Modello di Organizzazione, Gestione e Controllo

Versione 1.0 del 13 aprile 2021

INDICE

PARTE SPECIALE

Premesse

La presente parte speciale è relativa alla descrizione dei reati presupposto così come previsti dal D.Lgs. 231/2001 oltre alla valutazione dei rischi – *risk assessment*.

L'attività di analisi è stata svolta tenendo in considerazione gli aspetti che caratterizzano l'Ente in questione, in particolare:

- Attività in cui l'Ente opera,
- Struttura organizzativa,
- Sistema di deleghe e procure,
- Adozione di protocolli, procedure e istruzioni operative,
- Sistema di controllo interno.

Le risultanze di tale attività di analisi sono riassunte nella tabella contenuta nella presente sezione.

Metodologia di analisi

La metodologia adottata per l'analisi del rischio prevede per ciascun reato presupposto ai fini del D.Lgs. n. 231/01 venga fatta un'analisi che così si sintetizza:

- Individuazione delle attività all'interno delle quali i rischi possono manifestarsi,
- Livello di rischio connesso al singolo reato in base all'attività,
- Individuazione delle funzioni aziendali potenzialmente responsabili della commissione dei reati.

L'attività di *risk assessment* trova il suo fondamento in due elementi fondamentali:

- L'impatto: valutato su cinque livelli (molto basso – basso - medio – alto – molto alto) in funzione all'aspetto sanzionatorio e all'impatto reputazionale
- La probabilità fa riferimento a cinque parametri:

- Frequenza
- Rilevanza
- Accadimenti precedenti
- Poteri e strumenti
- Discrezionalità

Tali valori sono stati resi oggettivi nel rispetto della sottostante tabella:

Min	Max	Probabilità
0	1	MOLTO BASSA
1,1	2	BASSA
2,1	3	MEDIA
3,1	4	ALTA
4,1	5	MOLTO ALTA

La risultanza congiunta dei due valori fornisce l'indicazione del rischio preliminare di cui alla sottostante matrice:

		PROBABILITA'				
		MOLTO BASSA	**BASSA**	**MEDIA**	**ALTA**	**MOLTO ALTA**
IMPATTO	**MOLTO ALTO**	BASSO	MEDIO	ALTO	MOLTO ALTO	MOLTO ALTO
	ALTO	MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO
	MEDIO	MOLTO BASSO	BASSO	BASSO	MEDIO	ALTO
	BASSO	MOLTO BASSO	MOLTO BASSO	BASSO	BASSO	MEDIO
	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO	BASSO

L'analisi del sistema di controllo interno è altro elemento necessario per l'attività di *risk assesment.*
Il sistema dei controlli viene valutato sulla base di alcuni parametri che di seguito si evidenziano:

- **Esistenza di principi o regole di comportamento**: tale aspetto è un indice dell'esistenza di regole interne con evidenza delle aree del fare e del non fare a presidio dei processi aziendali.

- **Esistenza di deleghe / procure formalizzate**: tale aspetto è un buon indice, oltre che di chiarezza organizzativa, anche di esistenza di sistemi di deleghe dal vertice aziendale verso il basso e quindi di decentramento decisionale e diffusione delle responsabilità.

- **Esistenza di misure organizzative adeguate (aggiornamento di regolamenti, policy, procedure, disposizioni organizzative)**: tale aspetto risulta rilevante in quanto permette di valutare quanto il sistema aziendale sia formalizzato attraverso un sistema interno di regole che consenta di chiarire le modalità operative e le relative responsabilità, nell'ottica del *chi fa, che cosa, come*. Questo aspetto può essere considerato un tassello chiave sul quale poi implementare il sistema di controllo, una volta adottato il Modello di organizzazione e gestione.

- **Segregazione dei compiti (o sistema autorizzativo)**: la segregazione dei compiti e dei poteri in ambito aziendale è uno strumento fondamentale di *Corporate Governance*, finalizzato al coinvolgimento dei soggetti con diversi poteri decisionali, affinché nessuno possa disporre di poteri illimitati e svincolati dal controllo e dalla verifica di altri soggetti. La segregazione dei compiti a valenza diversa (autorizzativa, esecutiva, di controllo/monitoraggio) è un buon indice del sistema interno preventivo, salva la collusione tra i soggetti stessi, nella commissione dei reati.

- **Tracciabilità**: la valutazione del parametro "Tracciabilità" attiene all'esistenza di un valido supporto documentale tale da consentire di ricostruire con precisione la storia delle decisioni e dei provvedimenti aziendali, delle responsabilità coinvolte e delle valutazioni eseguite a supporto delle decisioni;

- **Esistenza ed efficacia dei controlli interni**: tale valutazione attiene al livello di attuale implementazione di sistemi di controllo e di monitoraggio che, anche in assenza di un Modello organizzativo, comunque l'azienda ha inteso realizzare per la prevenzione di rischi (a diversi livelli).

Ognuno di questi elementi è stato reso oggettivo utilizzando una scala di valori la cui somma fornisce il livello di controllo. L'incrocio tra i valori associabili al rischio preliminare e il livello di controllo esprime il cosiddetto rischio residuo. Tale rischio si esprime in una scala di cinque livelli, di cui alla sottostante matrice:

		RISCHIO				
		MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO
CONTROLLO	MOLTO ALTO	MOLTO BASSO	MOLTO BASSO	BASSO	MEDIO	MEDIO
	ALTO	MOLTO BASSO	MOLTO BASSO	BASSO	MEDIO	ALTO
	MEDIO	MOLTO BASSO	MOLTO BASSO	BASSO	MEDIO	ALTO
	BASSO	MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO
	MOLTO BASSO	MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO

A seguito delle analisi condotte è stato elaborato un prospetto che si allega alla presente in cui vengono catalogati i reati presupposto di cui al D.Lgs. 231/01 in base al livello di rischio determinato considerando l'attuale organizzazione di LABA.

In particolare, si riscontra un livello di **rischio alto** per le seguenti categorie di reato :

- Art. 25 quinquiesdecies - Reati tributari
- Art. 25 - octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Il livello di rischio è **medio o basso** per le seguenti categorie di reato :

- Art. 24 *bis* – Delitti informatici e trattamento illecito di dati
- Art. 25 *ter* – Reati societari
- *Art. 25* – Reati commessi nei rapporti con la Pubblica Amministrazione
- Art. 25 *septies* – Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
- Art. 25 *novies* – Delitti in materia di violazione del diritto d'autore
- Art. 25 *quinquies* – Delitti contro la personalità individuale
- Art. 25 *decies* – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria,
- Art. 25 *duodecies* – Impiego di lavoratori irregolari

Il livello di rischio è **molto basso ovvero non configurabile** per le seguenti categorie di reato :

- Art. 24 *ter* – Delitti di criminalità organizzata
- Art. 25 *bis1* – Reati contro l'industria e il commercio
- Art. 25 - *bis* - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
- Art. 25 *quater* – Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali
- Art. 25 *quater* 1 – Pratiche di mutilazione degli organi genitali femminili
- Art. 25 *sexies* – Abusi di mercato
- Art. 25 - *terdecies* - Razzismo e xenofobia
- Art. 25 *undecies* – Reati ambientali

PARTE SPECIALE

"A"

Reati nei Rapporti con la P.A.

A) CORRUZIONE E CONCUSSIONE

Art. 317 del codice penale - Concussione*

*Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni.***

*Nella concussione il privato è mero soggetto passivo, che subisce la condotta del pubblico ufficiale.
** Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190 e dall'art. 1 della legge 69 del 27 maggio 2015.

Art. 318 del codice penale - 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 od altra utilità, o ne accetta la promessa, è punito con la reclusione da uno a sei anni.**

* Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190 e dall'art. 1 della legge 69 del 27 maggio 2015.

Art. 319 del codice penale - 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.***

* La corruzione è reato a concorso necessario, in cui vengono puniti sia il Corrotto che il Corruttore, in quanto tra gli stessi esiste un accordo finalizzato ad ottenere un vantaggio reciproco. Per stabilire se un atto sia o meno contrario ai doveri d'ufficio occorre aver riguardo non soltanto all'atto in sé ma anche alla sua conformità a tutti i doveri di ufficio che possono venire in considerazione con la conseguenza che un atto può essere in se stesso non illegittimo e ciò nondimeno essere contrario ai doveri di ufficio.

** Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190 e dall'art. 1 della legge 69 del 27 maggio 2015.

Art. 319-bis del codice penale - Circostanze aggravanti

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

Art. 319-ter del codice penale - Corruzione in atti giudiziari

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni.
*Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni.**

* Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190 e dall'art. 1 della legge 69 del 27 maggio 2015.

Art. 319-quater del codice penale – 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 punico 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 punto con la reclusione fino a tre anni.
* Articolo introdotto dall'articolo 75 della L. 6 novembre 2012 n. 190 e modificato con legge 69 del 27 maggio 2015.

Art. 320 del codice penale - Corruzione di persona incaricata di un 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.

Art. 321 del codice penale - Pene per il corruttore

Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell' articolo 319-bis, nell' art. 319-ter e nell'articolo 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 od altra utilità.

Art. 322 del codice penale - Istigazione alla corruzione*

Chiunque offre o promette denaro od 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'articolo 318, ridotta di un terzo.

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a 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'articolo 319, ridotta di un terzo.

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

* Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190

Art. 322-bis del codice penale - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri *

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5 bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari ed agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale.

Le disposizioni degli articoli 319 quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria[1].

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

* Articolo così modificato dall'articolo 75 della L. 6 novembre 2012 n. 190

B) TRUFFA AI DANNI DELLO STATO

Art. 640 del codice penale - Truffa

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 euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1. se il fatto è commesso a danno dello Stato o di un 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;

[1] Tale ultimo inciso è stato aggiunto dalla legge 116 del 3 agosto 2009, recante "ratifica ed esecuzione della convenzione dell'organizzazione delle Nazioni Unite contro la corruzione adottata dall'Assemblea generale dell'ONU il 31 ottobre 2003 nonché norme dia adeguamento interno e modifiche al codice penale ed al codice di procedura penale". Tale nuova formulazione amplia in maniera rilevante le ipotesi di rischio.

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 un'altra circostanza aggravante.

Art. 356 del codice penale - Frode nelle pubbliche forniture

Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032.
La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente.

C) FRODE INFORMATICA

Art. 640-ter del codice penale - 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 o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

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

**Tale fattispecie* di reato assume rilievo, ai fini del Decreto, solo se realizzata in danno della P.A.
***Articolo così modificato dall'articolo 9 del Decreto Legge 14 agosto 2013 n. 93, poi convertito con modificazioni in Legge 15/10/2013 n. 119.*

D) REATI IN TEMA DI EROGAZIONI PUBBLICHE

Art. 316-bis del codice penale - Malversazione a danno dello Stato

Chiunque, estraneo alla pubblica amministrazione, 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 od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.

Art. 316-ter del codice penale - Indebita percezione di erogazioni a danno dello Stato

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 ad euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da euro 5.164 a euro 25.822. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Art. 640-bis del codice penale - Truffa aggravata per il conseguimento di erogazioni pubbliche

La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 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.

****

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, abusando della sua qualità o dei suoi poteri, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovute.
Tale forma di reato (residuale nell'ambito delle fattispecie di cui al D.Lgs. 231/2001) potrebbe ravvisarsi nell'ipotesi in cui un dipendente concorra nel reato del pubblico ufficiale o di un incaricato di pubblico servizio, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che da tale comportamento ne derivi, in qualche modo, un vantaggio per la Ente).

Corruzione per l'esercizio della funzione e Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318, 319, 320 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, riceva, per sé o per altri, denaro o altra utilità, o ne accetta la promessa, per l'esercizio delle sue funzioni o dei suoi poteri, per omettere o ritardare un atto del suo ufficio o per compiere un atto contrario al suo ufficio.

Tale fattispecie si realizza quando si determini un vantaggio a favore dell'offerente, in relazione ad un atto dovuto (ad esempio la velocizzazione di una pratica la cui evasione è di propria competenza), ovvero un atto contrario ai doveri del pubblico ufficiale (ad esempio garantire l'aggiudicazione di una gara) o dell'incaricato di pubblico servizio.

Istigazione alla corruzione (art. 322 c.p.)

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale non accetti l'offerta o la promessa.

Corruzione in atti giudiziari (art. 319 ter)

Tale ipotesi si configura nel caso in cui i reati di corruzione per un atto d'ufficio o contrario ai doveri d'ufficio, siano commessi per favorire la Ente quale parte in un processo civile penale o amministrativo.

Induzione indebita a dare o promettere utilità (art. 319 quater)

Tale ipotesi si configura quando 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.

Malversazioni a danno dello Stato o dell'U.E. (art. 316-bis c.p.).

Tale ipotesi di reato si configura nel caso in cui un soggetto, estraneo alla Pubblica Amministrazione, dopo avere ricevuto dallo Stato o da altro Ente Pubblico o dalla Comunità Europea contributi, sovvenzioni o finanziamenti, destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destini secondo le predette finalità.

Il reato può configurarsi anche con riferimento a finanziamenti già ottenuti in passato, che ora non vengano destinati alle finalità per cui erano stati erogati (tenuto conto che il momento in cui si consuma il reato coincide con la fase esecutiva).

Indebita percezione di erogazioni a danno dello Stato o dell'U.E. (art. 316-ter c.p.).

Tale ipotesi di reato si configura nei casi in cui 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 dalla Comunità Europea.

Tale ipotesi (residuale) di reato si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Il reato si realizza nel momento dell'ottenimento del finanziamento, non rilevando in questo caso l'uso fatto delle erogazioni.

Frode nelle pubbliche forniture (art. 356 c.p.)

Tale fattispecie punisce chiunque commette frode nell'esecuzione di contratti di fornitura conclusi con lo Stato, con un ente pubblico, o con un'impresa esercente servizi pubblici o di pubblica necessità. All'ente possono essere applicate sia le sanzioni pecuniarie che interdittive.

Per «contratto di fornitura» si intende ogni strumento contrattuale destinato a fornire alla P.A. beni o servizi. Il delitto di frode nelle pubbliche forniture è ravvisabile non soltanto nella fraudolenta esecuzione di un contratto di somministrazione (art. 1559 c.c.), ma anche di un contratto di appalto (art. 1655 c.c.); l'art. 356 c.p., infatti, punisce tutte le frodi in danno della pubblica amministrazione, quali che siano gli schemi contrattuali in forza dei quali i fornitori sono tenuti a particolari prestazioni.

Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, comma 2, n. 1 c.p.).

Tale 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 (o ad altro Ente Pubblico). 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, al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.).

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.
Tale fattispecie può realizzarsi nel caso in cui si pongano in essere raggiri o artifici, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.).

Tale ipotesi di reato si configura nel caso in cui, alterando le modalità di funzionamento di un sistema informatico o telematico, o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto, arrecando danno a terzi.

Tale fattispecie può realizzarsi qualora, ad esempio, una volta ottenuto l'accesso ad un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

I reati sopra descritti possono consumarsi in diverse aree operative.

