza (ad esempio Autorità Antitrust, Garante per la protezione dei dati personali etc.): comunicazioni, attività di supporto nello svolgimento dei relativi controlli, trasmissione dati etc.;

5. attività di distribuzione degli utili e delle riserve;

6. attività di valutazione, autorizzazione e gestione delle operazioni sul capitale (quali ad esempio aumenti e riduzioni di capitali, operazione di fusione e scissione, conferimenti in denaro ed in natura);

7. gestione delle incombenze societarie relative a operazioni sul capitale e su partecipazioni;

8. rapporti con terzi fornitori o clienti.

Nell'ambito di tali attività sensibili, ruolo preminente è svolto dal Consiglio di Amministrazione e dalla funzione Personale e Amministrazione e Finanza.

3.4 Il sistema dei controlli.

Il sistema dei controlli, applicabili alle attività individuate, è stato definito utilizzando come riferimento le linee guida ad oggi pubblicate dalle principali associazioni di categoria nonché le

best practice internazionali, ed è stato successivamente adottato dalla Società.

Per ognuna delle attività sono stati individuati *standard* di controllo specifici.

Relativamente all'attività sensibile di **"redazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico**" gli *standard* di controllo specifici sono i seguenti.

A_1 Istruzioni di chiusura contabile: devono esistere istruzioni rivolte alle Unità organizzative, che indichino dati e notizie che è necessario fornire alla funzione competente per la redazione del bilancio in relazione alle chiusure annuali di bilancio nonché le relative modalità e la tempistica.

B_1 Programmazione: Deve esistere un livello aziendale che prevede ruoli, responsabilità e scadenze relativamente al flusso informativo da fornire alle varie divisioni interne coinvolte nel processo di bilancio.

C_1 Tracciabilità: il sistema informatico utilizzato per la trasmissione di dati e informazioni deve garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascuna Unità Organizzativa coinvolta nel processo deve garantire la tracciabilità di tutti i dati e le informazioni finanziarie. Il responsabile della Amministrazione e Bilancio acquisisce dai responsabili delle unità coinvolte nel processo di bilancio una dichiarazione attestante la veridicità e completezza delle informazioni fornite ai fini della redazione del bilancio civilistico e consolidato.

Relativamente all'attività sensibile inerente ad **"operazioni su azioni e quote proprie, operazioni sul capitale e destinazione degli utili**", gli *standard* di controllo specifici sono i seguenti.

A_2 Utili e riserve: esistenza di una procedura che regolamenti la predisposizione di una relazione per il Consiglio di amministrazione che giustifichi la distribuzione di utili e riserve nel rispetto di quanto previsto dalla legge.

B_2 Regole: devono esistere regole formalizzate che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione del consiglio di amministrazione al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione.

Relativamente all'attività sensibile inerente a "**rapporti con fornitori o clienti "**, lo *standard* di controllo specifico ai fini della esclusione è il seguente.

A_3 Regole di comportamento: devono esistere regole di comportamento che invitino tutti coloro che hanno autonomia di spesa a comportarsi con la massima onestà e correttezza nello svolgimento delle operazioni con fornitori e clienti ed altri operatori economici in generale. Tali regole di comportamento devono, nello specifico, indicare che la Società sottolinea il dovere di non procedere ad alcuna dazione o promessa ad amministratori, direttori, sindaci, liquidatori o loro subordinati perché omettano o contravvengano ai propri doveri danneggiando la propria società a beneficio proprio o di terzi e di EOS srl o di qualsiasi altra società del suo gruppo.

Si considerano attività sensibili:

1. Acquisto e/o cessione di beni/servizi con controparti.

2. Selezione dei partner commerciali/finanziari e gestione dei relativi rapporti con controparti.

3. Assunzione di personale.

4. Gestione delle transazioni finanziarie.

Standard di controllo specifici applicabili a qualsiasi soggetto che intrattiene rapporti con terzi (per la stipulazione di contratti o altro)

- **Presenza di almeno un'altra persona di pari livello organizzativo:** deve essere presente almeno un'altra persona di pari livello nelle fasi più importanti della relativa attività (ad es. Trattative, accordi contrattuali, transazioni etc.);
- **Report:** devono esistere report/verbali dettagliati per ogni singola operazione o atto di procedura ed inviati al superiore gerarchico;

In aggiunta per le situazioni sensibili sono stati individuati i seguenti standard di controllo specifici. Relativamente all'attività sensibile di "a**cquisto e/o cessione di beni/servizi con controparti** gli standard di controllo specifici sono i seguenti.

E' fatto divieto di:

a) intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con soggetti privi di buona reputazione desumibili dalle liste delle referenze. Priorità saranno date a soggetti dotati di modello 231 e a soggetti con rating di legalità;

b) operare con partner dai requisiti di onorabilità e professionalità discutibili.

c) non operare se non sono verificati i requisiti minimi in possesso dei soggetti offerenti e devono esser fissati i criteri di valutazione delle offerte nei contratti standard.

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi di conseguenza.

IV. C - I REATI DI FALSITA' IN MONETE, CARTE DI PUBBLICO CREDITO E VALORI DI BOLLO RICHIAMATI DALL'ART. 25-*bis* DEL D.LGS. 231/2001.

4.1 Premessa

La legge 23 novembre 2001 n. 409, di conversione del D.L. n. 350/2001 recante disposizioni urgenti in vista dell'euro ha introdotto, all'art. 4, un nuovo articolo al decreto n. 231/01 (l'art. 25-bis) relativo alla falsità in monete, carte di pubblico credito e in valori di bollo.

4.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 25 bis sono:

art 473 del c.p. - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni

Si applica di seguito l'art 474 del c.p. - Introduzione nello Stato e commercio di prodotti con segni falsi

4.2.1 Art. 473 del codice penale

Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti,

modelli e disegni

Chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione da sei mesi a tre anni e con la multa da € 2.500,00 a € 25.000,00.

Soggiace alla pena della reclusione da uno a quattro anni e della multa da € 3.500,00 a € 35.000,00 chiunque contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati.

I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

Fattispecie

La norma in esame sanziona i comportamenti idonei a mettere in pericolo la certezza della proprietà industriale, distinguendo le seguenti modalità di condotta:

- contraffazione (ossia produzione di marchi o segni distintivi da parte di soggetti non autorizzati, in modo da ingannare il pubblico);
- alterazione (ossia modifica le caratteristiche materiali o formali di marchi o segni distintivi, col fine di creare l'apparenza di un valore superiore);
- fa uso di concerto con chi l'ha eseguita la contraffazione di marchi e segni ;
- contraffazione (ossia produzione di brevetti, disegni, modelli industriali da parte di soggetti non autorizzati, in modo da ingannare il pubblico);
- alterazione (ossia modifica le caratteristiche materiali o formali di brevetti, disegni, modelli industriali, col fine di creare l'apparenza di un valore superiore);
- fa uso di concerto con chi l'ha eseguita la contraffazione od alterazione di brevetti, disegni e modelli industriali;

Considerazioni applicative

Il reato è astrattamente ipotizzabile ma non privo di rischio concreto per la Società in quanto essa si avvale di prodotti con marchi e segni che determinano la vendibilità

Occasioni di reato

Ogni volta che si usi un bene con marchio contraffatto o alterato o con simbologia alterata o contraffatta a certificare la qualità.

Processi aziendali a rischio

Forniture di macchine e additivi

Vendite

4.2.2 Art. 474 del codice penale

Introduzione nello Stato e commercio di prodotti con segni falsi

Fuori dei casi di concorso nei reati previsti dall'articolo 473, chiunque introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati è punito con la reclusione da uno a quattro

anni e con la multa da € 3.500,00 a € 35.000,00.
Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello Stato, chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti di cui al primo comma è punito con la reclusione fino a due anni e con la multa fino a € 20.000,00.
I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

Considerazioni applicative

Si rinvia a quanto previsto nel paragrafo 4.2.1.

4.3 Attività sensibili nella Società

L'analisi dei processi aziendali della Società, svolta nel corso del progetto, ha consentito di individuare un'attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-bis del d.lgs. 231/2001. Qui di seguito è indicata l'attività sensibile o a rischio con riferimento ai reati di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni accanto all'introduzione nello Stato e commercio di prodotti con segni falsi.:

1. Ogni possibilità di detenere, utilizzare, importare commercializzare beni con marchio, disegno o segno distintivo o brevetto o modello e disegno contraffatto o alterato.

4.4 Il sistema dei controlli

Il sistema dei controlli, applicabili all'attività individuata, è stato definito utilizzando come riferimento le Linee guida di Assobiomedica, le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali.

Il Modello, in relazione all'attività ritenuta sensibile ai sensi dell'art. 25-bis del d.lgs. 231/2001, è strutturato secondo gli standard di controllo specifici di seguito indicati:

- Tracciabilità di filiera e tracciabilità dei materiali.
- Organizzazione, gestione e valutazione dei fornitori.
- Apposite clausole contrattuali con i fornitori e con i distributori.
- L'Organismo di Vigilanza viene informato di eventuali irregolarità.