In particolare, il reato di corruzione sussiste anche nel caso si consumi nei confronti di soggetti stranieri i quali, secondo la legge italiana, sono pubblici ufficiali o incaricati di pubblico servizio.
Ancora, merita ricordare che in taluni casi possono configurarsi sia corruzioni c.d. attive (l'amministratore o il dipendente corrompe un P.U. o un incaricato di pubblico servizio per far ottenere all'Ente qualcosa), sia corruzioni c.d. passive (l'esponente dell'Ente – nello svolgimento di un'attività di natura pubblicistica - riceve danaro per compiere un atto contrario ai doveri del proprio ufficio). Tale ultima forma d'illecito si verificherà sicuramente con minor frequenza della prima, giacché nella maggior parte dei casi si tratterà di corruzioni realizzate nell'esclusivo interesse della persona fisica senza, cioè, *interesse o vantaggio* della Ente. Tuttavia, non è possibile escludere che si verifichino corruzioni passive che generano responsabilità dell'Ente e ciò, verosimilmente, potrà avvenire con riferimento a quei soggetti di diritto privato la cui attività è, in tutto o in parte, da considerare come pubblica funzione o pubblico servizio.
Al fine di valutare i possibili ambiti aziendali esposti a maggior rischio è necessario premettere che:

- la qualifica di pubblico ufficiale va riconosciuta a tutti i soggetti, pubblici dipendenti o privati, che possono o debbono, nell'ambito di una potestà regolata dal diritto pubblico, formare e manifestare la volontà della pubblica amministrazione ovvero esercitare poteri autoritativi o certificativi (ciò che rileva, infatti, è l'attività in concreto svolta e non la natura, pubblica o privata, del soggetto);
- sono incaricati di un pubblico servizio coloro i quali, pur agendo nell'ambito di un'attività disciplinata nelle forme della pubblica funzione, mancano dei poteri tipici di questa, purché non svolgano semplici mansioni d'ordine, né prestino opera meramente materiale.

Con riferimento alla fattispecie di cui all'articolo 319 *ter* del codice penale – Corruzione in atti giudiziari – si precisa che costituisce "atto giudiziario" qualsiasi atto funzionale ad un procedimento giudiziario, indipendentemente dalla qualifica soggettiva di chi la realizza. L'ambito risulta pertanto di considerevole ampiezza.

Le ipotesi di responsabilità dell'Ente per concussione sono più circoscritte. Il comportamento concussivo per risultare rilevante ai fini del D.Lgs. 231/01 deve essere realizzato *nell'interesse o a vantaggio* dell'Ente e non, come solitamente accade, nell'esclusivo interesse del concussore.

Le **aree** ove il rischio si può presentare in misura maggiore possono individuarsi nei seguenti settori:

- amministratore e dirigente di 1^ fascia relativamente ai rapporti con i funzionari pubblici per gli adempimenti relativi, alle verifiche fiscali e previdenziali ed alla richiesta di contributi;
- consiglio di Amministrazione, relativamente alla gestione delle risorse finanziarie;
- attività che implicano rapporti con pubblici ufficiali, organi titolari di poteri autorizzativi, concessori, abilitativi, regolatori o ispettivi ed attività che implicano trattative con Amministrazioni e/o enti pubblici.

In relazione ai **principi di comportamento** che i destinatari devono seguire con riferimento alle sopra descritte ipotesi di reato, si possono fornire le seguenti indicazioni.
Tali linee guida si riferiscono a comportamenti relativi all'area del "fare" e del "non fare", specificando in chiave operativa quanto espresso dai principi del MOGC dell'Ente.

I responsabili delle funzioni che hanno contatti formali ed informali con la Pubblica Amministrazione devono:

- dare ai propri collaboratori indicazioni precise sulle modalità di comportamento da assumere con i diversi soggetti pubblici, infondendo la conoscenza della norma nonché la consapevolezza delle circostanze che possono essere a rischio reato;
- prevedere da e verso la P.A. idonei sistemi di tracciabilità dei flussi informativi relativi a potenziali incarichi che vengano delegati a soggetti esterni che operano in qualità di rappresentanti dell'Ente e che devono essere conferiti in maniera formale, prevedendo una apposita clausola di stretta osservanza dei principi etici adottati;
- prevedere che dipendenti e collaboratori esterni si impegnino a comunicare all'Organismo di Vigilanza, unicamente in forma non anonima, qualsiasi violazione o sospetto di violazione del Modello Organizzativo.

I soggetti che, per ragioni del loro ufficio, hanno rapporti con rappresentanti della P.A., devono:

- adempiere alle disposizioni di leggi e regolamenti vigenti;
- informare, formalizzando la comunicazione, il proprio superiore gerarchico diretto, indicando i motivi del rapporto con i Pubblici Ufficiali nonché le generalità degli stessi;
- operare nel rispetto dei poteri di rappresentanza, di firma, delle deleghe e delle procure a loro conferite.

Dovranno altresì osservarsi i seguenti obblighi :

- qualunque richiesta scritta o verbale proveniente dalle Autorità di Vigilanza dovrà essere soddisfatta nel rispetto dei termini richiesti e comunque nel più breve tempo possibile;
- i dati contenuti nella documentazione richiesta devono essere completi e veritieri e devono essere validati dal Responsabile della Direzione competente in materia;
- la eventuale carenza di informazioni deve essere adeguatamente motivata;
- tutte le segnalazioni periodiche alle Autorità previste da leggi e regolamenti devono essere effettuate nel rispetto delle scadenze stabilite;
- nel corso dell'attività ispettiva, deve essere prestata da parte delle Direzioni ispezionate la massima collaborazione utile all'espletamento degli accertamenti; in particolare devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo consenso del Responsabile.

Nel caso in cui gli operatori di LABA S.r.l. siano a conoscenza, in via diretta o indiretta, di comportamenti a rischio reato ex D.Lgs 231/01 in merito ai processi operativi di competenza, o altresì di notizie, anche derivanti da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto aziendale, sono tenuti a darne formale immediata comunicazione all'Organismo di Vigilanza.

Ad esempio, in caso di tentata concussione da parte di un pubblico funzionario nei confronti di un dipendente (o altri collaboratori) sarà necessario:

- non dare seguito alla richiesta;
- darne tempestivamente notizia al proprio Responsabile;
- provvedere, a cura del Responsabile, a darne segnalazione all'Organismo di Vigilanza.

Nei rapporti con i rappresentanti della P.A. **è vietato**:

- promettere o effettuare erogazioni in denaro aventi ad oggetto fini diversi da quelle istituzionali e di servizio;
- effettuare spese di rappresentanza senza giustificativi e aventi scopi diversi da obiettivi prettamente aziendali;
- promettere, con l'ausilio di terzi, in modalità impropria, l'esecuzione di opere/servizi (ad es. ristrutturazione di edifici privati residenziali, o altri interventi edili o stradali, ecc.);
- promettere o concedere direttamente o indirettamente omaggi/regalie dirette o indirette di ingente valore;
- procurare o promettere di procurare informazioni e/o documenti riservati;
- non adottare, in sede di incontri formali ed informali, anche tramite legali esterni e consulenti di parte, comportamenti tali da indurre i Giudici o i componenti del Collegio Arbitrale, nonché
  i rappresentanti della P.A. qualora siano parte del contenzioso, ad avvantaggiare indebitamente gli interessi dell'Ente;
- non adottare, nel corso delle fasi del procedimento anche tramite legali esterni e consulenti di parte, comportamenti tali da superare vincoli o criticità ai fini di tutelare l'Ente;
- non adottare, in sede di ispezioni/verifiche da parte di organismi pubblici o periti d'ufficio, comportamenti tali da influenzarne il giudizio nell'interesse dell'Ente;
- non adottare, in sede di decisione del contenzioso/arbitrato, comportamenti tali da influenzare indebitamente le decisioni dell'organo giudicante o le posizioni della P.A., qualora questa sia parte del contenzioso.

Nei confronti della P.A. è altresì vietato :

- esibire documenti/dati falsi o artefatti;
- assumere un comportamento menzognero al fine di indurre in errore la P.A. nella valutazione tecnico-economica riguardante i prodotti e servizi offerti/forniti;
- tralasciare volutamente informazioni dovute, al fine di rivolgere a proprio favore le decisioni della P.A.;
- destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali erano stati ottenuti;
- accedere, senza autorizzazione, ai sistemi informativi della P.A., al fine di procurarsi e/o modificare informazioni a vantaggio della Società;

- far ricorso a consulenti esterni, qualora l'attività richiesta possa essere svolta da dipendenti dell'Ente, ovvero in assenza di una comprovata e assoluta necessità di apporti professionali e tecnici, reperibili solo al di fuori dell'Ente;
- assumere o promettere di assumere soggetti, in violazione delle procedure interne, in modo idoneo ad influenzare l'indipendenza di giudizio delle Pubbliche Amministrazioni o ad indurle ad assicurare vantaggi per la Società;
- stringere intese o scambiare informazioni sulle offerte con le altre ditte inserite nell'elenco delle ditte di fiducia dell'Amministrazione Pubblica per concertare i prezzi o le altre condizioni dell'offerta;
- promettere o concedere vantaggi ad altri concorrenti affinché non concorrano all'appalto o ritirino l'offerta;
- tacere la richiesta o pretesa da parte dei dipendenti addetti o di chiunque possa influenzare le decisioni relative alla trattativa;
- promuovere, assecondare o tacere circa l'esistenza di un accordo illecito o di una pratica concertata a fini illeciti.

Tutti i Destinatari coinvolti nello svolgimento delle attività a rischio sopra individuate sono tenuti a conoscere e rispettare le regole ed i principi contenuti nel MOGC di LABA.

PROTOCOLLI

A. <u>Richiesta di autorizzazioni, concessioni e licenze ad Enti Pubblici</u>

Per quanto concerne i reati sopra elencati, si possono individuare come **attività "a rischio"** le attività concernenti il rapporto con il ministero dell'Istruzione dell'Università e della ricerca (MIUR)/ ANVUR per gestione accreditamento.

<u>Presidi</u>:

Compilazione di una scheda informativa/riepilogativa dei passi da percorrere.

- La scheda dovrà contenere:
- le Pubbliche amministrazioni competenti nel processo nonché le relative competenze ed iter decisionali (atti, delibere);
- i consulenti esterni locali coinvolti (i cui rapporti vengono formalizzati sulla base degli standard adottati);
- la documentazione interna da produrre a supporto delle richieste e la direzione tecnicamente competente;

- le autocertificazioni da produrre;
- la data di rilascio delle autorizzazioni / concessioni / licenze / permessi;
- il numero delle autorizzazioni / concessioni / licenze / permessi;
- il periodo di validità delle autorizzazioni / concessioni / licenze / permessi;
- il motivo dell'eventuale scadenza;
- l'identificazione dell'autorità che rilascia le autorizzazioni / concessioni / licenze / permessi;
- i sopralluoghi preliminari, concomitanti e finali, che si prevede siano effettuati dalle Autorità Competenti;
- effettuazione di verifica di congruenza fra quanto autorizzato, quanto realizzato e quanto dichiarato alla P.A. ai fini del pagamento dei corrispettivi previsti;
- esistenza di direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto dell'Ente, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dall'Ente.

Devono, inoltre, essere definite adeguate modalità di gestione delle eventuali deroghe ai principi sopra esposti.

Tracciabilità: è richiesta opportuna archiviazione delle schede sopra riportate.

B. Richiesta di contributi

Le attività potenzialmente sensibili sono:

- erogazione di borse di studio;
- rapporti con i Ministeri;
- rapporti con il Ministero dell'Istruzione, dell'Università e della ricerca (MIUR) /ANVUR per gestione accreditamento;
- partecipazione ad appalti per la realizzazione di progetti culturali;
- definizione di un elenco di documenti che devono essere trasmessi al MIUR/ANVUR per ottenere l'accreditamento;
- formale definizione dei ruoli che possono sottoscrivere, partecipare in nome e per conto dell'accademia allo svolgimento della gara, ottenere chiarimenti o specificazioni tramite idonea procura;
- approvazione delle richieste di finanziamento del vertice dell'accademia prima dell'invio della stessa alla P.A. coinvolta.

C. Mobilità Erasmus (borse di studio)

Aspetti operativi

- con cadenza annuale, l'Ufficio deputato effettua una richiesta di fondi alla Comunità Europea per finanziare il progetto Erasmus
- l'Agenzia Nazionale Indire comunica l'importo stanziato ed effettua il versamento dei fondi a favore di LABA (tutte le operazioni effettuate da tale agenzia vengono registrate sul portale Erasmus/servizi ai beneficiari).
- la mobilità Erasmus varia a seconda del beneficiario e della durata (i dati inerenti le singole attività vengono registrati nello strumento Mobility tool).
- l'ufficio Erasmus determina l'importo da versare attraverso il calcolatore comunitario.
- viene effettuato il versamento della quota
- ricalcolo dei fondi (Agenzia Nazionale)
- trascorsa metà mobilità (verso Aprile), l'Agenzia Nazionale effettua controlli dei fondi e procede come segue:

a) stanziamento altri fondi (qualora l'istituto ne avesse bisogno)

b) restituzione dell'importo non utilizzato (messo a disposizione di altri istituti).

D. Diritto allo studio

Aspetti operativi

Al momento del versamento della retta accademica, LABA riscuote € 140 di DSU per ogni studente.
LABA corrisponde a Regione Lombardia i contributi raccolti per la gestione degli interventi per DSU come segue:

- 85% entro febbraio dell'anno di riferimento
- 15% entro gennaio dell'anno successivo.

Nel mese di giugno, la Regione determina e comunica modalità e previsioni di finanziamento secondo questi criteri:

- Risorse regionali
- Tassa DSU studenti
- Fondo integrativo statale

Nel corso dell'anno, l'ufficio DSU deve compilare delle schede richieste dal Ministero e dalla Regione Lombardia.

I dati vengono forniti da diversi uffici :

- Ufficio Amministrativo (dati contabili sulla spesa dei contributi di gestione; dati contabili sulla contribuzione studentesca)
- Ufficio Erasmus (dati riguardanti la mobilità internazionale)
- Segreterie LABA (Dati riguardanti numero iscritti per calcolo tassa DSU)
- Ufficio DSU (dati riguardanti la mobilità internazionale)

Predisposizione bando da pubblicare sul sito (ufficio DSU):

- 30/09: data ultima di partecipazione e di invio documentazione
- 30/10: pubblicazione graduatoria provvisoria
- 30/11: pubblicazione graduatoria definitiva

Pagamento borse di studio (Ufficio amministrativo)

Gestione dei servizi per il diritto allo studio universitario – ufficio DSU LABA

LABA, tramite apposita convenzione con Regione Lombardia, gestisce per conto della Regione i servizi per il diritto allo studio universitario e l'emanazione dei bandi per l'assegnazione delle borse di studio.
La Regione corrisponde alla LABA dei contributi per la gestione degli interventi per il diritto allo studio nell'importo annuo definito sulla base dei seguenti criteri:

- per il 50% con riferimento al numero degli studenti immatricolati e iscritti ai corsi nell'anno accademico precedente;
- per il 50% in relazione al numero di borse di studio assegnate dall'Accademia nell'anno accademico precedente.

I contributi di gestione vengono versati alla LABA in due soluzioni nell'anno solare di riferimento.