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi di conseguenza.

V. D - I REATI IN TEMA DI DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO RICHIAMATI DALL'ART. 25-*bis 1* DEL D.LGS. 231/2001.

5.1 Premessa

La Legge n° 99 del 23 luglio 2009 all'Art. 15 comma 7, lettera b) ha introdotto nell'articolato del Decreto Legislativo 231/2001 l'art. 25 bis 1, che integra la lista dei Reati Presupposto per la

responsabilità degli Enti con **i reati in tema di delitti contro l'industria e il commercio**.

5.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 25 bis 1 sono:
- art 517 c.p - Vendita di prodotti industriali con segni mendaci

Si applica di seguito l'art 517 ter del c.p. - Introduzione nello Stato e commercio di prodotti con segni falsi

5.2.1 Art. 517 del codice penale

Vendita di prodotti industriali con segni mendaci

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 a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a due anni o con la multa fino a ventimila euro.

Fattispecie

La norma in esame sanziona la vendita o la messa a disposizione di opere d'ingegno o prodotti industriali con nomi, marchi o segni distintivi col fine di ingannare il pubblico sull'origine, provenienza o qualità dell'opera o del prodotto.

Considerazioni applicative

Il reato è astrattamente ipotizzabile ma non privo di rischio concreto per la Società in quanto essa si avvale di prodotti con marchi e segni che determinano la vendibilità in quanto marchiati CE etc.

Occasioni di reato

Ogni volta che si dovesse usare o mettere a disposizione un bene con marchio contraffatto o alterato o con simbologia alterata o contraffatta a certificare la qualità.

Processi aziendali a rischio

Forniture di macchine e additivi

Aree aziendali a rischio
Vendite
Ufficio gare pubbliche
Direzione
Amministrazione e finanza
Produzione
Ufficio risorse umane
Acquisti
Gestione degli ordini

Gestione fornitori

5.2.2 Art. 517 - ter del codice penale

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale

Salva l'applicazione degli articoli 473 e 474 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 è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a euro 20.000.
Alla stessa pena soggiace chi, 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 di cui al primo comma.
Si applicano le disposizioni di cui agli articoli 474 bis, 474 ter, secondo comma, e 517 bis, secondo comma.
I delitti previsti dai commi primo e secondo sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

La norma in esame sanziona la fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale.

Considerazioni applicative

Il reato è astrattamente ipotizzabile in quanto la Società fa produrre macchine che potrebbero avere parti protette da brevetto o quant'altro..

Occasioni di reato

Ogni volta che si dovesse fare produrre e commercializzare un bene prodotto usurpando titoli di proprietà industriale.

Processi aziendali a rischio

Forniture di macchine e additivi

Vendite

5.3 Attività sensibili nella Società

L'analisi dei processi aziendali della Società, svolta nel corso del progetto, ha consentito di individuare un'attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-bis 1 del d.lgs. 231/2001. Qui di seguito è indicata l'attività sensibile o a rischio con riferimento ai reati di vendita di prodotti industriali con segni mendaci accanto alla fabbricazione e commercializzazione di beni realizzati usurpando titoli di proprietà industriale:

1. Ogni possibilità di vendere macchine con contrassegni di qualità mendaci o falsi;
2. Fabbricare e vendere macchine copiando parti di altre coperte da brevetti.

5.4 Il sistema dei controlli

Il sistema dei controlli, applicabili all'attività individuata, è stato definito utilizzando come riferimento le Linee guida di Confindustria, le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali.

E' opportuno quindi che la società si impegni a:
1) porre in essere atti di concorrenza in modo da non ledere gli interessi dell'economia nazionale e nei limiti stabiliti dalla legge;
2) astenersi dall'imporre ai propri agenti, distributori o dipendenti condizioni contrattuali insostenibili e obiettivi di vendita eccessivi, tali da indurre i destinatari a porre in essere violazioni delle norme poste a tutela della libera concorrenza.

Il Modello, in relazione all'attività ritenuta sensibile ai sensi dell'art. 25-bis 1 del d.lgs. 231/2001, è strutturato secondo gli standard di controllo specifici di seguito indicati:

- Tracciabilità di filiera nell'area della produzione;
- Controlli produzione presso terzisti;
- Controllo qualità prodotto;
- Verifica congruenza prodotti finiti e forniti con ordini di acquisto;
- Scelta e verifica dei fornitori;
- Gestione e controllo magazzino (anche se presso terzi);
- Inserimento di apposite clausole nei contratti di agenzia, fornitura e distribuzione.

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi di conseguenza.

VI. E - REATI IN MATERIA DI CRIMINI INFORMARICI E TRATTAMENTO ILLECITO DEI DATI RICHIAMATI DALL'ART. 24-*bis* DEL D.LGS. 231/2001.

6.1 Premessa

La Legge 18 marzo 2008, n. 48, ratificando la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica (23 novembre 2001), ha anche approvato varie modifiche sia al Codice Penale sia a quello di Procedura Penale e ha introdotto, tra i reati presupposto della responsabilità amministrativa degli enti l'art. 24 bis, così estendendo tale responsabilità anche ai delitti informatici, in stretta coerenza con i profondi cambiamenti dipendenti dalla tecnologia digitale e dalla sua rapida evoluzione, nonché dalla convergenza e costante globalizzazione delle reti informatiche.

6.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 24 bis sono:

- art 615 ter - Accesso abusivo ad un sistema informatico o telematico
- art 615 quater - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

- art 615 quinquies - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- art 617 quater - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- art 617 quinquies - Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche
- art 635 bis - Danneggiamento di informazioni, dati e programmi informatici
- art 635 ter - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- art 635 quater - Danneggiamento dì sistemi informatici o telematici
- art 635 quinquies - Danneggiamento di sistemi informatici o telematici di pubblica utilità

6.2.1 Art. 615 ter del codice penale

Accesso abusivo ad un sistema informatico o telematico

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 e' 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.

La norma in esame sanziona introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero mantenersi contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Considerazioni applicative

Il reato è astrattamente ipotizzabile in quanto la Società da in uso macchine il cui sistema operativo è raggiungibile via web.

Occasioni di reato

Ogni volta che si dovesse, entrare nel sistema informatico, sia pure di una sola macchina presso terzi senza autorizzazione e cioè abusivamente e contro la volontà espressa o tacita di chi ha diritto di escludere per fare manutenzioni o verificare dati depositati nel sistema.

Processi aziendali a rischio

Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:

Vendite
ITC
Assistenza tecnica

6.2.2 Art. 615 quater del codice penale
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

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.
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.
Tale norma ha come scopo la protezione della riservatezza delle comunicazioni e delle informazioni che sempre più frequentemente sono trasmesse attraverso i sistemi informatici o telematici.
Vanno considerati non soltanto i sistemi informatici veri e propri, ma anche i personal computer qualora per ricchezza di dati contenuti possono essere considerati un vero e proprio sistema.

La norma in esame sanziona procurare abusivamente, riprodurre, diffondere, comunicare o consegnare codici, parola chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo.

Considerazioni applicative

Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato

Ogni volta che si dovesse procurare abusivamente, riprodurre, diffondere, comunicare o consegnare codici, parola chiave o altri mezzi idonei all'accesso ad un un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo. In altri termini cedere password di accesso attribuite dagli Enti.

Processi aziendali a rischio

Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:

Vendite

ITC
Assistenza tecnica

6.2.3 Art. 615 quinquies del codice penale

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

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.

Tale norma mira a reprimere la diffusione dei c.d. virus informatici, causa di gravi danni ai sistemi telematici. Per virus si intende un programma che contiene istruzioni tali da consentire di essere eseguite indipendentemente dalla volontà di chi l'ha creato e che ha come funzione il danneggiamento di dati e del sistema.
Il Decreto prevede che, in caso di commissione di detti delitti nell'interesse/vantaggio dell'ente, venga applicata la sanzione pecuniaria sino a trecento quote.

Considerazioni applicative

Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato

Ogni volta che si dovesse installare apparecchiature, dispositivi, o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni i dati o i programmi contenuti ovvero favorire l'interruzione totale o parziale del loro funzionamento.

Processi aziendali a rischio

Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:

Vendite
ITC
Assistenza tecnica

6.2.4 Art. 617 quater del codice penale

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

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 e' commesso: 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; 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; da chi esercita anche abusivamente la professione di investigatore privato.

Tale norma mira a reprimere l'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedirle o interromperle o diffondere dati appresi fraudolentemente in qualità di manutentore di sistema.

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse rivelare informazioni raccolte anche accidentalmente da sistemi informativi di terzi.
Ogni volta che si dovesse intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o lo si impedisca o lo si interrompa.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
Vendite
ITC
Assistenza tecnica

6.2.5 Art. 617 quinquies del codice penale

Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a 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.