LABA riscuote, in nome e per conto della Regione Lombardia, la tassa regionale per il diritto allo studio universitario (€ 140,00) in un'unica soluzione all'atto dell'immatricolazione e dell'iscrizione degli studenti ai corsi.
Tale tassa viene versata dall'ufficio amministrativo alla Regione Lombardia con le seguenti modalità:

- una quota pari all'85% del gettito complessivo della tassa entro e non oltre il mese di febbraio dell'anno accademico di riferimento;

- il restante 15% (al saldo del gettito complessivo della tassa bisogna sottrare l'importo totale del rimborso effettuato agli studenti che sono risultati idonei non beneficiari per insufficienza di fondi) entro il mese di gennaio dell'anno accademico successivo.

Nel mese di giugno la Regione Lombardia determina e comunica le modalità e le previsioni di finanziamenti per l'assegnazione dei benefici a concorso per il diritto allo studio universitario per l'anno accademico che deve ancora iniziare. Le previsioni indicative di finanziamento vengono calcolate con la seguente ripartizione:

- una percentuale in base risorse Regionali
- una percentuale dagli introiti della Tassa Regionale per il diritto allo studio;
- una percentuale in base al fondo integrativo statale.

Compilazione delle schede, inviate dal Ministero, per il riparto del fondo integrativo, dove vengono inseriti i dati per le borse di studio dell'anno accademico appena concluso.

E. Partecipazione a bandi di finanziamento - Richiesta di finanziamento

Gestione dei rapporti con gli enti Pubblici finanziatori, locali, nazionali ed europei, per l'ottenimento di finanziamenti, contributi o erogazioni pubbliche.

Le attività potenzialmente sensibili sono:

- Ricerca delle fonti di finanziamento
- Progettazione e attività di ricerca
- Contabilità e Rendicontazione
- Piani formativi aziendali

Protocolli:

Il Consiglio di Amministrazione effettuerà:

- un controllo di completezza, accuratezza e veridicità sulla richiesta di finanziamento, prima dell'invio alla P.A. coinvolta.

- una verifica che il progetto finanziato sia in linea con l'accordo definito con l'ente finanziatore.

F. Gestione di rapporti con soggetti pubblici in occasione di: verifiche, ispezioni, accertamenti, richieste di informazioni, ovvero in caso di richieste di licenze/autorizzazioni

Aspetti operativi:

- sono autorizzati ad intrattenere i predetti rapporti con Soggetti Pubblici i soggetti individuati dall'Ente ai quali sia stata formalmente rilasciata delega o procura in tal senso (ovvero i soggetti in loro vece designati e sotto il controllo dei medesimi);
- deve essere fornita la massima collaborazione nel rapporto con la P.A., fornendo le informazioni e i documenti dalla stessa richiesti in sede di verifica o ispezione, ovvero al fine del rilascio di autorizzazioni, licenze, brevetti o atti amministrativi di altra natura;
- in caso di verifiche o ispezioni, in assenza dei soggetti autorizzati ad intrattenere i predetti rapporti, ne deve essere informato l'Amministratore, il quale provvederà ad individuare i soggetti deputati a gestire la procedura ispettiva;
- tutti i moduli/documenti (e relativi allegati) da presentare alla Pubblica Amministrazione devono essere verificati, sotto il profilo formale e sostanziale, a cura del responsabile dell'attività (o del soggetto in sua vece designato) e dallo stesso siglati, prima di essere sottoposti alla firma del soggetto competente;
- deve essere redatta una reportistica sullo svolgimento delle verifiche/ispezioni;
- ove emergano criticità di qualsiasi natura nelle predette attività, ne deve essere immediatamente informato l'Amministratore Delegato e l'OdV.

Tracciabilità : è richiesta la raccolta per iscritto (mediante consegna di documenti siglati, o invio a mezzo email) di tutti i dati e informazioni necessari per l'espletamento delle predette attività ed altresì la conservazione di copia di tutta la documentazione relativa al rapporto consegnata/ricevuta, con indicazione dei soggetti coinvolti.

G. Procedimenti giudiziali

Nel corso di eventuali procedimenti giudiziali che vedono coinvolta LABA, il Consiglio di Amministrazione, dovrà:

- effettuare la nomina formale del soggetto deputato alla ricezione della notifica;
- inviare al Responsabile della funzione interessata la copia di tutti gli atti notificati a LABA;
- individuare i criteri di scelta in merito alla gestione interna o esterna della pratica;
- tracciare il processo di scelta del professionista individuato;
- inserire la clausola di rispetto dei principi etico-comportamentali nelle lettere di incarico.

Tracciabilità: Conservazione per ciascun contenzioso del supporto documentale per la durata di 10 anni.

H. Selezione, assunzione e progressioni di carriera del personale

Principi di controllo

Il sistema di controllo si basa sugli elementi qualificanti la **separazione di ruolo** tra le funzioni utilizzatrici della risorsa ed i soggetti delegati all'assunzione delle risorse, nonché dell'esistenza di **momenti valutativi tracciabili**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:
nella fase "**Acquisizione e gestione dei curricula-vitae**", tracciabilità delle fonti di reperimento dei CV (ad es., inserzioni, domande spontanee, presentazioni interne, ecc.);
nella fase "**Selezione**", rispetto del criterio della separazione organizzativa per le attività di valutazione delle candidature. In tale ambito:

- prevedere distinte modalità di valutazione tecnica e attitudinale del candidato;
- assegnare la responsabilità di tali valutazioni a soggetti distinti (es. la valutazione a cura della funzione "utilizzatrice della risorsa" deve essere sempre accompagnata da quella dei soggetti delegati all'assunzione delle risorse);
- richiedere la sottoscrizione formale delle suddette valutazioni da parte dei soggetti responsabili, a garanzia della tracciabilità delle scelte effettuate.

nella fase "**Formulazione dell'offerta e assunzione**":

- procedere alla scelta in base a valutazione di idoneità.
- in sede di sottoscrizione della lettera di assunzione, verificare l'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti.

nella fase "**Progressione di carriera**", individuare:

- criteri coerenti con quanto previsto dal nuovo CCNL.
- formalizzazione della valutazione della dirigenza;
- quantificazione di un *budget* legato agli incassi aziendali annuali;
- chiara definizione della procedura applicabile.

Sistema Autorizzativo

Tutte le attività relative alla selezione, assunzione e gestione del personale sono gestite dal responsabile delle risorse umane, sentito il Consiglio di Amministrazione.

Sistema Organizzativo

I soggetti competenti alla gestione delle attività di cui sopra trovano riscontro all'interno dell'Organigramma aziendale.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Si individuano di seguito ripartiti per singolo processo operativo i flussi da/verso l'OdV In particolare:

- **Richiesta di autorizzazioni, concessioni e licenze ad Enti Pubblici**:

con periodicità **semestrale** devono essere fornite all'Organismo di Vigilanza dal Consiglio di Amministrazione le seguenti informazioni:

- copia delle schede informative/riepilogative redatti dai responsabili delle Direzioni competenti;
- elenco concessioni/autorizzazioni/licenze ottenute;
- segnalazione fatti anomali per rilievo e/o frequenza;
- situazioni di riscontrata deviazione dalle procedure previste e relative motivazioni.

- **Stipula/negoziazione/esecuzione di contratti/convenzioni con Enti Pubblici** :

con periodicità **annuale** devono essere forniti dal Consiglio di Amministrazione all'Organismo di Vigilanza i seguenti documenti:

- elenco dei contratti/convenzioni stipulati con Enti Pubblici;
- elenco delle variazioni/modifiche tecniche e normative ai contratti/convenzioni stipulati;
- segnalazione con nota scritta di fatti anomali per rilievo e/o frequenza ovvero di qualunque criticità o conflitto di interesse ipotizzabile nell'ambito del rapporto con la P.A.;
- situazioni di riscontrata deviazione dalle procedure previste e relative motivazioni.

- **Gestione verifiche ed ispezioni da parte di Enti pubblici o Autorità di Vigilanza** :

con periodicità **semestrale** devono essere fornite all'Organismo di Vigilanza da parte dei soggetti delegati le seguenti informazioni:

- l'elenco delle ispezioni e verifiche e delle contestazioni da parte della P.A, con indicazione del loro esito, delle eventuali sanzioni e del relativo iter (definizione in adesione, ricorso, pagamento);
- una scheda per ciascuna ispezione con indicazione della natura della visita, delle informazioni assunte e della documentazione eventualmente richiesta;
- segnalazioni di possibili ostacoli/impedimenti relativi alle richieste di notizie e consultazioni ovvero allo svolgimento delle attività di controllo e di Vigilanza;

- **Gestione degli adempimenti presso Enti pubblici o Autorità di Vigilanza (in materia retributiva, previdenziale ed assistenziale e in materia di igiene e sicurezza sui luoghi di lavoro):**

con periodicità **semestrale** devono essere fornite all'Organismo di Vigilanza da parte del Consiglio di Amministrazione le seguenti informazioni:

- lista degli adempimenti con le relative scadenze;
- segnalazioni di possibili ostacoli/impedimenti relativi alle richieste di notizie e consultazioni ovvero allo svolgimento di adempimenti presso Enti Pubblici e Autorità pubbliche di Vigilanza;
- elenco delle operazioni effettuate in deroga alle procedure e/o promanate direttamente dai soggetti apicali

- **Procedimenti giudiziali :**

con periodicità **semestrale** devono essere fornite da parte del Presidente / Amministratore all'Organismo di Vigilanza le seguenti informazioni:

- report del contenzioso pendente e concluso con l'indicazione dell'oggetto, delle parti, dell'Autorità Giudiziaria competente, del grado di giudizio e del professionista eventualmente incaricato;
- elenco delle passività inserite nel fondo rischi aziendali;
- elenco dei professionisti cui sono stati affidati incarichi con la specifica di quelli cui sono stati erogati compensi superiori alle tariffe professionali, e l'indicazione delle motivazioni che giustificano la deroga.

Con **immediatezza** devono essere altresì fornite da parte del Consiglio di Amministrazione all'Organismo di Vigilanza:

- informazioni riguardanti situazioni di riscontrata deviazione dalle procedure previste e relative motivazioni;
- comunicazioni da parte di qualsiasi autorità relative a svolgimento di indagini per reati previsti dal D. Lgs. 231/01 nei confronti degli organi aziendali o dirigenti o dipendenti;
- elenco delle consulenze agli organi aziendali in merito a procedimenti penali previsti dal decreto;
- situazioni di riscontrata inadeguatezza e/o non effettività e/o non conformità al Modello e alle relative procedure.

PARTE SPECIALE

"B"

Reati Societari

L'ipotesi di commissione dei reati societari è stata inserita come ipotesi punibile ai sensi del Decreto dal D.lgs. 61/2002, che prevede sanzioni a carico degli enti "*in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti la loro carica*" .

Da quanto sopra, e da quanto verrà illustrato *infra*, emerge che i reati societari sono, nella maggioranza dei casi, "reati propri", ossia diventano punibili in quanto la condotta è posta in essere proprio da quei soggetti (amministratori, procuratori, direttori generali, sindaci, liquidatori, ecc.) che dovrebbero creare un sistema di controllo preventivo o, in ogni caso, collaborare con l'Organismo di Vigilanza.

I citati reati possono essere raggruppati, per quanto di specifico interesse in diverse tipologie:

A) Reati che attengono alla falsità in comunicazioni sociali;

B) Reati che incidono sul regolare funzionamento della società;

C) Reati che incidono sulla formazione del capitale sociale;

D) Reati che attengono alle funzioni di vigilanza;

E) Reati che attengono alla tutela del mercato;

F) Corruzione tra privati.

La legge 262 del 28 dicembre 2005 ha inciso sui reati societari in maniera piuttosto significativa, come verrà evidenziato nella presente parte speciale, introducendo, tra l'altro, una nuova figura di reato (di omessa comunicazione del conflitto di interessi di cui all'art. 2629-*bis* cod. civ.), modificando i contenuti di determinati reati e prevedendo, all'articolo 39, il raddoppio delle sanzioni pecuniarie previste dall'art. 25-*ter* del Decreto.

Più recentemente, il D.lgs. 39 del 27 gennaio 2010 ha abrogato l'articolo 2624 del cod. civ., richiamato dall'articolo 25 *ter* del Decreto, spostando nel proprio articolo 27 il reato di "*Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale*". Inoltre, il D.lgs. 39/10 ha eliminato dall'articolo 2625 del cod. civ., pure richiamato dall'art. 25 *ter* del Decreto, l'impedito controllo dei revisori, regolato ora dall'art: 29 del D.lgs. 39/10.

Quindi, la legge 6 novembre 2012, n. 190, ha sostituito l'articolo 2635 del cod. civ., introducendo la corruzione tra privati.

Infine, la legge 69 del 27 maggio 2015 ha modificato gli articolo 2621 e 2622 del codice civile ed introdotto, sempre nel codice civile, gli articoli 2621-*bis* e 2621-*ter*.

Nella presente parte speciale non verranno presi in considerazione i delitti di falso in prospetto (di cui all'art. 25-*ter*, lett. d ed e) ed omessa comunicazione del conflitto di interessi previsto dall'art. 2629-*bis* del codice civile (di

cui all'art. 25-*ter*, lett. r), trattandosi di fattispecie che interessano le società con titoli quotati in mercati regolamentati ovvero sottoposte a vigilanza come previsto nell'art. 2629-*bis* cod. civ.

A. REATI CHE ATTENGONO ALLA FALSITA' IN COMUNICAZIONI SOCIALI

Fuori dai casi previsti dall'art. 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 social, dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilavanti 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 essa appartiene, in modo concretamente idoneo a indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.
La stessa pena si applica anche se la falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto terzi.
**articolo così modificato dall'articolo 9 della legge 69 del 27 maggio 2015.*

Art. 2621 *bis* del codice civile – Fatti di lieve entità*

Salvo che costituisca più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e della dimensione 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'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942 n. 267. In tal caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

** Articolo introdotto dall'articolo 10 della legge 69 del 27 maggio 2015.*

Art. 2622 del codice civile - 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 registrazione in un mercato regolamentato, italiano o di altro Paese dell'Unione Europea i quali, al fine di conseguire per sé o per gli 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 essa appartiene, in modo concretamente idoneo ad indurre altri in errore sono puniti con la pena della reclusione da tre ad 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.

** articolo così modificato dall'articolo 11 della legge 69 del 27 maggio 2015.*

****

Considerazioni specifiche

L'articolo 2621 cod. civ. è volto alla tutela della trasparenza delle informazioni rivolte ai soci o al pubblico attraverso i bilanci, le relazioni e le altre comunicazioni sociali. Esso dà rilevanza penale anche alle condotte di false comunicazioni che non producono un danno patrimoniale ai soci o al pubblico, laddove, invece, questo è il profilo tutelato dal successivo art. 2622 cod. civ.
A seguito delle modifiche introdotte con la legge 69 del 27 maggio 2015, entrambi gli articoli descrivono un reato di condotta, differenziato attraverso la tipologia dell'ente.
Le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società. Accanto al bilancio, costituiscono l'oggetto materiale del reato soltanto quelle comunicazioni sociali previste dalla legge e diretta ai soci o al pubblico. Restano fuori da questo ambito le comunicazioni interorganiche (tra i diversi organi della società) e quelle con unico destinatario pubblico o privato. La fattispecie delle false comunicazioni sociali è un'ipotesi contravvenzionale caratterizzata dall'assenza di danno patrimoniale ai soci o ai creditori, a cui è riservato un trattamento sanzionatorio più lieve rispetto a quello del successivo articolo 322 cod. pen. È richiesta la

consapevole volontà di ingannare, ossia di determinare un errore nei soci o nel pubblico in ordine alla effettiva situazione patrimoniale della società e di procurare attraverso l'inganno un ingiusto profitto all'agente o ad altri. La fattispecie di cui all'articolo 322 cod. pen. è invece costruita come reato di danno in quanto si consuma quando la comunicazione falsa cagioni un danno patrimoniale per i soci o per i creditori. Ne deriva che occorrerà accertare la sussistenza di un nesso causale tra la comunicazione falsa volta a trarre in inganno ed il danno patito dai soci o dal pubblico.

Peraltro, la legge 262 del 2005 ha inciso significativamente su entrambi gli articoli, innanzitutto inserendo tra i soggetti attivi dei reati anche i dirigenti preposti alla redazione dei documenti contabili societari, figura introdotta dall'art. 14 della legge stessa.

In entrambi gli articoli, poi, il legislatore ha introdotto (comma 5 dell'art. 2621 cod. civ. e comma 9 dell'art. 2622 cod. civ. sanzioni pecuniarie ed interdittive per i soggetti responsabili anche per le condotte di falsificazione rimaste al di sotto delle soglie di punibilità (di cui ai commi 3 e 4 dell'art. 2621 cod. civ. e commi 7 e 8 dell'art. 2622 cod. civ.). Peraltro, si tratta di misure che il Decreto prevede per gli enti e che la legge 262/2005 applica alle persone fisiche.

Inoltre, nell'art. 2622 cod. civ. è stata *(i)* introdotta la società tra i soggetti danneggiati legittimati a proporre la querela (ipotesi che, essendo in *re ipsa* escluso l'interesse o il vantaggio per la società, esula dai fini di cui al presente Modello) e *(ii)* previsto, dai commi 4 e 5, il concetto del "grave nocumento ai risparmiatori", ossia del nocumento che abbia riguardato un certo numero di risparmiatori o sia consistito nella distruzione o riduzione del valore di titoli di una certa entità, concetto che riguarda, quindi, le società quotate in mercati regolamentati.

In generale, con riferimento ad entrambi gli articoli, si evidenzia come il bilancio e la nota integrativa che lo correda solo in apparenza scaturiscono automaticamente dalla contabilità generale ed, infatti, molte delle voci che compongono tali documenti necessitano di stime, le quali comportano, inevitabilmente, margini di soggettività non eliminabili anche con l'utilizzo di tecniche specialistiche e sono influenzate anche dalla correttezza e veridicità delle informazioni rilevanti ai fini della loro composizione e valutazione.

La redazione del bilancio, coinvolge, quindi, molte funzioni aziendali e non solo il settore amministrativo. Infatti, ancorché questa funzione sia la detentrice dei saldi contabili di fine anno e delle norme tecniche per la formazione del bilancio, tali saldi costituiscono soltanto il punto di partenza del processo di formazione del bilancio stesso, nel quale intervengono *managers* e titolari di altre funzioni.

Quanto al livello al quale possono commettersi i reati in esame, è evidente che questi reati saranno commessi il più delle volte da chi formalmente è responsabile di questi documenti e cioè gli amministratori, i procuratori ed i dirigenti preposti alla redazione degli stessi. È anche possibile che reati di questo genere siano commessi dai responsabili di funzione, dotati di un certo potere discrezionale, ancorché circoscritto. In questi casi il reato potrà dirsi consumato solo se la falsità sia consapevolmente condivisa dai soggetti "qualificati" (amministratori, procuratori, dirigenti, ecc.) che nel recepire il dato falso lo fanno proprio inserendolo nella comunicazione sociale. Se non vi è tale partecipazione cosciente e volontaria da parte dei soggetti "qualificati", non solo tali soggetti non

potranno essere ritenuti responsabili, ma, altresì, il reato non sarà configurabile. Infatti, trattandosi di reati "propri", è indispensabile quantomeno la partecipazione di un soggetto provvisto della qualifica soggettiva voluta dalla legge. Peraltro, l'esperienza insegna che le falsità commesse dai "subalterni" vengono realizzate nel loro interesse esclusivo (per esempio per coprire un ammanco di cassa) e ben difficilmente nell'interesse dell'ente. Ciò esclude, come è noto, ogni responsabilità ai sensi del Decreto. Nel caso, invece, più frequente, di falsità realizzata dal subordinato su indicazione, ad esempio, degli amministratori e/o dei procuratori (si pensi al caso di valutazioni mendaci di crediti o partecipazioni, realizzate nell'interesse della società), la responsabilità dell'ente non potrà escludersi.

In riferimento a LABA, per quanto concerne i reati sopra elencati, si possono individuare come **attività "a rischio"** le attività di :

- Coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di: rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari, economici.
- Corretta tenuta dei rapporti amministrativi con i terzi (clienti).
- Gestione amministrativa e contabile dei cespiti.
- Accertamento delle poste valutative quali crediti e fondi rischi.
- Accertamenti di tutti gli altri fatti amministrativi in corso d'anno (es. costi del personale, finanziamenti attivi e passivi, interessi).
- Verifica dati provenienti dal sistema gestionale aziendale.
- Corretto calcolo delle imposte da versare.

Le aree aziendali ove il rischio si può presentare in misura maggiore possono individuarsi, pertanto, nei seguenti settori:

- Organi apicali di governo societario (Consiglio di Amministrazione e procuratori);
- Direzione Amministrativa
- Ufficio societario
- Organi di controllo (Collegio Sindacale e revisori contabili);

I reati sopra menzionati potrebbero essere commessi, ad esempio, qualora un soggetto "apicale" richieda di effettuare iscrizioni in bilancio non corrette o non veritiere o effettui comunicazioni sociali non corrispondenti al vero o ometta informazioni rilevanti.

Fermo restando quanto si dirà *infra*, in via generale, in relazione ai principi di comportamento che i destinatari devono seguire per contrastare tale fenomeno a livello aziendale sarà utile adempiere a quanto segue:

- promuovere l'osservanza, accuratezza, chiarezza e completezza delle informazioni fornite e la segnalazione di eventuali conflitti di interesse;
- assicurare la formazione di tutti i responsabili di funzione e del personale che gestisce la redazione del bilancio e delle altre comunicazioni sociali;
- prevedere procedure che indichino le scadenze per l'espletamento delle varie fasi necessarie alla redazione delle scritture sociali e per la comunicazione ai vertici aziendali delle informazioni e dei dati rilevanti;
- prevedere l'obbligo, per il responsabile di funzione che fornisce dati e informazioni relativi al bilancio o ad altre comunicazioni sociali, di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse;
- mettere la bozza di bilancio tempestivamente a disposizione degli amministratori e, per l'esame di competenza, anche dell'Organismo di Vigilanza, certificando documentalmente l'avvenuta consegna di detta bozza;
- prevedere una o più riunioni, delle quali si dovrà redigere verbale - tra il Collegio Sindacale e l'Organismo di Vigilanza - prima della riunione che il Consiglio di Amministrazione ha convocato per l'approvazione del bilancio – avente ad oggetto l'esame del documento stesso.

Bisognerà inoltre, in pendenza della stesura delle bozze delle scritture sociali, prevedere e regolamentare l'eventuale incontro dell'Organismo di Vigilanza con il Collegio Sindacale per l'esame delle scritture stesse, dei quali incontri si dovrà redigere verbale.

B. REATI CHE INCIDONO SUL REGOLARE FUNZIONAMENTO DELLA SOCIETA'

B.1. Impedito controllo

Art. 2625 del codice civile

*Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 Euro.**

Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata 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'art. 116 del testo unico di cui al d.lgs. 24 febbraio 1998 n. 58.

1. * Articolo così modificato dal D.lgs. 39 del 27 gennaio 2010. L'impedito controllo dei revisori è ora oggetto dell'articolo 29 del D.lgs. 39/10, il quale non è però richiamato dall'art. 25 *ter* del Decreto.

****

Considerazioni specifiche

Solo la fattispecie prevista dal secondo comma può comportare una responsabilità ai sensi del Decreto. Infatti, nel caso previsto dal primo comma la condotta, seppur sostanzialmente identica, non integra reato, essendo prevista soltanto una sanzione amministrativa. Si ribadisce, ancora una volta, che il fatto deve essere realizzato *nell'interesse o a vantaggio* della Società.

Il soggetto attivo è sempre l'amministratore. L'elemento soggettivo è costituito dal dolo generico e si sostanzia in qualsiasi comportamento commissivo o omissivo, con il quale gli amministratori e/o i procuratori impediscono il controllo da parte del Collegio Sindacale o dei soci.

Nel caso di LABA per quanto concerne tale reato "proprio", sono "a rischio" le attività e le condotte che gli amministratori ed i procuratori (ed i loro collaboratori) tengono in relazione allo svolgimento delle attività di controllo previste dalla legge e svolte dal Collegio Sindacale e le condotte tenute in relazione ai controlli previsti dal Modello e che siano idonee ad ostacolare i controlli sull'esercizio attività sociale o sulla rappresentazione contabile della stessa.

In tale ambito, si configurano come **attività "a rischio"** :

- Gestione delle scritture contabili e dei libri sociali
- Rapporti con gli organi di controllo (Collegio Sindacale), relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e alle attività di verifica della gestione aziendale

Le possibili modalità di commissione del reato sopra menzionato da parte dell'amministratore, del Presidente del Consiglio di Amministrazione, dell'amministratore delegato, ove nominato, o di uno o più procuratori o dei loro collaboratori sono chiaramente individuate dalla norma.

In relazione al reato di impedito controllo, che può essere commesso dagli amministratori e/o dai procuratori (reato proprio), si rimanda a quanto si dirà *infra*, in via generale, in relazione ai principi di comportamento che i destinatari devono seguire a livello aziendale.

In ogni caso è necessario:

- prevedere un'adeguata formazione/informazione di tutto il *management* della Società sulle regole di governo societario e su quelle contenute nel presente Modello e rendere il *management* stesso consapevole del sistema sanzionatorio vigente sia a livello normativo che aziendale;
- predisporre quindi un sistema definito di responsabilità e rendere coerente con le responsabilità previste l'eventuale sistema di deleghe;
- istituzionalizzare l'incontro periodico dell'Organismo di Vigilanza con il Collegio Sindacale per verificare l'osservanza della disciplina prevista in tema di governo societario ed il rispetto della stessa da parte del *management* e dei dipendenti;
- istituzionalizzare un'informativa periodica ai vertici aziendali attinente allo stato dei rapporti con il Collegio Sindacale e con le altre autorità che devono eventualmente svolgere controlli sulla Società.

B.2. Illecita influenza sull'assemblea

Art. 2636 del codice civile

Chiunque, con atti simulati o fraudolenti determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto è punito con la reclusione da sei mesi a tre anni.

****

Considerazioni specifiche

Il reato di illecita influenza sull'assemblea, che può essere commesso da chiunque, è difficilmente ipotizzabile in relazione al Decreto, in quanto di solito tende a procurare profitto per il soggetto agente e non è commesso *a vantaggio* e *nell'interesse* della Società. In ogni caso, anche per tale fattispecie di reato è utile adottare tutte le misure illustrate al punto precedente.

C. REATI CHE INCIDONO SULLA FORMAZIONE DEL CAPITALE SOCIALE

Art. 2626 del codice civile - Indebita restituzione dei conferimenti

Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamene, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno.

Art. 2627 del codice civile - Illegale ripartizione degli utili e delle riserve

Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno.

La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Art. 2628 del codice civile - Illecite operazioni sulle azioni o quote sociali o della società controllante

Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno.

La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale e' stata posta in essere la condotta, il reato è estinto.

Art. 2629 del codice civile - Operazioni in pregiudizio dei creditori

Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Art. 2632 del codice civile - Formazione fittizia del capitale sociale

Gli amministratori ed i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale della società mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni

in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono punti con la reclusione fino ad un anno.

Art. 2633 del codice civile - Indebita ripartizione dei beni sociali da parte dei liquidatori

I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

****

Considerazioni specifiche

Il bene giuridico oggetto di tutela, nelle fattispecie sopra menzionate, è costituito dalla integrità del capitale sociale e delle riserve non distribuibili per legge. Si tratta di reati "propri" che possono essere commessi solo dai soggetti espressamente indicati, fermo restando che gli stessi possono incaricare un terzo di porre in essere la condotta di cui alla norma.
In relazione alle procedure atte ad impedire la commissione delle presenti figure di reato è utile adottare tutte le misure già illustrate in relazione all'impedito controllo, ferma restando la necessità di procedure autorizzative per acquisti di azioni proprie, nonché procedure chiare ed esaustive che disciplinino le operazioni di distribuzione degli utili, aumento e riduzione del capitale, fusione e scissione societaria e, in sede di liquidazione, le operazioni di ripartizione dei beni sociali.

****

D. REATI CHE ATTENGONO ALLE FUNZIONI DI VIGILANZA

Art. 2638 del codice civile – Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori di società od enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in

base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti in tutto o in parte fatti che avrebbero dovuto comunicare concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori di società, o enti e i soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti a obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

La pena è raddoppiata 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'art. 116 del testo unico di cui al d.lgs. 24 febbraio 1998, n.58.

****

Considerazioni specifiche

L'articolo prevede fattispecie delittuose diverse per modalità di condotta e momento offensivo: la prima centrata sul falso commesso al fine di ostacolare le finzioni di vigilanza; la seconda sulla realizzazione intenzionale dell'evento di ostacolo attraverso qualsiasi condotta (attiva o omissiva).

Nel caso di LABA, per quanto concerne tale reato, sono "a rischio" le attività e le condotte che gli amministratori, i procuratori, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori (ed i loro collaboratori) tengono in relazione allo svolgimento delle attività di controllo previste dalla legge e svolte da Autorità Pubbliche di Vigilanza e che siano idonee – ad esempio, anche mediante la presentazione di documenti o il rilascio di affermazioni false, incomplete, generiche, confuse e/o imprecise – ad ostacolare i controlli sull'esercizio dell'attività sociale o sulla rappresentazione contabile della stessa.

In tale ambito, si configurano come operazioni "a rischio" le operazioni di registrazione e rappresentazione dell'attività d'impresa e le operazioni relative alla documentazione, archiviazione e conservazione delle informazioni sull'attività sociale, nonché le operazioni di comunicazione e gestione delle informazioni di impresa.

In relazione al reato di ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza, che può essere commesso da amministratori, procuratori, direttori generali, sindaci, dirigenti preposti alla redazione dei documenti contabili societari e liquidatori di società, è utile adottare tutte le misure illustrate in relazione

all'impedito controllo, fermo restando l'obbligo di relazionare periodicamente al vertice aziendale circa i rapporti con le Autorità Pubbliche di Vigilanza.

E. REATI CHE ATTENGONO ALLA TUTELA DEL MERCATO

Art. 2637 del codice civile – Aggiotaggio

Chiunque diffonde notizie false ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico
ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni.