Tale norma mira a reprimere l'installazione, fuori dai casi consentiti dalla legge, apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse installare apparecchiature per intercettare, impedire o interrompere comunicazioni.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
Vendite
ITC
Assistenza tecnica

6.2.6 Art. 635 bis del codice penale

Danneggiamento di informazioni, dati e programmi informatici

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, 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 di sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.
Tale norma mira a reprimere fuori dai casi in cui la condotta configura un più grave reato, la distruzione, il deterioramento, la cancellazione, l'alterazione o soppressione di informazioni, dati o programmi informatici altrui

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
ITC
Assistenza tecnica

6.2.7 Art. 635 ter del codice penale

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

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, 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.

Tale norma mira a reprimere fuori dai casi in cui la condotta configura un più grave reato, la distruzione, il deterioramento, la cancellazione, l'alterazione o soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da Enti Pubblici o di pubblica utilità

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
ITC
Assistenza tecnica

6.2.8 Art. 635 quater del codice penale

Danneggiamento di sistemi informatici o telematici

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Tale norma mira a reprimere fuori dai casi in cui la condotta configura un più grave reato, la distruzione, il danneggiamento di sistemi informatici o telematici

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
ITC
Assistenza tecnica

6.2.9 Art. 635 quinquies del codice penale

Danneggiamento di sistemi informatici o telematici di pubblica utilità

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 ostacolare 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.
Tale norma mira a reprimere fuori dai casi in cui la condotta configura un più grave reato, la distruzione, il danneggiamento di sistemi informatici o telematici di pubblica utilità

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Forniture di macchine
ITC
Assistenza tecnica

Unità organizzative coinvolte:
ITC
Assistenza tecnica

6.3 Attività sensibili nella Società

L'analisi dei processi aziendali della Società, svolta nel corso del progetto, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 24-bis del d.lgs. 231/2001:

1. l'accesso abusivo a sistemi informatici o telematici;
2. la detenzione e la diffusione di codici di accesso a sistemi informatici o telematici;
3. la diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico o telematico;
4. l'intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche;
5. l'installazione di apparecchiature atte ad intercettare impedire od interrompere comunicazioni informatiche o telematiche;
6. il danneggiamento di informazioni, dati e programmi informatici utilizzati o meno dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
7. il danneggiamento di sistemi informatici o telematici e/o di pubblica utilità;

6.4 Il sistema dei controlli

Il sistema dei controlli, applicabili all'attività individuata, è stato definito utilizzando come riferimento le Linee guida di Assobiomedica, le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali.
È necessario prevedere delle prescrizioni che specifichino le modalità di utilizzo interno della posta elettronica e della rete internet da parte dei lavoratori; devono poi essere indicate le modalità di utilizzo degli strumenti informatici messi a disposizione ed, eventualmente, con quale modalità – preventivamente pubblicizzata nel sistema disciplinare – vengono effettuati i controlli (VEDASI REGOLAMENTO);

E' fatto divieto di effettuare il trattamento dei dati personali mediante sistemi di software ed hardware che mirano al controllo a distanza dei dipendenti. Questi sistemi ad esempio sono:

1) lettura e registrazione dei messaggi di posta elettronica (al di là di quanto strettamente necessario per svolgere il servizio e-mail);
2) riproduzione e memorizzazione di pagine web visitate dal lavoratore;
3) analisi occulta dei computer portatili affidati in uso.

Il Modello di organizzazione, gestione e controllo adottato da EOS fissa i principi (nel proprio codice etico), progetta delle procedure ed implementa i propri sistemi di protezione con una finalità penal preventiva propria di ogni Modello ex D.Lgs. 231/2001.
Tutte le attività devono essere tracciate affinché si possano facilitare controlli sia sui contenuti che sulle modalità, il tutto nel rispetto della normativa della riservatezza.

Il Modello, in relazione all'attività ritenuta sensibile ai sensi dell'art. 24-bis del d.lgs. 231/2001, è strutturato secondo gli standard di controllo specifici che muovono dai sotto elencati elementi dispositivi.

E' fatto espresso divieto, a carico degli esponenti aziendali, in via diretta, ed a carico dei collaboratori esterni, tramite apposite clausole contrattuali, di:

- porre in essere comportamenti tali, da integrare le fattispecie di reato considerate al capitolo 6.3
- porre in essere comportamenti che, sebbene non risultino tali, da costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Premesso che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli, nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

1. Formare un documento informatico falso o alterarne uno vero,
2. contraffare certificati o autorizzazioni,
3. fare apparire adempiute le condizioni richieste per la validità di un documento informatico mediante contraffazione o alterazione del medesimo;
4. simulare la copia di un documento informatico simulando l'esistente di un documento informatico pubblico o privato originale;
5. rilasciare una copia in forma legale o rilasciare una copia di un documento informatico pubblico o privato diversa dall'originale;
6. nell'accedere agli archivi informatici di una pubblica amministrazione, inserire deliberatamente dati falsi negli elaboratori elettronici dell'archivio o modificare quelli esistenti in relazione ad atti o a documenti ivi registrati;
7. attestare falsamente ad un pubblico ufficiale, in un documento informatico pubblico, fatti dei quali l'atto è destinato a provare la verità;
8. scrivere tramite documenti informatici false indicazioni nell'effettuare le registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza o nelle notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali;
9. formare un documento informatico privato falso, o alterare un documento informatico privato vero, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, in tutto o in parte, e fare uso del medesimo documento oppure lasciare che altri ne facciano uso;
10. abusando di un documento informatico del quale si ha il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, scrivere un documento diverso da quello al quale si è obbligati;
11. fare uso di un documento informatico falso redatto da terzi e di cui si conosce la falsità;
12. distruggere, sopprimere od occultare, in tutto o in parte, un documento informatico pubblico o un documento informatico privato vero;
13. introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero mantenersi contro la volontà espressa o tacita di chi ha il diritto di escluderlo;
14. accedere ad un sistema informatico aziendale di terzi per finalità diverse da quelle per le quali si è stati autorizzati;
15. diffondere consapevolmente in sistemi informatici di terzi un programma informatico avente per effetto l'alterazione del funzionamento di sistemi informatici (c.d. Virus);
16. procurare abusivamente, riprodurre, diffondere, comunicare o consegnare codici, parola chiave o altri mezzi idonei all'accesso ad un un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo;

17. procurare abusivamente il codice o la scheda idonei ad accedere al sistema informatico o telematico di terzo protetto (c.d. criptato) da misure di sicurezza;
18. procurare passwords e gli altri mezzi di accesso in violazione di specifiche norme pubblicistiche o privatistiche, anche di tipo contrattuale, poste a salvaguardia della segretezza dei documenti informatici;
19. introdursi abusivamente in un sistema informatico o telematico di pertinenza di terzi;
20. procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi, o programmi informatici diretti a 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;
21. diffondere un programma avente per scopo ed effetto l'alterazione di alcune funzionalità telematiche dei sistemi informatici di terzo;
22. intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedirle o interromperle;
23. installare, fuori dai casi consentiti dalla legge, apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
24. distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui;
25. 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;
26. rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui, o ostacolare gravemente il loro funzionamento, mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici, o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;
27. distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità, o ostacolare gravemente il loro funzionamento, mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici, o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi di conseguenza.

VII. F - REATI COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO RICHIAMATI DALL'ART. 25-septies DEL D.LGS. 231/2001.

7.1 Premessa

L'art. 25 septies è stato introdotto nel Decreto Legislativo 231/2001 dall'art. 9 della L. 3 agosto 2007, n. 123 recante misure in tema di tutela della salute e della sicurezza sul lavoro. Tale articolo è stato nuovamente riformulato in sede di attuazione della delega al Governo per il riassetto della normativa in materia di sicurezza, ad opera del Decreto Legislativo 9 aprile 2008, n. 81 (T.U.S.).
Di recente il Testo Unico è stato ulteriormente modificato dal D.Lgs. 3 agosto 2009.
Il T.U.S., non solo all'art. 300 riformula l'art. 25-septies, ma tratta anche, all'art. 30, delle caratteristiche che gli Enti dovrebbero tenere in debita considerazione nella redazione ed adozione dei loro Modelli di organizzazione, gestione e controllo.

7.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 25 septies:

- art 489 - Omicidio colposo
- art 490 - Lesioni personali colpose

7.2.1 Art. 589 del codice penale

Omicidio colposo

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.
Se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.
Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

Si applica di seguito l'art. 55 D.Lgs 81/2008 relativamente alle sanzioni per il datore di lavoro

La norma sanziona chi cagiona per colpa la morte in conseguenza della omissione della valutazione dei rischi e della completa adozione del documento di valutazione dei rischi (di cui agli articoli 17, comma 1, lettera a e 28 del Testo Unico delle Sicurezza), o in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (di cui all'art. 18 del Testo Unico delle Sicurezza).