****

Considerazioni specifiche

Per quanto riguarda tale fattispecie di reato, va sottolineato che per "notizia" si intende un'indicazione sufficientemente precisa di circostanze di fatto. Non viene ravvisato l'estremo della divulgazione quando le notizie non siano state diffuse o rese pubbliche, ma siano dirette solo a poche persone.
La notizia è da considerarsi falsa quando, creando una falsa rappresentazione della realtà, sia tale da trarre in inganno gli operatori determinando un rialzo o ribasso dei prezzi non regolare. Per altri artifici si deve intendere qualsiasi comportamento che, mediante inganno, sia idoneo ad alterare il corso normale di prezzi.
Per l'esistenza del reato è sufficiente una situazione di pericolo concreto, in quanto è necessario che le notizie mendaci o le operazioni simulate o gli altri artifici siano concretamente idonei a provocare un'effettiva lesione.
Si tratta di un reato comune, che può essere commesso da chiunque nel caso di questi il rischio è molto basso.
Per quanto concerne tale reato, sono "a rischio" le attività e le condotte degli amministratori, procuratori, sindaci, dirigenti o dipendenti che diffondano notizie false relative ai dati economico-finanziari della società o dati relativi a situazioni inerenti alla gestione della società o pongano in essere operazioni simulate.
In relazione a tale reato sarà opportuno predisporre un programma di formazione ed informazione specifica dei dipendenti ed i dirigenti per le attività a cui sono preposti nonché prevedere un controllo relativo alla pubblicazione o divulgazione a terzi di tutti i dati riguardanti la situazione economica e finanziaria e la gestione della società ed evitare che possano essere poste in essere operazioni simulate.

F. CORRUZIONE TRA PRIVATI

Art. 2635 del codice civile – Corruzione tra privati

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori che, a seguito della dazione o della promessa di denaro od altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi interenti al loro ufficio o agli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.

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

Chi dà o promette denaro od altra utilità 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 dall'atto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

****

Considerazioni specifiche

La legge 190 del 2012, che ha integrato il catalogo dei reati di cui al Decreto introducendo la corruzione tra privati nei casi previsti dal terzo comma dell'art. 2635 cod. civ., ha modificato detto articolo, intanto nella rubrica (introducendo esplicitamente il richiamo alla corruzione tra privati), ed ha subordinato l'applicabilità della fattispecie al fatto che la condotta non costituisca più grave reato.

Rispetto alla previgente formulazione si assiste:

i) ad un allargamento della platea dei soggetti attivi, includendo anche i soggetti sottoposti alla direzione o vigilanza altrui;

ii) all'introduzione dell'autonoma rilevanza del comportamento del soggetto che effettua o promette la dazione del denaro o di altra utilità (che è la fattispecie inserita nel Decreto).

Ulteriore elemento di novità è la rilevanza data alla violazione degli obblighi di fedeltà oltre agli *"obblighi inerenti al proprio ufficio"*. Questa circostanza sembra confermare che la *ratio* incriminatrice della norma sia da ravvisarsi nell'esigenza di reprimere le forme di *mala gestio* connesse ad un fenomeno di deviazione dal buon andamento societario.

È inoltre disposto un inasprimento della pena, che prevede ora la reclusione da uno a tre anni, assegnando alla fattispecie di "corruzione tra privati" un carattere di maggior disvalore rispetto al reato affine di "infedeltà patrimoniale" (art. 2634 cod. civ.).
Ai fini della responsabilità ex D.lgs. 231/01, rileva il comportamento dei corruttori, ossia di coloro i quali promettono denaro o utilità agli amministratori, ai procuratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci, ai liquidatori e alle persone sottoposte alla direzione o vigilanza di uno dei soggetti appena indicati.
In relazione a tale reato sarà opportuno attuare uno stretto controllo dei flussi finanziari, verificare il rispetto dei limiti di spesa di ciascun soggetto autorizzato, controllare la documentazione aziendale, selezionare adeguatamente i consulenti esterni e predisporre un programma di formazione ed informazione specifica dei dipendenti, dei collaboratori esterni e dei dirigenti per le attività a ciascuno affidate ed a cui sono preposti.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come attività "a rischio":

- la redazione del bilancio, della relazione sulla gestione e delle altre comunicazioni sociali e, più in generale, le attività di rilevazione, registrazione e rappresentazione dell'attività d'impresa nei suddetti atti e le attività relative alla gestione delle informazioni di impresa;
- le operazioni societarie che possono incidere sull'integrità del capitale sociale e creare pregiudizio ai creditori;
- le attività di controllo previste dalla legge e dal presente Modello;
- le attività di controllo da parte di Autorità Pubbliche di Vigilanza;
- le attività di gestione delle risorse finanziarie e dei rapporti con terzi in genere.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i responsabili di funzione, i sindaci ("Soggetti Apicali"), nonché i dipendenti soggetti a vigilanza e controllo da parte dei suddetti soggetti apicali (i "Destinatari"), devono osservare nell'ambito delle attività "a rischio" sopra individuate, al fine di impedire il verificarsi dei reati previsti nel Decreto e, specificamente, i reati societari.
Ai soggetti apicali sono equiparati, ai sensi dall'art. 2639 cod. civ., ai fini *de quo*, coloro che svolgono tali funzioni di fatto, esercitando i poteri tipici di queste funzioni in maniera continuativa e significativa.
I Destinatari devono astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.

Per ciascuna delle attività a rischio sopra individuate, i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- non vi sia identità soggettiva tra chi assume o attua le decisioni, chi è tenuto a dare evidenza contabile delle stesse e chi è tenuto ad effettuare sulle stesse i controlli previsti dalla legge;
- i documenti riguardanti l'attività d'impresa siano conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi possa essere consentito solamente al soggetto competente secondo le norme aziendali interne, o ad un suo delegato, nonché al Collegio Sindacale ed all'Organismo di Vigilanza;
- non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non giustificati in relazione al tipo di incarico effettuato ed alla prassi ed alle tariffe vigenti in ambito locale.

Oltre alle specifiche azioni da intraprendere, i Destinatari:

A. Nell'ambito delle attività relative alla redazione del bilancio, della relazione sulla gestione e delle altre comunicazioni sociali:

- devono tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, al fine di fornire ai soci ed ai terzi un'informazione completa, veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e di segnalare tempestivamente situazioni anomale, comunicando altresì all'Organismo di Vigilanza le eventuali richieste, da chiunque avanzate, di ingiustificata variazione dei dati già contabilizzati o dei criteri di rilevazione, registrazione dei dati o di rappresentazione contabile già utilizzati;
- non devono rappresentare o trasmettere - per l'elaborazione e la rappresentazione in bilanci, relazioni ed in altre comunicazioni sociali - dati falsi, lacunosi, o comunque non rispondenti alla realtà, sulla situazione economica, finanziaria e patrimoniale della Società o omettere la comunicazione di dati ed informazioni imposti dalla legge sulla situazione economica, finanziaria e patrimoniale della Società.

B. Nell'ambito delle operazioni societarie che possono incidere sull'integrità del capitale sociale e creare pregiudizio ai creditori:

- devono osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire sempre nel rispetto delle procedure aziendali interne che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

- devono disciplinare le responsabilità operative e decisionali attinenti alle singole operazioni di aumento/riduzione del capitale sociale e di fusione o scissione della Società con altre società;
- non devono restituire i conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori della legittima riduzione del capitale sociale in qualsiasi forma, né ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- non possono effettuare riduzioni di capitale al di fuori delle ipotesi di legge o effettuare aumenti di capitale attribuendo quote per un valore inferiore al loro valore nominale;
- non possono, in sede di liquidazione della Società, distrarre i beni sociali dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli.

A. Nell'ambito delle attività di controllo previste dalla legge e dal Modello ed alla formazione della volontà sociale:

- devono assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando, mediante la anticipata e tempestiva trasmissione di tutta la documentazione sulla gestione della Società, ogni forma di controllo sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà aziendale;
- non devono porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o la comunicazione di notizie ed informazioni false o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati (Collegio Sindacale);
- non devono determinare o influenzare l'assunzione delle deliberazioni dell'assemblea ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

D. Nell'ambito delle attività di controllo da parte di Autorità Pubbliche di Vigilanza:

- devono effettuare con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti;
- non devono esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti in relazioni alle condizioni economiche, patrimoniali o finanziarie della Società, né porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza da parte delle suddette Autorità.

E. Nell'ambito le attività di gestione delle risorse finanziarie e dei rapporti con i terzi in genere:

- devono controllare adeguatamente i collaboratori esterni della Società e la congruità dei corrispettivi pagati rispetto all'attività svolta ed alla prassi generale del settore;
- devono rispettare le funzioni attribuite e le procedure interne della Società relative ai rapporti con i terzi e relazionare regolarmente i competenti organi societari, e periodicamente anche l'Organismo di Vigilanza, circa tali rapporti.

Per tutte le operazioni di carattere significativo che coinvolgano la gestione delle risorse finanziarie è necessario seguire le seguenti procedure:

- non deve esserci identità soggettiva tra chi assume o attua le decisioni, chi è tenuto a dare evidenza contabile delle stesse e chi è tenuto ad effettuare sulle stesse i controlli previsti dalla legge;
- devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti con le competenze gestionali e con le responsabilità organizzative affidate alle singole persone;
- il superamento dei limiti fissati può avvenire solo nel rispetto delle vigenti procedure autorizzative e previa adeguata motivazione;
- le operazioni che comportano l'utilizzazione di risorse economiche e/o finanziarie devono avere una causale espressa ed essere, anche in ottemperanza ai principi generali sopra richiamati, documentate, registrate correttamente e verificabili;
- l'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, che ne attesta la congruità: in caso di operazioni ordinarie o compiute entro i limiti quantitativi indicati, la motivazione può essere limitata al riferimento alla classe o tipologia di spesa alla quale appartiene l'operazione, mentre nelle operazioni straordinarie o eccedenti i limiti quantitativi, la motivazione deve essere analitica.

L'Organismo di Vigilanza di LABA curerà che le procedure previste nel presente paragrafo siano idonee al rispetto delle prescrizioni nello stesso contenute e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza circa la deroga attuata e le ragioni che hanno portato alla stessa.

In ogni caso sono fatte comunque salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"C"

Dichiarazioni all'autorità giudiziaria

La legge 116 del 3 agosto 2009 ("*Ratifica ed esecuzione della convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione adottata dall'Assemblea generale dell'ONU il 31 ottobre 2003 nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale*") ha introdotto nel Decreto l'articolo 25-*novies* (poi divenuto articolo 25-*decies* con il D.lgs. 121 del 2011, che ha corretto l'errore di numerazione) rubricato "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

Si tratta del delitto di cui all'articolo 377-*bis* del codice penale.

Art. 377-*bis* del codice penale – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quanto questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.

****

Considerazioni specifiche

Lo scopo della norma in esame è tutelare l'interesse pubblico al corretto svolgimento dell'Autorità Giudiziaria, evitando interferenze volte a turbare la ricerca della verità processuale, e che coloro i quali sono chiamati a rendere dichiarazioni utilizzabili in un procedimento penale possano ricevere indebite pressioni o illecite coercizioni.

La condotta sanzionata consiste nell'uso della violenza o della minaccia o nell'offerta o promessa di denaro od altra utilità al fine di indurre taluno, chiamato a rendere dichiarazioni utilizzabili in un processo, a non rendere alcuna dichiarazione ovvero a rendere dichiarazioni mendaci (fattispecie a dolo specifico).

Il delitto si consuma nel momento e nel luogo in cui viene posta in essere la condotta di costrizione o l'offerta o la promessa di denaro od altra utilità.

L'ipotesi delittuosa si realizza anche nella forma del tentativo.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** le seguenti aree:

- Procuratori speciali e Consiglio di Amministrazione (relativamente alla gestione del contenzioso)

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano :

- Gestione dei rapporti con i Giudici competenti, con i relativi consulenti tecnici e ausiliari, nell'ambito di giudizi civili, penali, amministrativi, giuslavoristici e tributari (procedimenti giudiziari)

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente, qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare.
- conservare a cura della funzione competente i documenti riguardanti l'attività d'impresa nelle suddette aree a rischio con modalità tali da non poter essere modificati, l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.
- conservare la documentazione per eventuali controlli da parte dell'Organismo di Vigilanza.

Per l'area a rischio sopra individuata i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia evitato qualunque comportamento che abbia lo scopo o l'effetto di indurre qualsiasi soggetto a rilasciare false dichiarazioni nell'ambito di un processo penale;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- non devono essere corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non giustificati in relazione al tipo di incarico svolto ed alla prassi e alle tariffe vigenti in ambito locale;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"D"

Omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

L'articolo 9 della legge 3 agosto 2007 n. 123 ha introdotto nel Decreto l'articolo 25 - *septies*, relativo ai reati di omicidio colposo e di lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro successivamente modificato dall'articolo 300 del D.lgs. 81 del 9 aprile 2008 (attuativo della legge n. 123).

Art. 25-*septies* - Omicidio colposo e lesioni colpose gravi o gravissime, commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

1. In relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote, Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.
2. Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.
3. In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi.

Per completezza, si riportano di seguito, le ipotesi di delitto di cui alla sopra menzionata disposizione:

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 sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.

Si applica la pena della reclusione da tre a dieci anni se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale da:
1) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma2, lettere c), del decreto legislativo 30 aprile 1992 n. 285 e successive modificazioni;
2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope.

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.

Art. 590 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 euro trecentonove.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 ad euro 619; se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 ad euro 1.239.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle 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 ad euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica si sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285 e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro 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.

Per la prima volta viene prevista la responsabilità amministrativa degli enti per reati di natura colposa. Naturalmente, è necessario ricordare che le fattispecie di reato sopra riportate assumono rilevanza ai fini del Decreto e, quindi, del presente Modello, laddove gli stessi reati siano commessi "*a vantaggio"* o "*nell'interesse*" della Società. Data la natura colposa dei reati in questione, la responsabilità dell'ente è configurabile solo se dal fatto illecito sia derivato per la società un vantaggio che potrebbe consistere anche in un risparmio di tempi e costi connessi all'implementazione delle misure a salvaguardia dell'igiene e della salute sul lavoro.
Le norme in materia di salute e sicurezza dei lavoratori e sulla tutela dell'igiene nei luoghi di lavoro costituiscono un *corpus* molto ampio e composito, affiancandosi le molte discipline speciali alla disciplina generale applicabile in tale materia. Ed infatti la Legge n. 123/2007 ha dato delega al Governo per il riassetto e la riforma delle disposizioni in materia di salute e sicurezza dei lavoratori nei luoghi di lavoro, mediante uno o più decreti legislativi da emanarsi entro nove mesi dalla data di entrata in vigore della legge stessa, nel limite del livello di protezione, sicurezza e tutela attualmente vigenti (art. 1, comma 3: "*I decreti di cui al presente articolo non possono disporre un abbassamento dei livelli di protezione, di sicurezza e di tutela o una riduzione dei diritti e delle prerogative dei lavoratori e delle loro rappresentanze*"

L'ATTUALE CONTESTO NORMATIVO

Il D.lgs. 9 aprile 2008 n. 81

Con riferimento alla disciplina generale, viene in primo luogo in rilievo, il D.lgs. 81/2008 titolato "*Attuazione dell'articolo 1 della legge 3 agosto 2007 n. 123, in materia di tutela della sicurezza e della salute dei lavoratori*

sul luogo di lavoro", il quale – come precisato dall'art 3 (campo di applicazione) - prescrive misure per la tutela della salute e per la sicurezza dei lavoratori durante il lavoro, in tutti i settori di attività privati o pubblici e per tutte le tipologie di rischio.
Successivamente, il D.lgs. 81/08 è stato più volte modificato e integrato, da ultimo con il D.lgs. 106 del 3 agosto 2009.