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Vendite
Manutenzioni

Unità organizzative coinvolte:
ITC
Assistenza tecnica
Vendite

7.2.2 Art. 590 del codice penale

Lesioni personali colpose

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a 309 euro.
Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da 123 euro a 619 euro; se è gravissima, della reclusione da tre mesi a due anni o della multa da 309 euro a 1.239 euro.
Se i fatti di cui al secondo comma sono commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre

mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.
Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.
Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

Le condotte punite dai reati in esame consistono nel cagionare colposamente la morte o le lesioni personali gravi e gravissime dei lavoratori. Ai fini della commissione di questi reati rileva una qualsiasi condotta, sia attiva (anche non violenta), sia omissiva (consistente nel non aver impedito il verificarsi dell'incidente).
Gli eventi naturalistici previsti dai reati in questione sono per l'art. 589 c.p. la morte e per l'art. 590 c.p. le lesioni gravi e gravissime. Ai sensi delle norme in esame si ravvisano:
(i) **lesioni gravi**:
- se dal fatto deriva una malattia o un'incapacità di attendere alle proprie occupazioni per un tempo superiore ai 40 gg.
- se il fatto produce l'indebolimento permanente di un senso o di un organo;
(ii) **lesioni gravissime**:
- se dal fatto deriva una malattia certamente o probabilmente insanabile;
- se dal fatto deriva la perdita di un senso;
- se dal fatto deriva la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o delle capacità di procreare, ovvero una permanente e grave difficoltà nella favella.
I reati di cui agli articoli 589 e 590 sono reati colposi, ciò significa che l'evento (morte / lesioni) non è voluto dal soggetto agente, ma si è verificato per una negligente inosservanza di leggi, ordini e discipline, miranti a prevenire eventi dannosi o pericolosi da parte di chi aveva l'obbligo di osservarle.
Il concorso di colpa del dipendente non ha alcun effetto esimente (salvo l'ipotesi in cui la condotta del lavoratore si configuri come abnorme, inopinabile ed esorbitante rispetto alle direttive ricevute ed al procedimento lavorativo, nonché atipica ed eccezionale).

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie anche malauguratamente.

Processi aziendali a rischio
Manutenzioni

Unità organizzative coinvolte:
ITC
Assistenza tecnica
Vendite
In generale tutte

7.3 Attività sensibili nella Società

In generale si deve premettere che tutte le attività aziendali devono considerarsi attività in cui potrebbe accadere un infortunio ad un dipendente e devono essere prese in considerazione dal DVR.

Nel DVR sono specificamente indicate le misure di sicurezza che le Società hanno attuato allo scopo di ridurre i rischi ed in particolare i rischi riferibili alle attività lavorative sopra indicate.
Fermo restando quanto sopra, ai fini dell'implementazione del Modello organizzativo 231 con riferimento ai reati presupposto di cui all'art. 25 *septies*, la Società ha considerato di fondamentale importanza (i) verificare che il proprio sistema organizzativo garantisca, su base continuativa ed in maniera formalizzata, lo svolgimento delle attività lavorative nel pieno rispetto e nella corretta applicazione delle norme antinfortunistiche e degli standard di sicurezza posti a presidio della salute e dell'integrità fisica dei dipendenti e (ii) adeguare detto sistema organizzativo, ove necessario.
La Società ai sensi dell'art. 6 del Decreto, ha pertanto individuato come attività a potenziale rischio di violazione delle norme antinfortunistiche le seguenti attività inerenti la gestione della sicurezza aziendale (attività che sono specificamente regolate da norme di legge e/o regole di buona prassi in materie antinfortunistiche):

- gestione delle attività dirette a fornire un adeguato livello di conoscenza al RSSP e agli ASPP sui temi disciplinati dalla normativa di riferimento in tema di salute, igiene e sicurezza sul luogo di lavoro;
- gestione delle attività dirette a offrire un adeguato programma di formazione, in termini di tempo e temi trattati, a tutti i dipendenti aziendali ed in particolare per coloro che svolgono attività più a rischio;
- gestione delle attività di esecuzione ed aggiornamento del *risk assessment*, svolto ai fini della normativa vigente, in tema di salute, igiene e sicurezza sul luogo di lavoro, anche attraverso l'impiego di consulenti esterni alla Società esperti in dette tematiche;
- gestione delle attività di aggiornamento dei presidi di controllo e delle relative procedure, definiti alla luce del *risks assessment* svolto di cui al punto precedente;
- gestione delle attività di redazione del DVR e dei piani di sicurezza nel rispetto della normativa vigente in tema di salute, igiene e sicurezza sul luogo di lavoro interni ed esterni, sia presso le proprie strutture sia presso i siti dei clienti;
- gestione delle attività di verifica costante presso i luoghi di lavoro sul rispetto del DVR e dei piani di sicurezza di cui al punto precedente;
- gestione delle attività di verifica sugli oneri sostenuti per rendere operativi il DVR ed i piani di sicurezza, affinché siano in grado di garantire il massimo livello di sicurezza sui luoghi di lavoro;
- gestione delle attività di manutenzione delle attrezzature, dei macchinari e degli impianti utilizzati, al fine di limitare possibili incidenti da questi provocati;
- gestione delle attività dirette a garantire l'effettuazione di visite mediche secondo protocollo sanitario per ogni categoria lavorativa;
- gestione delle attività di distribuzione, a tutti i lavoratori secondo le mansioni affidate, di dispositivi di protezione individuale e di attrezzature idonee a salvaguardare la salute e la sicurezza degli stessi e di costante verifica sul loro corretto impiego e funzionalità;
- gestione delle attività di monitoraggio sul rispetto degli orari di lavoro da parte del personale, ai fini della prevenzione di infortuni in momenti della giornata potenzialmente più a rischio;
- gestione delle attività di coordinamento tra tutti i soggetti, indicati dal D.Lgs. 81/2008 (ad esempio, datore di lavoro, RSPP, RLS, medico competente), nell'applicazione delle disposizioni in materia di salute, igiene e sicurezza sul luogo di lavoro;

Tutti i Destinatari del Modello adottano regole di condotta conformi ai principi contenuti (i) nel Codice Etico della Società, nella parte dedicata ai principi di condotta nei confronti dei dipendenti e dei collaboratori, che qui si intende integralmente richiamata, (ii) nel Decreto 81 e nella normativa vigente in materia di antinfortunistica, tutela della sicurezza, dell'igiene e della salute nei luoghi di lavoro (iii) nel DVR predisposto dalla Società e nelle procedure ed istruzioni operative e (iv) nel presente Modello.
Devono pertanto intendersi presupposto e parte integrante del presente Modello i principi di comportamento individuati nei C.C.L.L. nel Codice Etico della Società e tutta la

documentazione predisposta dalla Società per l'assolvimento degli obblighi imposti dalla normativa antinfortunistica quali, in via esemplificativa, il DVR, i piani per la gestione dell'emergenza, etc.
Il presente Modello, come già specificato, non deve sostituirsi o duplicare gli obblighi e responsabilità di legge disciplinate in capo ai soggetti individuati dal Decreto 81 e dalla normativa antinfortunistica applicabile. Costituisce, invece, un ulteriore presidio di controllo e verifica dell'adeguatezza delle attività organizzative poste in essere dalla Società per dotarsi di struttura e organizzazione in materia di tutela della sicurezza e della salute nei luoghi di lavoro adeguata, efficiente e pienamente rispondente alla normativa vigente.
Nell'attuazione del proprio sistema organizzativo con specifico riferimento alla sicurezza aziendale e nello svolgimento delle attività dallo stesso programmate la Società ed i Destinatari del presente Modello, ciascuno per quanto di propria competenza, devono osservare tutte le leggi, i regolamenti e le procedure in materia di sicurezza del lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano lo svolgimento delle attività lavorative.

7.4 Il sistema dei controlli

Il sistema dei controlli, applicabili all'attività individuata, è stato definito utilizzando come riferimento le Linee guida di Assobiomedica, le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali.

Le procedure di prevenzione organizzano la gestione della sicurezza aziendale ed in particolar modo le attività di vigilanza e controllo che la Società intende attuare allo scopo di assicurare, al massimo livello possibile, che tutti i soggetti coinvolti nella tutela della sicurezza e della salute nei luoghi di lavoro adempiano correttamente alle previsioni di legge.

Si ribadisce, che i principi e protocolli su cui si fonda il Modello per quanto riguarda la prevenzione dei reati di cui all'art. 25 *septies* sono unicamente volti a monitorare e garantire l'effettiva e piena attuazione delle prescrizioni normative, senza interferire nell'autonomia decisionale e gestionale dei singoli soggetti competenti per legge e per delega in relazione al sistema organizzativo della sicurezza aziendale alla luce della normativa specifica in materia
Per quanto riguarda la **struttura organizzativa della Società e dei suoi impianti** si prevedono i seguenti principi:

- il budget approvato annualmente dalla Società contenga una sezione dedicata che espliciti i fondi destinati all'implementazione ed al mantenimento del sistema di gestione in materia di sicurezza;
- l'organigramma in materia di sicurezza consenta di individuare le responsabilità, i compiti organizzativi e operativi di dirigenti, preposti e le mansioni di ciascun dipendente della Società in materia di sicurezza e dell'igiene e salute sul lavoro;
- l'organigramma della sicurezza sia opportunamente reso conoscibile a tutto il personale a tutti i livelli;
- il datore di lavoro e l'OdV si assicurano che siano nominati tutti i soggetti previsti dalla normativa di settore, che siano muniti di adeguate, chiare e sufficientemente specifiche deleghe, che dispongano delle competenze e qualità necessarie, che abbiano poteri, anche di spesa, sufficientemente adeguati all'incarico e che siano effettivamente esercitate le funzioni e le deleghe conferite;
- il datore di lavoro, prima di procedere alla delega delle proprie funzioni in merito alla sicurezza, o alla nomina di un RSPP o di un medico competente, o di un consulente invia il curriculum di ogni candidato all'OdV, il quale potrà esprimere un parere in merito all'effettiva competenza e adeguatezza dei profili prescelti a ricoprire l'incarico.

Per quanto riguarda l'**attività di formazione ed addestramento** e **l'adempimento degli obblighi in materia di sicurezza da parte di tutti i dipendenti e lavoratori presso gli stabilimenti della Società** si applicano i seguenti principi:

- l'RSPP, avvalendosi anche della collaborazione del medico competente, predisponga il piano annuale di formazione in materia della sicurezza ed il consuntivo delle attività di formazione ed informazione svolte nell'anno precedente e ne invii copia al Consiglio, al Datore di lavoro ed all'OdV;
- sia previsto un sistema che consenta di valutare il livello di apprendimento dei partecipanti ai corsi di formazione in materia di sicurezza ed i risultati siano convenientemente formalizzati;
- sia garantita idonea formazione di lavoratori interinali di cui la Società si avvalga;
- sia garantita un'efficace attività di formazione informazione ed addestramento sui contenuti dei Piani per la gestione delle emergenze
- le mansioni e gli obblighi generali e specifici di ciascuna mansione in materia di sicurezza siano opportunamente resi conoscibili a tutto il personale.

Organizzazione e sviluppo Risorse Umane
Per quanto riguarda l'**attività di gestione operativa in materia di sicurezza** si applicano i seguenti principi:

- sia previsto che i lavoratori comunichino senza indugio all'RSPP ed al RLS le carenze e le anomalie riscontrate nel sistema di gestione della sicurezza adottato dalla Società;
- l'RSPP predisponga prima dell'inizio dell'attività presso gli impianti della Società di terze imprese il DVR che indichi le misure che sono state applicate per eliminare le interferenze; detto documento deve essere allegato al contratto che verrà sottoscritto con l'impresa appaltatrice da parte della Funzione competente (acquisti)alla stipula del contratto;
- sia data tempestivamente notizia all'RSPP dell'introduzione di eventuali nuovi macchinari, nuove apparecchiature, nuove sostanze o prodotti nelle lavorazioni, lo spostamento di macchine ed apparecchiature ed ogni e qualsiasi modifica nei luoghi di lavoro che possa impattare sulla valutazione dei rischi;
- sia previsto che il personale, i rappresentanti sindacali aziendali, il rappresentante dei lavoratori per la sicurezza, il medico competente, i responsabili del servizio di prevenzione e protezione e il datore di lavoro possono segnalare all'OdV informazioni e notizie sulle eventuali carenze nella tutela della salute e sicurezza nei luoghi di lavoro cui non sia dato pronto rimedio da parte della Società;
- il medico competente predisponga e correttamente attui un adeguato piano di sorveglianza sanitaria, di cui dà comunicazione all'RSPP;
- che la consegna dei dispositivi di protezione individuale ai dipendenti sia comprovata dall'apposizione di una firma per ricevuta da parte dei dipendenti;
- che siano conservati dalle Funzioni Responsabili presso gli impianti i libretti e le istruzioni per l'utilizzo delle macchine e delle apparecchiature e che siano aggiornati con le verifiche e le manutenzioni effettuate a norma di legge i record relativamente all'applicativo elettronico di gestione della procedura di gestione e manutenzione impianti;
- siano predisposti, correttamente formalizzati ed aggiornati i Manuali delle procedure per la gestione delle emergenze dove deve essere data adeguata formalizzazione della nomina degli addetti incaricati; delle dotazioni antincendio e di sicurezza disponibili; delle modalità attuate per le verifiche periodiche dei presidi anti incendio e di primo soccorso; delle procedure di intervento che devono essere attuate dagli addetti alle squadre e da tutto il personale per affrontare le situazioni di emergenza;e delle prove di evacuazione effettuate.

Per quanto riguarda l'**attività di monitoraggio, ispezione e controllo** si applicano i seguenti principi:

- l'RSPP coadiuvi i responsabili di Funzione al monitoraggio dell'applicazione delle misure di sicurezza previste nell'ambito delle attività della specifica Funzione coinvolta attraverso la redazione di procedure e/o *check lists* di controllo condivise;
- l'RSPP, l'RLS e il medico competente comunichino al datore di lavoro, ai dirigenti e all'OdV il programma delle visite ispettive annuali programmate ed il numero di visite a

sorpresa ed i verbali delle visite di controllo e delle ispezioni tecniche (specificando ove programmate ed ove a sorpresa) effettuate, evidenziando eventuali non conformità;

- l'RSPP, l'RLS e il medico competente comunichino al datore di lavoro, ai dirigenti e all'OdV ogni impedimento all'esercizio delle loro funzioni affinché siano adottate le decisioni conseguenti;
- i soggetti qualificati come datori di lavoro, l'RSPP ed il medico competente comunichino senza indugio al Consiglio di Gestione gli incidenti che rivestono la natura di lesioni gravi o gravissime circostanziando le carenze, le anomalie e le inadempienze riscontrate; copia della comunicazione sia inviata anche all'OdV;
- l'RSPP renda disponibile copia di ogni DVR ad ogni suo aggiornamento al datore di lavoro, all'OdV e ai RLS;
- i soggetti qualificati come datori di lavoro, RSPP ed il medico competente aggiornino periodicamente (almeno annualmente) il Consiglio e l'OdV della Società in merito alle tematiche relative alla sicurezza sui luoghi di lavoro, ed in particolare fornendo copia del verbale relativo alla riunione annuale di sicurezza prevista dalla normativa;
- in caso di ispezioni amministrative relative agli adempimenti di cui al D.Lgs. 81/2008 o comunque inerenti aspetti della sicurezza partecipino i soggetti a ciò espressamente delegati. L'OdV dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Funzione aziendale di volta in volta interessata; di tutto il procedimento relativo all'ispezione devono essere redatti appositi verbali, che verranno trasmessi all'OdV al quale dovranno essere altresì trasmessi i verbali ed i rilievi dell'autorità di controllo;
- le attività di monitoraggio e verifica del sistema di gestione in materia di sicurezza condotte dall'OdV siano effettuate periodicamente e formalizzate e trasmesse al Consiglio, al Datore di Lavoro ai dirigenti delegati per la sicurezza e all'RSPP.

L'OdV cura che le procedure di attuazione delle procedure di prevenzione sopra indicate siano idonee al rispetto dei principi e delle prescrizioni in essi contenute ed adeguate alle finalità indicate. L'OdV propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

VIII. G - REATI IN TEMA DI VIOLAZIONE DEL DIRITTO D'AUTORE RICHIAMATI DALL'ART. 25- novies DEL D.LGS. 231/2001.

8.1 Premessa

La Legge n° 99 del 23 luglio 2009 all'rt. 15 comma 7, lettera c) ha introdotto nell'articolato del Decreto Legislativo 231/2001 l'art. 25 novies, che integra la lista dei Reati Presupposto per la responsabilità degli Enti con i reati di violazione del diritto d'autore e di altri diritti connessi al suo esercizio.

8.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

I reati presupposto potenziali riscontrati in azienda ex art 25 novies:

- art 171 - legge 633/1941- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio
- art 171 bis - Legge 633/1941

8.2.1 Art. 171 - legge 633/191

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Salvo quanto disposto dall'art. 171 bis e dall'articolo 171 ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
(…)
a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
(…)
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui 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.

La norma punisce la messa a disposizione con immissione in un sistema di reti telematiche, di opere dell'ingegno protette o parti di esse, mediante qualsiasi tipo di connessione. La tutela è estesa anche alle opere altrui non destinate alla pubblicità, la cui diffusione avviene con usurpazione della paternità dell'opera, deformazione, mutilazione o altra modificazione dell'opera medesima.