Gli obblighi relativi alle norme sulla sicurezza di cui al citato decreto si applicano, per quanto può specificamente rilevare ai fini del Decreto, al datore di lavoro, ai dirigenti ed ai preposti[2], ma – deve ritenersi – anche alle strutture e/o figure interne aziendali e/o esterne che hanno ricevuto specifico incarico dagli stessi ai fini della gestione, applicazione e controllo delle norme, misure e procedure dettate in materia di sicurezza ed igiene sul lavoro.

Senza pretesa di esaustività, si evidenzia come Il D.lgs. 81/2008 contiene numerosi obblighi, tra cui quelli posti a carico del datore di lavoro – nei rispettivi ambiti ed alle specifiche condizioni di applicazione - in materia: di comunicazione alle ASL ed all'Ispettorato del Lavoro ed agli altri organismi ispettivi; di organizzazione dei rapporti con i servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione dell'emergenza; di informazione e formazione dei lavoratori; di provvedimenti in materia di pronto soccorso; di organizzazione e gestione dei luoghi di lavoro; di attrezzature di lavoro e relativa informazione, formazione ed addestramento; di Dispositivi di Protezione Personale e relativa informazione, formazione ed addestramento; di movimentazione manuale dei carichi e relativa informazione, formazione ed addestramento; di uso di videoterminali e relativa informazione, formazione ed addestramento; di protezione da agenti cancerogeni e relativa informazione, formazione ed addestramento; di protezione da agenti biologici e relativa informazione, formazione ed addestramento.
In caso di affidamento di lavori all'interno dell'azienda o di singole unità produttive della stessa, il datore di lavoro ha obblighi specifici (articolo 26) anche nei confronti delle imprese appaltatrici, di quelle che eseguono i lavori in forza di contratti di somministrazione e dei lavoratori autonomi comunque a tal fine impegnati.
Concorrono all'applicazione ed al rispetto delle norme e delle misure e procedure di sicurezza adottate dal datore di lavoro: il servizio di prevenzione e protezione organizzato (ed utilizzato ai fini della sicurezza) dal datore di lavoro, il responsabile del servizio di prevenzione e protezione interno o esterno all'azienda (nominato dallo stesso datore), gli addetti al servizio di prevenzione e protezione interno o esterno all'azienda (nominati dallo stesso datore), il rappresentante per la sicurezza ed e il medico competente, nominato dal datore di lavoro nei casi previsti dal D.lgs. 81/2008, nonché i lavoratori incaricati dallo stesso datore di attuare le misure di prevenzione in particolari campi.

Ai sensi dell'articolo 20 del D.lgs. 81/2008, ogni singolo lavoratore è tenuto a prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle sue azioni o omissioni, conformemente alla sua formazione ed alle istruzioni e ai mezzi forniti dal datore di lavoro ed a rispettare le norme di sicurezza e di igiene del lavoro, ivi incluse le specifiche misure e procedure appositamente adottate a livello aziendale e ad usare i dispositivi di protezione individuale messi a loro disposizione.

Obblighi e responsabilità specifiche sono altresì previste dal richiamato D.lgs. 81/2008 a carico anche dei progettisti dei luoghi e posti di lavoro ed a carico degli installatori e montatori di impianti e macchinari.

Il D.lgs. 81/2008 ha anche approvato incisivi interventi in materia di salute e sicurezza sul lavoro. Tra gli altri, l'articolo 26, comma 5, prevede l'obbligo di indicare specificamente, a pena di nullità, nei contratti di somministrazione, di appalto e di subappalto, di cui agli articoli 1559, 1655 e 1656 del codice civile "*anche qualora già in essere al momento dell'entrata in vigore del D.lgs. 81/2008*", i costi "*delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze nella lavorazioni*". A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori e le organizzazioni sindacali dei lavoratori. A tale proposito la Conferenza delle Regioni e delle Province autonome, in data 20 marzo 2008, ha adottato delle linee guida in materia di stima dei costi della sicurezza nei contratti pubblici dei servizi a frontiere, con ciò fornendo utili criteri applicabili anche negli appalti privati.

Sempre l'articolo 26, comma 8, prevede l'obbligo per il personale occupato dall'impresa appaltatrice o subappaltatrice di munirsi di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Lo stesso obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto (articolo 21, comma 1, lettera c).

Vi è da aggiungere che è di fondamentale importanza l'articolo 14 del D.lgs. 81/2008 (in precedenza articolo 5 della legge n. 123/07) come modificato dal D.lgs. 106/2009, secondo cui gli organi di vigilanza del Ministero del Lavoro e della Previdenza Sociale possono adottare provvedimenti di sospensione di un'attività imprenditoriale "*in relazione alla parte dell'attività imprenditoriale interessata dalle violazioni quando riscontrano l'impiego di personale non risultante dalla documentazione obbligatoria in misura pari o superiore al 20 per cento del totale dei lavoratori presenti sul luogo di lavoro, nonché in caso di gravi e reiterate violazioni in materia di tutela della salute e della sicurezza sul lavoro*". Inoltre, lo stesso articolo 14 dispone che il provvedimento di sospensione sia comunicato alle competenti amministrazioni, "*al fine dell'adozione, da parte del Ministero delle infrastrutture e dei trasporti, di un provvedimento interdittivo alla contrattazione con le pubbliche amministrazioni ed alla partecipazione a gare pubbliche. La durata del provvedimento è pari alla citata sospensione nel caso in cui la percentuale dei lavoratori irregolari sia inferiore al 50 per cento del totale dei lavoratori presenti sul luogo di lavoro; nel caso in cui la percentuale dei lavoratori irregolari sia pari o superiore al 50 per cento del totale dei*

lavoratori presenti sul luogo di lavoro, ovvero nei casi di gravi e reiterate violazioni in materia di tutela della salute e della sicurezza sul lavoro, ovvero nei casi di reiterazione la durata è incrementata di un ulteriore periodo di tempo pari al doppio della durata della sospensione e comunque non superiore a due anni; nel caso di reiterazione la decorrenza del periodo di interdizione è successiva al termine del precedente periodo di interdizione; nel caso di non intervenuta revoca del provvedimento di sospensione entro quattro mesi dalla data della sua emissione, la durata del provvedimento è pari a due anni, fatta salva l'adozione di eventuali successivi provvedimenti di rideterminazione della durata dell'interdizione a seguito dell'acquisizione della revoca della sospensione".

Si segnala, infine che, con Circolare n. 33 del 10 novembre 2009, il Ministero del Lavoro e della Previdenza Sociale, ha emanato le istruzioni applicative e i chiarimenti relativi al provvedimento di sospensione, resisi necessari alla luce delle modifiche apportate al D.lgs. 81/2008 dal D.lgs. 109/2009. La nuova Circolare viene così a sostituire la precedente, n. 10797 del 22 agosto 2007.

****

Considerazioni specifiche

Al fine di valutare i possibili ambiti aziendali esposti a maggior rischio è necessario premettere che:

A. la normativa antinfortunistica e sulla sicurezza ed igiene sul lavoro interessa sia la sede aziendale, sia ogni unità produttiva, intesa quale stabilimento o struttura finalizzata alla produzione di beni o servizi, dotata di autonomia finanziaria e tecnico funzionale;

B. oltre ai lavoratori subordinati ed autonomi che svolgono attività lavorativa nella sede aziendale e nelle unità produttive, la normativa deve essere osservata anche nei confronti (ed a tutela) degli appaltatori, subappaltatori e somministratori di lavoro che operano, comunque, in tali sedi;

C. la sanzione amministrativa prevista dal Decreto (come modificato dalla L. 123/2007) a carico della società, in caso di omicidio e/o lesioni gravi o gravissime verificatosi per inosservanza della richiamata materia – che si aggiunge alle sanzioni penali irrogate, ai sensi della normativa generale, ai soggetti che violano dette norme - è applicabile, oltre che in caso di dolosa violazione (ossia preordinata e volontaria), anche se la violazione stessa è commessa con colpevole inosservanza delle norme medesime (ossia per negligenza, imprudenza o imperizia);

D. i reati di cui alla presente parte speciale vengono puniti anche ove cagionati da condotte omissive, ossia in tutti i casi in cui il soggetto interessato abbia omesso di porre in essere tutti gli accorgimenti e le misure idonee ad evitare il verificarsi delle fattispecie previste;

E. l'elemento soggettivo consiste nella c.d. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte ad impedire gli eventi dannosi previsti dalla norma incriminatrice.

Nel caso di LABA si possono individuare come **attività "a rischio"** le attività che genericamente riguardano la gestione della sicurezza nei luoghi di lavoro.

Si ritiene che interessati dalle disposizioni della presente parte speciale siano, oltre al datore di lavoro, ai dirigenti ed ai preposti:

- i soggetti facenti parte del servizio di prevenzione e protezione organizzato dal datore di lavoro;
- il responsabile del servizio di prevenzione e protezione interno o esterno all'azienda (nominato dallo stesso datore di lavoro);
- gli addetti al servizio di prevenzione e protezione interno o esterno all'azienda;
- il rappresentante per la sicurezza a livello aziendale;
- il medico competente, nominato dal datore di lavoro nei casi previsti all'art. 18 del D.lgs. 81/2008;
- i lavoratori incaricati dallo stesso datore di lavoro di attuare le misure di prevenzione in particolari campi;
- i singoli lavoratori.

I reati sopra menzionati potrebbero essere commessi da tali soggetti ove - naturalmente - non adempiano esattamente ed integralmente a tutti gli obblighi, funzioni e compiti previsti a loro carico dalla normativa richiamata (cui si rimanda) ed ove non osservino le procedure e misure adottate a livello aziendale in materia di salute, sicurezza ed igiene nei luoghi di lavoro e ciò anche, ad esempio, ove detto inadempimento avvenga attraverso l'omissione di informazioni dovute, di alterazione di documenti necessari a livello aziendale a tali fini e di alterazione di documenti da presentare ad autorità di controllo in tale materia o attraverso la produzione di documenti falsi per far risultare rispettate le normative richiamate o per attestare a tal fine atti, fatti o circostanze inesistenti o, ancora, per modificare dati già trasmessi.

In ogni caso, oltre a quanto si dirà *infra*, in via generale, in relazione ai principi di comportamento che i destinatari della normativa richiamata devono seguire, con riferimento alle sopra descritte ipotesi di reato dovranno essere adottate procedure che consentano:

1. di attuare un controllo preventivo e continuativo delle attività a rischio, della valutazione dei rischi e delle misure di sicurezza adottate ed attuate a livello aziendale e della documentazione aziendale predisposta a tal fine, provvedendo ad aggiornare la stessa;

2. di definire ed attuare la circolazione delle informazioni e delle buone pratiche utili a favorire la promozione e la tutela della salute, sicurezza ed igiene nei luoghi di lavoro;
3. di garantire la costante formazione ed aggiornamento del personale e dei lavoratori che gestiscono o sono tenuti ad osservare le procedure in materia di salute, sicurezza ed igiene sul lavoro;
4. di controllare e monitorare costantemente la concreta applicazione e rispetto delle procedure e delle misure adottate a livello aziendale ai fini della salute, sicurezza ed igiene nei luoghi di lavoro ed il costante utilizzo da parte dei lavoratori dei dispositivi di protezione individuali.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno di LABA si possono individuare come aree "a rischio", le seguenti aree:

- Consiglio di Amministrazione
- Direzione Amministrativa
- RSPP (relativamente agli adempimenti di cui all'articolo 33 del D.lgs. 81/2008, tra cui, nello specifico, individuazione dei fattori di rischio, valutazione dei rischi ed individuazione delle misure per la sicurezza e salubrità degli ambienti di lavoro, elaborazione delle misure preventive e protettive, elaborazione delle procedure di sicurezza, proposizione di programmi di formazione ed informazione dei lavoratori).

All'interno delle aree sopra richiamate, le operazioni "a rischio" nelle quali possono essere commessi i reati di omicidio colposo e lesioni personali gravi o gravissime di cui all'articolo 25-*septies* del Decreto sono:

- Adempimenti in materia di sicurezza e salute del lavoro.
- Nomina RSPP e medico competente.
- Determinazione del budget per la sicurezza.
- Elaborazione ed aggiornamento DVR per tutti i rischi aziendali e DUVRI.
- Individuazione e formazione dirigenti e preposti
- Formazione ed informazione ai dipendenti e collaboratori.
- Fornitura DPI adeguati al rischio.
- Formazione ed informazione ai dipendenti.
- Gestione rapporti con consulenti esterni.
- Adempimenti in materia di prevenzione incendio e primo soccorso.
- Manutenzione attrezzature ed impianti presso le sedi di lavoro, ecc.

La presente parte speciale indica le regole di condotta che i datori di lavoro, i procuratori, i dirigenti e preposti (ma anche i lavoratori, subordinati ed autonomi, gli appaltatori, i subappaltatori ed i somministratori di lavoro ed i terzi che abbiano rapporti con la Società nonché le figure chiamate a garantire l'applicazione a livello aziendale della normativa richiamata) che agiscono nell'ambito delle aree a rischio sopra individuate (i "Destinatari") devono osservare, al fine di impedire il verificarsi dei suddetti delitti, puniti anche in forza del Decreto.

I Destinatari devono attenersi ai seguenti principi:

A. stretta osservanza delle leggi, dei regolamenti, delle procedure e delle misure di prevenzione e protezione e di igiene adottate a livello aziendale;
B. osservanza dei criteri di massima trasparenza e correttezza nell'instaurazione di qualsiasi rapporto con qualsiasi autorità di vigilanza nella materia *de qua* (quali, ad esempio, ASL territorialmente competenti, Ispettorati del lavoro, Direzioni Provinciali del Lavoro, Vigili del Fuoco, Istituti previdenziali, ecc);
C. attenta e corretta predisposizione e conservazione nella sede aziendale o nell'unità produttiva, dei documenti riguardanti la materia della sicurezza e salute dei lavoratori e l'igiene dei luoghi di lavoro, documenti che dovranno essere redatti con modalità tali da non poter essere modificati, se non con apposita evidenza e che potranno essere accessibili solamente al soggetto competente o ad un suo delegato, secondo le norme aziendali interne;
D. astenersi dal porre in essere comportamenti che integrino le fattispecie delittuose sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.

Ai fini dell'attuazione dei comportamenti di cui sopra, i Destinatari devono mantenere un costante rapporto di informazione con gli organi aziendali di vertice e con l'Organismo di Vigilanza, interpellare quest'ultimo anche per questioni interpretative attinenti all'osservazione ed alle procedure preventive previste dal presente Modello e riferire immediatamente all'Organismo di Vigilanza circa eventuali situazioni di irregolarità, trasmettendo allo stesso ogni documentazione pertinente e tenendo a disposizione dello stesso tutta la documentazione relativa.

I Destinatari devono rendere edotti i terzi che, a vario titolo, entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

L'Organismo di Vigilanza di LABA curerà che le procedure previste nel presente paragrafo siano idonee al rispetto delle prescrizioni nello stesso contenute e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"E"

Ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita

L'articolo 63 del Decreto Legislativo 21 novembre 2007 n. 231 ha introdotto nel Decreto l'articolo 25-*octies*, relativo ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Art. 648 del codice penale – Ricettazione

Fuori dai 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 farli acquistare, ricevere od occultare, è punito con la reclusione da due od otto annui e con la multa da euro 516 a euro 10.329.