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse incorrere nella fattispecie

Processi aziendali a rischio
Manutenzioni
Vendite

Unità organizzative coinvolte:
ITC
Assistenza tecnica
Vendite

8.2.2 Art. 171 bis - legge 633/191

Chiunque 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 Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne 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. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.
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 in violazione delle disposizioni di cui agli articoli 64-quinquies e 64- sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

La norma punisce ogni condotta di duplicazione di software che avvenga ai fini di profitto. Di conseguenza, è esposta al rischio di sanzione qualsiasi impresa che, per esempio, utilizzi programmi non originali al fine di ottenere un risparmio oppure che, ed è un caso piuttosto diffuso, pratichi l'installazione di un numero di copie del programma superiore a quello previsto dalla licenza d'uso. Anche il secondo comma dell'articolo in commento è pregnante, in quanto sanziona le violazioni delle disposizioni a protezione delle banche dati: l'impresa che a qualsiasi titolo gestisca una banca dati dovrà predisporre dei protocolli, per esempio, per la trasmissione a terzi di opere contenute in dette raccolte (tipico caso delle aziende farmaceutiche che offrono a medici, in consultazione, articoli di carattere scientifico).

Considerazioni applicative
Il reato è astrattamente ipotizzabile per la Società.

Occasioni di reato
Ogni volta che si dovesse installare un sistema di macchine
La messa a disposizione di pubblicazioni riservate

Processi aziendali a rischio
Installazioni e Manutenzioni
Vendite
marketing

Unità organizzative coinvolte:
ITC
Assistenza tecnica
Vendite
Marketing

8.3 Attività sensibili nella Società

Esaminata la struttura organizzativa di EOS e società del gruppo e le mansioni attribuite ad ogni funzione aziendale e collaborazioni esterne si ritiene che tutte le aree aziendali, in quanto fornite di Personal Computer possano essere considerate aree di rischio.

8.4 Il sistema dei controlli

Il sistema dei controlli, applicabili all'attività individuata, è stato definito utilizzando come riferimento le Linee guida di Assobiomedica, le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché le *best practice* internazionali.
Si tratta di fattispecie che hanno perlopiù attinenza con determinati settori aziendali, quali telecomunicazioni, cinematografia ecc., lontani dall'attività in genere svolta dalle associate di Assobiomedica. Tuttavia, non si esclude che taluni delitti violativi della proprietà intellettuale possano essere commessi.

Si dispone per l'espresso divieto, a carico degli esponenti aziendali, in via diretta, ed a carico dei collaboratori esterni, tramite apposite clausole contrattuali, di:
1. porre in essere comportamenti tali, da integrare le commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633 sopra descritti;
2. porre in essere comportamenti che, sebbene non risultino tali, da costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:
a) abusivamente riprodurre, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere scientifiche o didattiche, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
b) abusivamente fabbricare, importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti coperti da licenze non acquistate;

E' compito dell'OdV monitorare che non emergano all'interno dell'azienda possibili rischi di commissione dei reati previsti dal presente capo e verificare che EOS operi perché:

- si adotti e si preveda adeguata diffusione del Codice etico e comportamentale
- si programmi idonea formazione del personale
- si definisca e si regolamenti l'affidamento e la custodia degli strumenti informatici
- si definisca e si regolamenti i limiti di utilizzo degli strumenti informatici, contemplando di norma la sola possibilità di utilizzo per lo svolgimento delle attività lavorative e non per usi personali
- si dispongano regole sull'utilizzo di dispositivi e di credenziali di accesso e sulla loro utilizzazione, compreso l'uso delle aree dei server aziendali
- si definisca e regolamenti l'impiego della rete internet e della posta elettronica
- sia tracciato l'acquisto, l'installazione e l'utilizzo di software aziendali
- si preveda una procedura gestionale dell'utilizzo – previa corretta autorizzazione – di opere quali: fotografie, relazioni scientifiche, interviste ecc.) non di appartenenza dell'ente.

IX. H - I DELITTI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO

9.1 Premessa

In sede di recepimento delle direttive 2005/60/CE e 2006/70/CE il comma 3 dell'articolo 63 del Dlgs 231/2007 ha inserito nell'ambito del Dlgs 231/2001 l'articolo 25-octies, che ha attratto nell'ambito della responsabilità amministrativa di società ed enti i reati di:

- ricettazione (articolo 648 c.p.)
- riciclaggio (articolo 648-bis c.p.)
- impiego di denaro, beni o utilità di provenienza illecita (articolo 648-ter c.p.).

Successivamente la Legge n. 186 del 15.12.2014, pubblicata sulla Gazzetta Ufficiale n. 292 del 17 dicembre 2014, recante "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio", in particolare, l'articolo 3, comma 5 apporta all'articolo 25-octies del decreto legislativo 231/2001 il reato di autoriciclaggio art 648-ter 1.

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

A tal fine, riportiamo, qui di seguito, una breve descrizione dei reati richiamati dall'art. 25-octies del d.lgs. 231/2001.

9.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a rischio

9.2.1 Art. 648 del codice penale Ricettazione

"Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.
La pena è della reclusione sino a sei anni e delle multa sino a euro 516, se il fatto è di particolare tenuità.
Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile ovvero manchi una condizione di procedibilità riferita a tale delitto".

Fattispecie

Lo scopo dell'incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell'evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

Per "*acquisto*" dovrebbe intendersi l'effetto di un attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.

Il termine "r*icevere*" starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.

Per "*occultamento*" dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.

La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico (come precisato dalla giurisprudenza), tra l'autore del reato principale e il terzo acquirente.

L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".

Il reato di ricettazione può essere remotamente realizzato in poche aree aziendali.

Considerazioni applicative

Il reato è ipotizzabile per la Società.

Occasioni di reato

Rapporti con clienti o fornitori coinvolti in attività illecite ricadenti nelle fattispecie in oggetto.
Ricezione e reimpiego di mezzi finanziari costituenti proventi da attività illecita
Impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale.
Pagamento di prestazioni immateriali o servizi di consulenza che possono a loro volta rilevare quali veicoli di riciclaggio di denaro.

Processi aziendali a rischio

Gestione del processo di acquisto.
Gestione del processo di commercializzazione di prodotti e servizi.
Adempimenti contabili per la gestione di flussi finanziari e di transazioni finanziarie.
Organizzazione di congressi o eventi
Funzioni / Aree aziendali a rischio

Amministratori
Personale e Amministrazione e Finanza
Marketing
Vendite

9.2.2 Art. 648-bis del codice penale Riciclaggio.

"Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da lire due milioni a lire trenta milioni.
La pena è aumentata quando il fatto commesso nell'esercizio di un'attività professionale.
La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'art. 648".

Fattispecie

Lo scopo dell'incriminazione del reato di riciclaggio è quello di impedire che gli autori dei reati possano far fruttare i capitali illegalmente acquisiti, rimettendoli in circolazione come capitali ormai "depurati" e perciò investibili anche in attività economiche produttive lecite. In tal modo, la norma incriminatrice persegue anche un ulteriore obiettivo-finale, vale a dire scoraggiare la stessa commissione dei reati principali, mediante le barriere frapposte alla possibilità di sfruttarne i proventi.

Per "sostituzione" si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Il "trasferimento" consiste nella condotta tendente a ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.

Le "operazioni" idonee ad ostacolare l'identificazione dell'illecita provenienza potrebbero essere considerate quelle in grado di intralciare l'accertamento da parte della autorità giudiziaria della provenienza delittuosa dei valori provenienti dal reato.

Come sopra visto, al delitto si ricollegano un'aggravante e un'attenuante. L'aggravante è ravvisata nei confronti di chi compie il reato esercitando un'attività professionale della quale, quindi, abusa. L'attenuante attiene al reato presupposto e tiene conto dell'esigenza di ridurre una pena edittale molto pesante in casi in cui, in sostanza, si riciclano utilità e si ostacola l'identificazione di proventi che conseguono a delitti non gravi.

Considerazioni applicative
Occasioni di reato
Processi aziendali a rischio
Funzioni / Aree aziendali a rischio

Valgono le medesime considerazioni sub art. 648.

9.2.3 Art. 648-ter
Impiego di denaro, beni o utilità di provenienza illecita

"***Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da lire due milioni a lire trenta milioni.***
La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.
La pena è diminuita nell'ipotesi in cui al secondo comma dell'art. 648. Si applica l'ultimo comma dell'art. 648".

Fattispecie

Anche in questa fattispecie, è prevista la circostanza aggravante dell'esercizio di un'attività professionale ed è esteso ai soggetti di cui all'ultimo comma dell'art. 648, ma la pena è diminuita se il fatto è di particolare tenuità.

L'inserimento nel codice del delitto in esame nasce dal rilievo che i profitti della criminalità organizzata debbono essere contrastati tenendo conto di una duplice prospettiva: mentre in un primo momento occorre impedire che il c.d. "denaro sporco", frutto dell'illecita accumulazione, venga trasformato in denaro pulito, in un secondo momento è necessario fare in modo che il capitale, pur così emendato dal vizio di origine, non possa trovare un legittimo impiego.

La condotta, espressa dall'inciso "*impiega in attività economiche o finanziarie*", consente due rilievi. Da un lato il riferimento specifico alle attività finanziarie intende con evidenza coinvolgere la vasta cerchia di intermediari, bancari e non, i quali operano in questo campo. D'altro lato tale coinvolgimento, a titolo di concorso nel reato, è favorito dal verbo "impiegare" la cui accezione è per certo più ampia rispetto al termine "investire", che suppone un impiego finalizzato a particolari obiettivi, ed esprime il significato di "usare comunque".

Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente di escludere la funzione meramente professionale (sanitaria, educativa, ecc.), dove ha assoluta prevalenza l'aspetto intellettuale (es.: costituzione di uno studio medico); non naturalmente quando essa si accompagni ad una struttura di tipo imprenditoriale (per esempio il denaro di illecita provenienza è impiegato nella costruzione e attrezzatura di una clinica privata). Esclusi i profili sic et simpliciter professionali, è opportuno porre in rilievo che il termine in esame consente del pari di non comprendere nella sfera di operatività della norma gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico. Inoltre la funzione integrativa e, per così dire residuale dell'illecito in esame emerge dal rilievo che esso resta escluso, oltreché, come indicato nel caso di concorso nei reati presupposti, altresì quando risultino realizzate le ipotesi criminose degli artt. 648 e 648-bis.

Considerazioni applicative
Occasioni di reato
Processi aziendali a rischio
Funzioni / Aree aziendali a rischio

Valgono le medesime considerazioni sub art. 648.

9.2.4 Art. 648-bis 1 Autoriciclaggio

"Chiunque impiega i proventi di un delitto non colposo in attività economiche o finanziarie, ovvero li impiega con finalità speculative, è punito con la reclusione da quattro a dodici anni e con la multa da euro 10.000 ad euro 100.000, se dal fatto deriva nocumento alla libera concorrenza, alla trasparenza e all'andamento dei mercati.
Se i proventi derivano da un delitto doloso per il quale è stabilita la pena della reclusione nel massimo fino a cinque anni, si applica la pena della reclusione fino a sei anni.
La pena è aumentata se il fatto è commesso nell'esercizio di un'attività professionale, bancaria o finanziaria.
La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648.
Si applica in ogni caso l'ultimo comma dell'articolo 648".

Fattispecie

L'Autoriciclaggio identifica le attività di ripulitura di proventi illeciti, mediante una serie di operazioni che consentono di nascondere la provenienza delittuosa e di trasformarli in capitali leciti da immettere sul mercato.
La norma punisce colui che dopo aver commesso o concorso a commettere un delitto non colposo impiega, sostituisce o trasferisce denaro beni o altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
In virtù delle disposizioni di autoriciclaggio la responsabilità amministrativa dell'ente sorge se la persona, ad essa appartenente, pone in essere le condotte di riciclaggio o reimpiego di denaro o beni provenienti da reati che ha direttamente compiuto, o che ha concorso a compiere.

Anche in questa fattispecie, è prevista la circostanza aggravante dell'esercizio di un'attività professionale ed è esteso ai soggetti di cui all'ultimo comma dell'art. 648, ma la pena è diminuita se il fatto è di particolare tenuità.

L'inserimento nel codice del delitto in esame nasce dal rilievo che i profitti da reato debbono essere contrastati facendo in modo che il capitale non possa trovare un legittimo impiego.

L'impatto del nuovo reato riguarda, da un lato, la movimentazione dei flussi finanziari illeciti provenienti dall'esterno della società (che devono essere «reinvestiti»/reimmessi nell'ente), dall'altro, il flusso delle provviste illecite formatesi all'interno dell'ente (c.d. «endogene» all'ente), a cui segua un'ulteriore condotta che sia di concreto ostacolo alla identificazione della provenienza delittuosa del bene, del denaro o dell'altra utilità oggetto del reato.

Considerazioni applicative

Il reato è ipotizzabile per la Società.

Occasioni di reato

Operazioni finanziarie o di investimento effettuate con denaro di provenienza delittuosa

Processi aziendali a rischio

Gestione del processo di acquisto.
Gestione del processo di investimento.

Gestione del processo di trasferimento di disponibilità e di transazioni finanziarie.
Organizzazione di congressi o eventi

Funzioni / Aree aziendali a rischio

Amministratori
Amministrazione e Finanza

9.3 Attività sensibili per la Società

L'analisi dei processi aziendali della Società, svolta nel corso del progetto, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-octies del d.lgs. 231/2001. Qui di seguito vengono indicate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita:

1. Gestione dei flussi finanziari e delle transazioni finanziarie con controparti
2. Gestione di contratti di acquisto e/o vendita con controparti
3. gestione delle sponsorizzazioni

9.4 Il sistema dei controlli

Il sistema dei controlli, applicabili alle attività individuate, è stato definito utilizzando come riferimento le Linee guida di Confindustria e quelle ad oggi pubblicate dalle principali associazioni di categoria nonché le best practice internazionali, ed è stato successivamente adottato dalla Società.

Per tutte le attività sensibili devono essere rispettati gli standard di controllo fissi di cui alla precedente sezione II, nonché i seguenti standard di controllo specifici.

M_11 **Identificazione; Verifica:** deve essere verificata l'identità e l'attendibilità commerciale e professionale dei fornitori e partner commerciali e finanziari sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici – protesti, procedure concorsuali – o acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di persone politicamente esposte come definite all'art. 1 dell'allegato tecnico del d.lgs. 231/2007);

N_12 **Verifiche dei pagamenti:** deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza tra destinatari /ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;

O_13 **Controlli su flussi finanziari:** devono essere effettuati controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti /operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio di terrorismo etc.), degli Istituti di credito utilizzati di credito (sede legale delle banche coinvolte nelle operazioni e istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;

P_14 **Divieto di uso di denaro contante:** deve esistere un divieto di utilizzare denaro

contante oltre limiti predeterminati e di importo esiguo nell'ambito di operazioni di cassa aziendale per spese bagatellari;

Q_15 **Verifiche di tesoreria:** devono essere effettuate delle verifiche sulla Tesoreria (es. rispetto delle soglie per i pagamenti in contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità etc.);

R_16 **selezione tecnica di fornitori:** occorre determinare i requisiti minimi dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard;

S_17 **SLA:** deve essere identificata una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard;

T_18 **gestione dei contratti con clienti e fornitori**: deve essere identificato un organo /unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità;

U_19 **Regole disciplinari:** devono esistere regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio;

V_20 **joint venture:** devono essere determinati i criteri di selezione, stipulazione ed esecuzione di accordi /joint venture con altre imprese per la realizzazione di investimenti;

Z_21 **Documentazione:** deve esistere un'adeguata documentazione degli accordi /joint venture ed obbligo di conservare la relativa documentazione in apposito archivio, con divieto di cancellare o distruggere i documenti archiviati;

AA_22 **congruità degli investimenti:** deve essere verificata della congruità economica di eventuali investimenti effettuati in joint venture (es. rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di due diligence etc.);

BB_23 **compliance di gruppo:** deve essere verifcato il livello di adeguamento delle società controllate rispetto alla predisposizione di misure e controlli antiriciclaggio;

CC_24 **Formazione del personale in materia antiriciclaggio**: devono essere adottati adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

DD 25 Tax Control Framework, che costituisce strumento volto a prevenire le irregolarità fiscali e, di conseguenza, anche l'autoriciclaggio, scongiurando cioè il rischio che i proventi derivanti dalla commissione dei reati tributari possano essere autoriciclati nello svolgimento dell'attività economica, imprenditoriale o finanziaria delle società.

X. I - REATI CONTRO LA PERSONALITA' INDIVIDUALE RICHIAMATI DALL'ART. (art. 25-*quinquies del d.lgs 231/2001*);

5.1 Premessa

I profili di rischio rilevanti con riferimento ai reati previsti dall'art. 25-quinquies del d.lgs. 231 del 2001 possono, verosimilmente, ravvisarsi con riferimento ai soli casi in cui la società agisca in concorso con soggetti terzi.
In proposito va sottolineato che, affinché sussista la possibilità di imputare l'illecito alla società, è necessario che il reato sia stato commesso nell'interesse o a vantaggio della società medesima e non semplicemente avvalendosi della sua struttura per il perseguimento di profitto riferibile esclusivamente al soggetto attivo.