La pena è della reclusione sino a sei anni e della 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 o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

****

Considerazioni specifiche

L'interesse tutelato dalla norma in esame è l'incriminazione di traffici che abbiano per oggetto le cose provenienti da delitti. Presupposto della ricettazione è l'esistenza di un delitto anteriore, ma non è necessario che tale delitto sia giudizialmente accertato nei confronti dell'autore del reato.

Scopo della previsione è quella di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale e, in via mediata, di evitare la commissione di quest'ultimo imponendo limiti alla circolazione dei beni provenienti dal reato stesso.

La ricettazione è un reato comune, che può essere commesso da chiunque, e di danno, in quanto richiede l'offesa del bene protetto.

L'elemento soggettivo del reato è il dolo specifico, poiché oltre alla coscienza e volontà del fatto tipico, vi è l'ulteriore scopo di procurare a sé o ad altri un profitto.

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 euro 1.032 a euro 15.493.*

La pena è aumentata quando il fatto è 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'articolo 648".

****

Considerazioni specifiche

La norma in esame presenta un'oggettività giuridica complessa: oltre alla tutela di interessi di natura patrimoniale, il delitto è posto a tutela dell'ordine economico in relazione ai turbamenti che l'attività di riciclaggio può generare quanto alla libertà e correttezza del mercato.

Scopo della disposizione è quello di impedire che gli autori dei reati possano far fruttare i capitali illegalmente acquisiti, rimettendoli in circolazione "ripuliti" e dunque investibili anche in attività economiche produttive lecite. In tal modo, la norma si propone anche l'obiettivo di scoraggiare la commissione del reato principale, ostacolando la possibilità di sfruttarne i proventi.

L'elemento soggettivo del reato è il dolo generico consistente nella coscienza e volontà di compiere attività di riutilizzazione di denaro, beni o altre utilità di provenienza illecita. L'ignoranza circa la provenienza degli stessi esclude il dolo e, dunque, il reato, mentre continua a sussistere la punibilità a titolo di dolo eventuale in caso di dubbio circa la fonte dei beni o delle altre utilità.

Il reato si consuma nel momento in cui è compiuta la sostituzione o il trasferimento o l'operazione atta ad ostacolare l'identificazione della provenienza delittuosa del denaro o dei beni o di altre utilità.

È quindi necessario informare tutti i soggetti interessati all'interno della Società della normativa di riferimento e della procedura in materia di gestione delle risorse finanziarie di cui all'Allegato A al presente Modello e portare a conoscenza degli stessi ogni eventuale modifica o aggiornamento.

Art. 648-ter del codice penale – 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 648bis, 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 euro 1.032 a euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648.

Si applica l'ultimo comma dell'articolo 648.

****

Considerazioni specifiche

Si tratta di una fattispecie che si differenzia dall'ipotesi di riciclaggio (art. 648-bis cod. pen.) poiché, mentre quest'ultimo reato prevede la sostituzione, il trasferimento o le operazioni di ostacolo alla identificazione delle provenienze illecite, la figura in esame punisce l'impiego in attività economiche o finanziarie delle stesse.
Si ritiene che per "impiegare" debba intendersi "investire": dunque, si fa riferimento ad un utilizzo a fini di profitto.
Vengono punite, in sostanza, anche quelle attività mediate che non sostituiscono immediatamente i beni provenienti da taluni illeciti, ma che comunque consentono l'occultamento dei capitali illeciti e l'arricchimento delle associazioni criminali colpendo una serie di attività di investimento solo apparentemente legali (quali ad esempio, attività di arricchimento derivante da appalti, concessioni, commercio, attività di gioco o scommesse, ecc.)
L'elemento soggettivo del reato è costituito dal dolo generico. È configurabile anche l'ipotesi del tentativo.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come aree "a rischio" le seguenti aree:

- Consiglio di Amministrazione
- Direzione Amministrativa
- Ufficio tesoreria

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano la gestione della tesoreria e della cassa (es. ricevimento pagamenti in contante).

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione :

- I Destinatari devono astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.

- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- siano effettuati i necessari controlli sui beni e le risorse di provenienza esterna;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati;
- siano effettuate con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

La presente Sezione della Parte Speciale prevede, inoltre, l'espresso divieto di effettuare o ricevere pagamenti in contanti, salvo che si tratti di somme di modico valore, o di acquisti urgenti, che non possano essere preventivati.

PROTOCOLLI

Gestione dei flussi finanziari in entrata ed instaurazione e gestione dei rapporti di incasso continuativi

Principi di controllo

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e dei **livelli autorizzativi** da associarsi alle operazioni.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:

- richiesta dell'ordine di pagamento o di messa a disposizione effettuazione del pagamento, o Controllo/riconciliazioni a consuntivo;
- esistenza di livelli autorizzativi sia per la richiesta, che per l'ordine di pagamento o di messa a disposizione, articolati in funzione della natura dell'operazione (ordinaria/straordinaria) e dell'importo;
- esistenza e diffusione di *specimen* di firma in relazione ai livelli autorizzativi definiti per la richiesta;
- effettuazione di periodica attività di riconciliazione dei conti intrattenuti con banche;
- tracciabilità degli atti e delle singole fasi del processo (con specifico riferimento all'annullamento dei documenti che hanno già originato un pagamento).

Eventuali modalità non standard (relative sia a operazioni di natura ordinaria che straordinaria) devono essere considerate “in deroga" e soggette, pertanto, a criteri di autorizzazione e controllo specificamente definiti riconducibili a:

- individuazione del soggetto che può richiedere l'operazione;
- individuazione del soggetto che può autorizzare l'operazione;
- indicazione, a cura del richiedente, della motivazione;

- designazione (eventuale) della risorsa abilitata all'effettuazione/autorizzazione dell'operazione attraverso procura *ad hoc*.

Aspetti operativi

- **Incassi (Tesoreria , Ufficio amministrativo**) :

➢ Fatture vendita : monitoraggio conti correnti in base allo scadenziario. A seguito del mancato incasso si procede con il sollecito.

➢ Retta studenti : se pagamento si procede alla ottenuto registrazione contabile, se è insoluto si avvia la procedura recupero crediti (responsabile amministrativo)

- **Pagamenti**:

➢ Fornitori (pagamento con RIBA o B/B) : trasmissione elenco corredato di copia fattura dalla responsabile amministrativa all'AD per approvazione. Quindi caricamento in home banking per pagamento.

➢ Dipendenti : ricezione flusso dal consulente del lavoro, verifica correttezza dall'AD. Ottenuta l'approvazione, si procede al pagamento.

➢ Contributi e tasse : caricate da Ufficio amministrativo (stessa procedura dei fornitori). Pagate dal consulente tramite procedura Entratel. Trasmissione del flusso, verifica amministrativa e dell'AD che sia tutto corretto. Quindi il consulente procede con il pagamento.

Sistema Organizzativo

Le aree di responsabilità sono formalmente definite attraverso apposite deleghe/procure

Organizzazione interna a supporto dell'Odv

Con periodicità **semestrale** devono essere fornite all'Organismo di Vigilanza da parte dell'Amministratore ovvero suo delegato le seguenti informazioni:

- elenco dei flussi monetari e/o finanziari non standard (operazioni straordinarie e/o in deroga) realizzati nel periodo;
- elenco delle funzioni aziendali che possono richiedere flussi monetari e/o finanziari in modalità non standard (allegando le relative deleghe operative e specimen di firma);

Più in generale, Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.
Inoltre, in ottemperanza a quanto previsto dall' articolo 52 del Decreto Legislativo 231/2007 (così come modificato dal D.lgs. 151 del 25 settembre 2009) l'Organismo di Vigilanza:

- comunica, senza ritardo, alle autorità di vigilanza di settore tutti gli atti o i fatti di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate dall'autorità di vigilanza del settore;
- comunica, senza ritardo, ai legali rappresentanti della Società le infrazioni agli obblighi di segnalazione di operazioni sospette (di cui all'articolo 41 del D.lgs. 16 novembre 2007) di cui ha notizia;
- comunica, entro trenta giorni, al Ministero dell'economia e delle finanze le infrazioni di cui ha notizia relativamente alle limitazioni all'uso del contante e dei titoli al portatore (di cui agli articoli 49 e 50 del D.lgs. 16 novembre 2007);
- comunica, entro trenta giorni, alle autorità di vigilanza del settore le infrazioni agli obblighi di registrazione (di cui all'articolo 36 del D.lgs. 16 novembre 2007) di cui ha notizia.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.
Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"F"

Reati tributari

La Legge 19 dicembre 2019, n. 157, a conversione del D.L. 26 ottobre 2019, n. 124 (recante "*Disposizion urgenti in materia fiscale e per esigenze indifferibili"*), ha inserito l'art. 25-*quinquiesdecies* al D.Lgs. 231/2001, rubricato "*Reati tributari*". Si tratta di una serie di reati, contemplati nel D.Lgs. 10 marzo 2000, n. 74 "*Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205*", i quali ampliano il novero dei reati presupposto, estendendo la responsabilità amministrativa da reato delle società/enti anche all'ambito penale tributario.
Va premesso che l'art.1 del D.Lgs. 10 marzo 2000, n.74, enuclea una serie di definizioni di carattere generale applicabili a tutti i reati tributari, ai fini di una migliore comprensione delle disposizioni normative:

a) per "fatture o altri documenti per operazioni inesistenti" si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, emessi a fronte di operazioni non realmente effettuate in tutto o in parte o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero che riferiscono l'operazione a soggetti diversi da quelli effettivi;
b) per "elementi attivi o passivi" si intendono le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e le componenti che incidono sulla determinazione dell'imposta dovuta;
c) per "dichiarazioni" si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
d) il "fine di evadere le imposte" e il "fine di consentire a terzi l'evasione" si intendono comprensivi, rispettivamente, anche del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e del fine di consentirli a terzi;
e) riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il "fine di evadere le imposte" ed il "fine di sottrarsi al pagamento" si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
f) per "imposta evasa" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;
g) le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
g-bis) per "operazioni simulate oggettivamente o soggettivamente" si intendono le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero le operazioni riferite a soggetti fittiziamente interposti;

g-ter) per "mezzi fraudolenti" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

Inoltre, va premesso anche che le sanzioni pecuniarie indicate nelle singole fattispecie di reati tributari sono aumentate di un terzo, nel caso in cui l'ente/società abbia conseguito un profitto di rilevante entità nella commissione di tali reati.[3]

A. FATTISPECIE DI REATI TRIBUTARI (Art. 25-quinquiesdecies, comma 1, D.Lgs. 231/2001)

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (Art. 2, D.Lgs. 10 marzo 2000, n.74)

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.[4]

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni. [5]

****

Considerazioni specifiche

Trattasi di un reato commissivo, tramite il quale il legislatore ha inteso rinforzare la tutela del bene giuridico protetto (vale a dire l'interesse dell'Erario alla percezione dei tributi), che si consuma nel momento della presentazione o della trasmissione in via telematica della dichiarazione nella quale sono indicati gli elementi

1. [3] A norma dell'art.25-*quinquiesdecies,* comma 2.
2. [4] L'ente è punito con la sanzione pecuniaria fino a cinquecento quote, a norma dell'art. 25-*quinquiesdecies,* comma 1, lett. a), del D.Lgs. 231/2001
3. [5] L'ente è punito con la sanzione pecuniaria fino a quattrocento quote, a norma dell'art.25-*quinquiesdecies*, comma 1, lett. b), del D.Lgs. 231/2001

passivi fittizi. Esso ha natura istantanea e si consuma con la presentazione della dichiarazione annuale ai fini delle imposte sui redditi o sul valore aggiunto, non avendo rilievo le dichiarazioni periodiche e quelle relative ad imposte diverse, con la conseguenza che il comportamento di utilizzazione di fatture o altri documenti per operazioni inesistenti, si configura come meramente strumentale e prodromico per la realizzazione dell'illecito, nonché penalmente irrilevante. Ciò in quanto il delitto di cui all'art. 2 citato è posto a tutela dell'interesse patrimoniale dello Stato a riscuotere ciò che è fiscalmente dovuto e nell'ambito e nei limiti in cui è dovuto in forza del diritto tributario.

Nel caso previsto dal comma 2, la sanzione prevista dall'art.25-*quinquiesdecies,* comma 1, lett. a), è quella pecuniaria, fino a cinquecento quote. Nel caso previsto dal comma 2-*bis*, invece, vale a dire se l'ammontare degli elementi passivi fittizi è inferiore ad euro centomila, si applica la sanzione pecuniaria prevista dalla lett. b), fino a quattrocento quote.

- **Dichiarazione fraudolenta mediante altri artifici** (Art. 3, D.Lgs. 10 marzo 2000, n.74)

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

****

Considerazioni specifiche

La fattispecie delineata è un reato a soggettività ristretta, potendo essere realizzato solo da coloro che sono obbligati alla presentazione della dichiarazione dei redditi, e a condotta bifasica che si articola in due segmenti: 1) la dichiarazione mendace e 2) l'attività ingannatoria a sostegno del mendacio materializzato nella dichiarazione. Il reato, previsto dall'art. 25-*quinquiesdecies*, comma 1, lett. c), prevede la sanzione pecuniaria fino a cinquecento quote, nel caso in cui la dichiarazione fraudolenta sia effettuata compiendo operazioni simulate oggettivamente o soggettivamente, nonché nel caso in cui l'ente si sia avvalso di documenti falsi o altri mezzi, al fine di indicare in dichiarazione degli elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizi.

- **Emissione di fatture o altri documenti per operazioni inesistenti** (Art. 8, D.Lgs. 10 marzo 2000, n.74)

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.[6]

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni. [7]

****

Considerazioni specifiche

L'emissione di fatture per operazioni inesistenti è un reato istantaneo, che si consuma nel momento in cui l'emittente perde la disponibilità della fattura, non essendo richiesto che il documento pervenga al destinatario, né che quest'ultimo lo utilizzi. La fattispecie in oggetto si realizza allorché un soggetto, al fine di consentire a terzi l'evasione sulle imposte dei redditi o dell'IVA, emetta o rilasci fatture o altri documenti per operazioni inesistenti: in tal caso, la sanzione pecuniaria è prevista fino a cinquecento quote (art.25-*quinquiesdecies*, comma

4. [6] L'ente è punito con la sanzione pecuniaria fino a cinquecento quote, a norma dell'art.25-*quinquiesdecies*, comma 1, lett. d), del D.Lgs. 231/2001
5. [7] L'ente è punito con la sanzione pecuniaria fino a quattrocento quote, a norma dell'art.25-*quinquiesdecies*, comma 1, lett. e), del D.Lgs. 231/2001

1, lett. d), ridotta a quattrocento quote nel caso in cui l'importo non corrispondente al vero è inferiore ad euro centomila (art.25-*quinquiesdecies*, comma 1, lett. e).