5.2 Repertorio dei reati ed individuazione delle aree e funzioni aziendali a

rischio

5.2.1 Reati finalizzati alla repressione della tratta di persone.

Si ritengono attività a rischio quelle connesse all'agevolazione, in qualsiasi forma, di singoli o associazioni, che:
- riducano o mantengano una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento (art. 600 c.p.);
- pongano in essere tratta di persone che si trovino nelle condizioni sopra indicate, ovvero le inducano o le costringano, in qualsiasi modo, a fare ingresso o a soggiornare o a uscire dal territorio italiano o a trasferirsi al suo interno (art. 601 c.p.);
- acquistino o alienino o cedano una persona che si trova in una delle condizioni sopra descritte (art. 602 c.p.).

A titolo esemplificativo, si segnala che potrà configurarsi un'ipotesi di concorso dell'ente nei reati di riduzione o mantenimento in schiavitù o servitù, tratta di persone, acquisto e alienazione di schiavi, commessi da terzi (e quindi, ove sussista un interesse o un vantaggio per la società, una responsabilità per il conseguente illecito di questa) nel caso in cui la società fornisca ad un soggetto le risorse economiche necessarie per la costituzione o il mantenimento di una struttura organizzativa finalizzata allo sfruttamento di prostitute o lavoratori non regolari, ovvero a favorire il loro ingresso nel nostro paese a fini di sfruttamento.

Considerazioni applicative

Il reato appare remoto anche se è astrattamente ipotizzabile per la Società in caso di ricorso diretto o indiretto a manodopera o subforniture.

Occasioni di reato

Stipulazione di contratti di appalto mediante i quali vengono corrisposte risorse economiche per la costituzione o il mantenimento di una struttura organizzativa finalizzata allo sfruttamento di lavoratori non regolari, ovvero a favorire il loro ingresso nel nostro paese ai fini di sfruttamento.
Assunzione di lavoratori non regolari.

Processi Aziendali a rischio

Adempimenti relativi alla selezione e all'assunzione di personale interinale.
Gestione di contratti di appalto

Funzioni / Aree aziendali a rischio

Amministratori

5.2.2 Reati finalizzati alla repressione del caporalato

"Intermediazione illecita e sfruttamento del lavoro (art**. 603 bis c.p**.) ", in base a cui si stabilisce:
- Salvo che il fatto costituisca piu' grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:
1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di

sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.
Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.
Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o piu' delle seguenti condizioni:
1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali piu' rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantita' e qualita' del lavoro prestato;
2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.
Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla meta':
1) il fatto che il numero di lavoratori reclutati sia superiore a tre;
2) il fatto che uno o piu' dei soggetti reclutati siano minori in eta' non lavorativa;
3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro».

Considerazioni applicative

Il reato è astrattamente ipotizzabile per la Società con riferimento all'impiego di personale proveniente da subappalti.

5.3 Attività sensibili nella Società

L'analisi dei processi aziendali della Società, svolta nel corso del progetto, ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-quinquies del d.lgs. 231/2001. Qui di seguito vengono indicate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati contro la personalità individuale:

1. Attività che prevedono il ricorso diretto o indiretto a manodopera (es.: affidamenti di appalti).

2. Gestione di server della Società o di siti Internet.

5.4 Il sistema di controlli

Il sistema dei controlli, applicabili alle attività individuate, è stato definito utilizzando come riferimento le Linee guida di Confindustria, e le linee guida ad oggi pubblicate dalle principali associazioni di categoria, nonché dalle best practice internazionali.

Per ognuna delle attività devono essere rispettati gli standard di controllo fissi di cui alla Sezione II, nonché i seguenti standard di controllo specifici.

Relativamente all'attività sensibile relativa allo svolgimento di "**attività che prevedono il ricorso diretto o indiretto a manodopera (es.: affidamenti di appalti)**" gli standard di controllo specifici sono i seguenti:

A_1 **selezione del personale interinale**: l'assunzione di tale personale deve avere luogo in conformità alla normativa vigente, tramite società di somministrazione di lavoro temporaneo debitamente autorizzate.

B_1 **sub-appalto**: i contratti di sub-appalto dei propri fornitori devono essere soggetti ad autorizzazione scritta previa verifica dei sub-appaltatori.

Relativamente all'attività sensibile di "**gestione di server della Società o di siti Internet**" gli standard di controllo specifici sono i seguenti:

A_3 **Sicurezza informatica**: devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di Information Security Management System.

A_4 **Divieto di acquisire, utilizzare, diffondere e/o cedere** materiale pedo-pornografico.

5.4.1 Principi generali di comportamento ad evitare contatti con reclutatori o ferme di "caporalato"

E' fatto divieto di contrarre per forniture, lavori e servizi con i nominativi ovvero organizzazioni che praticano forme di reclutamento intermediando illecitamente con sfruttamento del lavoro e, qualora fossero individuati, si deve congelare il rapporto e le eventuali prestazioni e corresponsioni pecuniarie che ne fossero maturate nel frattempo.

Per maggiore cautela relativamente alle modalità più utili per mitigare qualsiasi rischio di relazione con soggetti associati che possano praticare forme di reclutamento illecite , la società provvederà ad aggiornare il proprio contratto standard di fornitura di servizi specificatamente menzionando che qualora fosse determinato illecito ex art 603 bis viene a cadere ogni rapporto con diritto a pretendere eventuali danni.
Sarà compito del responsabile acquisti nel raccogliere la firma di presa d'atto del modello significare sia all'appaltatore e sia al sub appaltatore, che avrà superato la medesima analisi di affidabilità, fare sottoscrivere la presa di conoscenza del Modello di Organizzazione Gestione e controllo di EOS Srl e l'adesione al Codice Etico di EOS Srl. Il comportamento mira a prevenire qualsiasi comportamento illecito sia di appaltatori sia di sub appaltatori.
Il controllo sulla insussistenza di qualsiasi problematica è consentito dal contratto che prevede il diritto di accesso ai documenti aziendali del fornitore per valutare il comportamento.
Il responsabile, qualora se ne verificasse la circostanza di rendersi opportuno un accesso, ne darà notizia all'Amministratore.
Le prassi saranno le seguenti:

- Accesso consentito con ampia disponibilità e riscontro documentale positivo il contratto continua con segnalazione agli Amministratori;
- Accesso non consentito ovvera scarsa disponibilità al riscontro, ovvero documentazione non probatoria o mancante il responsabile segnalerà agli Amministratori la circostanza al fine della interruzione del rapporto;

L’eventuale evidenziazione dovrà essere segnalata, una volta accertato il fondamento su possibili anomalie del rapporto, anche all’OdV.

ALLEGATO 1
DELEGHE

ALLEGATO 2
POTERI DI FIRMA OPERATIVI

ALLEGATO 3
POTERI DI FIRMA BANCARI

ALLEGATO 4A

Dichiarazione
MOD. CONSULENTE

Il sottoscritto,

Nome e Cognome: ……..……

N. matricola: ……..……

in qualità di Consulente nominato in data …/…/ …/…/ …/…/…/…/… in relazione alla seguente categoria di operazioni: ……..……

dichiara

- di essere pienamente a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento dell'incarico, con particolare ma non esclusivo riferimento alle procedure interne che lo riguardano come da estratto; e

si impegna

- a non commettere alcuno dei reati considerati dal d. lgs. n. 231/01 e successive modifiche ed integrazioni e a non commettere violazioni delle procedure interne e dei protocolli del modello di organizzazione, gestione e controllo adottato dalla Società, come descritti o riferiti nel Modello; e
- a fornire al Responsabile e all'Organismo, a loro semplice richiesta, qualsiasi informazione o documentazione necessaria o opportuna in relazione alla suddetta categoria di

Operazioni.

…… ……

Data Firma del Consulente

DICHIARAZIONE DI RICEVUTA

(*da compilarsi a cura dell'Organismo di Vigilanza)*

Il sottoscritto, in qualità di membro dell'Organismo di Vigilanza, dichiara di aver ricevuto il presente modulo.

……. …….

Data Firma

ALLEGATO 5B

Dichiarazione
MOD. PARTNER

Il sottoscritto,

Denominazione: ……

Sede: ……

rappresentante ……

in qualità di partner commerciale della Società in relazione alla seguente categoria di Operazioni: ……

dichiara

- di essere pienamente a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento delle Operazioni; e

si impegna

- a improntare i comportamenti finalizzati all'attuazione dell'iniziativa comune alla Società a principi di trasparenza e di correttezza e nella più stretta osservanza delle disposizioni del Decreto; e
- a fornire al Responsabile e all'Organismo di Vigilanza della Società, a loro semplice richiesta, qualsiasi informazione o documentazione necessaria o opportuna in relazione alla suddetta categoria di Operazioni.

…… ……

Data Firma del Partner

DICHIARAZIONE DI RICEVUTA

(*da compilarsi a cura dell'Organismo di Vigilanza*)

Il sottoscritto, in qualità di membro dell'Organismo di Vigilanza, dichiara di aver ricevuto il presente modulo.

…….. ……

Data Firma