- **Occultamento o distruzione di documenti contabili** (Art. 10, D.Lgs. 10 marzo 2000, n.74)

1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

****

Considerazioni specifiche

Il delitto di occultamento della documentazione contabile ha natura di reato permanente, in quanto la condotta penalmente rilevante si protrae sino al momento dell'accertamento fiscale, che coincide con il *dies a quo* da cui decorre il termine di prescrizione[8]. La fattispecie, prevista dall'art.25-*quinquiesdecies*, comma 1, lett. f), prevede una sanzione pecuniaria fino a quattrocento quote, nel caso in cui vengano occultati o distrutti dei documenti o delle scritture contabili, la cui conservazione è obbligatoria, al fine di evadere le imposte sui redditi o sul valore aggiunto.

- **Sottrazione fraudolenta al pagamento di imposte** (Art. 11, D.Lgs. 10 marzo 2000, n.74)

1. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o

compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi

6. [8] Cassazione Sez. 3, 5974/2013.

fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

****

Considerazioni specifiche

La fattispecie costituisce reato di pericolo, integrato dal compimento di atti simulati o fraudolenti volti a occultare i propri o altrui beni, idonei a pregiudicare l'attività recuperatoria dell'amministrazione finanziaria, a prescindere dalla sussistenza di un'esecuzione esattoriale in atto. Ai fini dell'integrazione del reato in esame - che sanziona la condotta di chiunque alieni simulatamente o compia atti fraudolenti su beni al fine di sottrarsi al versamento delle imposte o di sanzioni ed interessi pertinenti a dette imposte - non è necessario che sussista una procedura di riscossione in atto[9]. La fattispecie, prevista dall'art.25-*quinquiesdecies*, comma 1, lett. g), prevede una sanzione pecuniaria fino a quattrocento quote, nel caso in cui un soggetto alieni simulatamente o compia altri atti fraudolenti sui propri o su altrui beni, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto o di sanzioni amministrative, nonché nel caso in cui indichi nella documentazione presentata ai fini della procedura di transizione fiscale degli elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

B. REATI DI LOTTA CONTRO LA FRODE CHE LEDE GLI INTERESSI FINANZIARI DELL'UNIONE MEDIANTE IL DIRITTO PENALE (Art. 25-quinquiesdecies, comma 1-bis, D.Lgs. 231/2001)

Con il Decreto Legislativo n. 75 del 14 luglio 2020 è stata recepita in via definitiva la Direttiva (UE) 2017/1371 (cd. Direttiva PIF) del Parlamento europeo e del Consiglio Europeo del 5 luglio 2017,

recante norme per la "*lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*". All'art.25-*quinquiesdecies* è stato aggiunto il comma 1-*bis*.

- **Dichiarazione infedele** (Art. 4, D.Lgs. 10 marzo 2000, n.74)

1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali

7. [9] Cassazione Sez. 7, 46523/2019

relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

****

Considerazioni specifiche

È prevista una sanzione pecuniaria fino a 300 quote, a norma dell'art.24-*quinquiesdecies*, comma 1-*bis*, lett. a), per il reato di dichiarazione infedele.

- **Omessa dichiarazione** (Art. 5, D.Lgs. 10 marzo 2000, n.74)

1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

****

Considerazioni specifiche

Per il reato di omessa dichiarazione, l'art. 25-*quinquiesdecies*, comma 1-*bis*, lett. b), prevede una sanzione pecuniaria fino a 400 quote.

- **Indebita compensazione** (Art. 10-*quater*, D.Lgs. 10 marzo 2000, n. 74)

1. È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.

2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

****

Considerazioni specifiche

Per il reato di indebita compensazione, l'art.25-*quinquiesdecies*, comma 1-*bis*, lett. c), prevede una sanzione pecuniaria fino a 400 quote

PRINCIPI GENERALI DI COMPORTAMENTO

Di seguito vengono esposte le linee guida di comportamento da seguire per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex lege 231.

Tali linee guida si riferiscono a comportamenti relativi all'area del "fare" e del "non fare", specificando in chiave operativa quanto espresso dai principi del MOGC dell'Ente.

La presente Parte Speciale prevede l'espresso divieto a carico dei destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra indicate;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato sopra indicate, possano potenzialmente diventarlo ;

È inoltre sancito l'espresso obbligo di:

- tenere comportamenti in linea con i principi espressi nel presente Modello Organizzativo;
- rispettare le procedure adottate con particolare riferimento a quelle relative alla gestione delle attività sensibili di seguito elencate;
- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- assicurare la veridicità dei dati predisposti;
- assicurare la trasparente gestione delle forniture, di beni e servizi;
- acquistare beni di provenienza garantita e servizi e/o qualsiasi altra utilità ad un prezzo che, salvo casi eccezionali e certificati (quali ad esempio acquisti da aste giudiziarie o da fallimenti), sia commisurato alla qualità e quantità dei beni stessi in base al valore di mercato;
- rispettare la normativa fiscale-tributaria;
- garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali.

PROTOCOLLI

Nell'ambito di tutte le operazioni che concernono le attività sensibili il sistema di controllo dovrà basarsi sui seguenti principi di controllo.

1. **Gestione dei flussi delle transazioni finanziarie, gestione della fiscalità, gestione amministrativo - contabile**

Principi di controllo

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della **valutazione** complessiva delle forniture.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:

- Gestione della contabilità generale
- Gestione delle attività di predisposizione del bilancio di esercizio e delle relazioni periodiche relative alla situazione economica e finanziaria della società
- Gestione della piccola cassa
- Gestioni incassi e pagamenti
- Monitoraggio degli aggiornamenti normativi in ambito fiscale
- Gestione e monitoraggio del calendario fiscale
- Processo di determinazione degli importi dovuti, dei versamenti e della presentazione delle dichiarazioni relative alle imposte sui redditi e sul valore aggiunto
- Liquidazione e versamento dei tributi
- Predisposizione e presentazione delle dichiarazioni fiscali
- Tenuta e custodia della documentazione obbligatoria
- Attività di calcolo e imputazione in compensazione di eventuali crediti nei confronti dell'Erario.
- Processo di archiviazione e tenuta della documentazione di cui è obbligatoria la conservazione.

- I comportamenti devono uniformarsi al rispetto dei requisiti normativi.
- Eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto devono essere gestiti assicurando il rispetto di leggi, regolamenti e principi contenuti nel Modello ex D.lgs.231/2001 e norme collegate.
- Verificare il rispetto della normativa esistente nel caso di compensazioni tra crediti tributari e debiti tributari per I.V.A..
- Verificare la reale corrispondenza tra versamenti e dichiarazioni.
- Verificare la quadratura circa la corrispondenza degli importi dovuti a titolo di I.V.A. con i registri e i relativi conti di contabilità generale.
- Assicurare che le operazioni per le quali è richiesto l'utilizzo o l'impiego di risorse economiche o finanziarie abbiano l'indicazione di una causale e la loro documentazione e registrazione sia in conformità ai principi di correttezza professionale e contabile.
- Verificare la precisa finalità delle figure giuridiche (es. creazione di un trust), quindi verificare l'esistenza di precise richieste da parte dell'amministrazione finanziaria (documenti giustificativi), al fine di evitare la creazione di strutture fittizie finalizzate a nascondere beni.

- È fatto divieto occultare e/o distruggere in tutto o in parte le scritture contabili e/o i documenti di cui è obbligatoria la conservazione
- E' fatto divieto porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti, o che ostacolino lo svolgimento dell'attività di controllo e/o di revisione da parte degli organi di controllo.
- E' fatto divieto ostacolare, in ogni modo, l'effettuazione di verifiche, accertamenti ed ispezioni da parte di Autorità di settore, fiscali o giudiziarie.
- Permettere e garantire lo svolgimento dell'attività di analisi del bilancio di verifica, la predisposizione del prospetto di bilancio e la condivisione con il management aziendale e con gli organi di controllo.
- Tutti i dati e le informazioni necessarie alla redazione del bilancio e degli altri documenti contabili della Società devono essere chiari, completi e rappresentare in modo veritiero la situazione economica, finanziaria e patrimoniale della Società.
- La rilevazione, la trasmissione e l'aggregazione dei dati e delle informazioni contabili, per la redazione del bilancio di esercizio, deve avvenire con modalità tali (anche per il tramite del sistema informativo contabile aziendale) da assicurare che vi sia sempre evidenza dei passaggi del processo di formazione dei dati, e sia sempre individuabile il soggetto che ha inserito i dati nel sistema.
- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla redazione dei documenti previsti dalla normativa fiscale e tributaria, con particolare riguardo alle dichiarazioni rivolte all'Amministrazione Finanziaria, al fine di fornire a quest'ultima un'informazione veritiera e corretta sulle obbligazioni d'imposta della Società e, più in generale, elementi reali e attendibili afferenti il rapporto giuridico tributario tra Società ed Erario.
- Garantire la tracciabilità dei profili di accesso, con il supporto di sistemi informatici, nel processo di identificazione dei soggetti che inseriscono i dati nel sistema, garantendo la separazione delle funzioni e la coerenza dei livelli autorizzativi, nell'ambito della rilevazione, trasmissione e aggregazione delle informazioni contabili finalizzate alla predisposizione non solo delle comunicazioni sociali, ma anche delle dichiarazioni fiscali.

E' fatto divieto di :

- Omettere o fornire dati ed informazioni inesatte o non complete imposte dalla legge sulla situazione economica, patrimoniale e finanziaria della società.
- Violare, eludere, evadere obblighi di dichiarazione, attestazione, certificazione di natura tributaria previsti dalla legge.

- Indicare in una delle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Organismo di Vigilanza

Sulla base delle informazioni e delle documentazioni ricevute, l' Organismo di Vigilanza potrà valutare la coerenza tra quanto descritto dal responsabile di funzione e quanto formalizzato all'interno della procedura.

2. Gestione delle spese di rappresentanza e delle ospitalità

Principi di controllo

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della **valutazione** complessiva delle forniture.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:

- Gestione delle spese di rappresentanza e delle ospitalità
- Identificazione dei soggetti aziendali autorizzati a rappresentare l'azienda nei rapporti con la P.A. per il sostenimento di spese di rappresentanza.
- Definizione delle tipologie, dei limiti e delle finalità delle spese di rappresentanza/ospitalità consentiti.
- Adozione di sistemi di tracciabilità delle spese di rappresentanza/ospitalità offerti e dei relativi destinatari.
- Definizione di specifici livelli approvativi in relazione all'erogazione di spese di rappresentanza/ospitalità.
- Definizione delle modalità di rendicontazione delle spese di rappresentanza/ospitalità effettuate, con indicazione del beneficiario e dello scopo della spesa.

3. Gestione del personale

Principi di controllo

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della **valutazione** complessiva delle forniture.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:

- Gestione amministrativa del personale
- Gestione note spese del personale

• Identificazione delle modalità di apertura e successiva gestione dell'anagrafica del dipendente.
• Verifica della completezza e accuratezza delle buste paga.
• Autorizzazione all'esecuzione del pagamento degli stipendi.
• Verifica della coerenza tra bonifici effettuati al personale e cedolini.
• Definizione della modalità di rendicontazione delle spese effettuate, con indicazione dello scopo della spesa.
• Definizione delle modalità di approvazione dei resoconti e dei conseguenti rimborsi delle spese sostenute.

PROCEDURA ACQUISTI

Acquisti area didattica

1. Il responsabile di dipartimento compila apposito modulo di richiesta (in cui è indicato nome del richiedente, prodotto/servizio richiesto, prezzo, sezione del budget cui imputare l'acquisto).
2. Al modulo di richiesta va allegato preventivo (a meno che ciò non sia necessario);
3. Nel compilare il modulo il responsabile di dipartimento farà esclusivamente riferimento ad un paniere di fornitori preventivamente selezionato dall'Amministrazione - partner ufficiali)
4. Il responsabile di dipartimento sottoscrive il modulo;
5. Il modulo va poi validato dal direttore/vice direttore che controlla la conformità dell'ordine al budget e alle necessità dell'Accademia;
6. Per eventuali urgenze (non ve ne dovrebbero essere) va contattata immediatamente Roberta che autorizza in deroga (salvo poi produrre in ogni caso l'ordine di spesa come da punti precedenti);
7. Il modulo va poi consegnato all'ufficio acquisti (Michela Marchina):
    a. Se la spesa è prevista a budget l'amministrazione procede con l'ordine;
    b. Vanno esclusi tassativamente i pagamenti con rimessa diretta o anticipati (le eccezioni vanno gestite ed autorizzati dal Responsabile amministrativo – Roberta Bilancini);
    c. Se la spesa non è prevista dal budget ed è di importo < 500 euro l'ufficio acquisti procede con l'ordine;
    d. per importi maggiori necessaria firma dell'amministratore delegato – Emanuela Zanchetta /

Gianluca Delbarba;

8. L'ufficio acquisti informa la persona incaricata del ritiro della merce inviandogli copia dell'ordine;
9. Il soggetto incaricato alla consegna verifica la conformità della merce all'ordine e l'integrità della stessa;
10. I documenti in originale vanno poi consegnati in Amministrazione all'ufficio acquisti;
11. In Amministrazione l'ufficio acquisti abbina bolla/fattura accompagnatoria ricevuta dal soggetto incaricato coneventuale fattura pro-forma e con l'ordine controllando correttezza;
12. Il tutto viene consegnato in Amministrazione – Lorena Maggioni – che abbina fattura elettronica con bolla/ordine.

Acquisti e servizi manutenzione

1. Il soggetto responsabile delle varie sedi rileva la necessità di manutenzione e compila apposito ordine a meno che il materiale non sia già disponibile a magazzino in cui è indicato nome del richiedente, prodotto/servizio richiesto, prezzo, immobile di riferimento);
2. La rilevazione di dette necessità può essere rilevata anche dagli amministratori provvisti di delega (arch. Bracchi). Essi segnalano il tutto al soggetto incaricato responsabile di sede che procederà come da punto 1;
3. Al modulo di richiesta va allegato preventivo (a meno che ciò non sia necessario);
4. Nel compilare il modulo il soggetto incaricato farà esclusivamente riferimento ad un paniere di fornitori preventivamente selezionato dall'Amministrazione - partner ufficiali);
5. nel caso di importi > 500 € deve essere allegato il relativo preventivo di spesa;
6. Il soggetto incaricato mette la data e sottoscrive il modulo;
7. Il responsabile delle manutenzioni - Valentino Ungaro - raccoglie i moduli di richiesta corredati di eventuali allegati (preventivi), ne controlla la correttezza formale e autorizza la spesa sottoscrivendoil modulo a sua volta.
8. I documenti in originale vanno poi consegnati in Amministrazione all'ufficio acquisti a cura del responsabile delle manutenzioni;
9. Per eventuali urgenze (rotture, guasti etc.) va contattata immediatamente la responsabile di funzione che autorizza in deroga (salvo poi produrre in ogni caso l'ordine di spesa come da punti precedenti).
10. Il responsabile amministrativo controlla il rispetto del budget nel suo complesso;
11. Per il resto procedura identica alla procedura "Area didattica" a partire dal punto 7 e successivi.

Acquisti per uffici

1. Il responsabile dell'ufficio compila apposito modulo di richiesta (in cui è indicato nome del richiedente, prodotto/servizio richiesto, prezzo, sezione del budget cui imputare l'acquisto);
2. Il medesimo responsabile controlla il rispetto del budget annuale sulla base di rendiconto mensile ricevuto dall'ufficio amministrazione;
3. Al modulo di richiesta va allegato preventivo (a meno che ciò non sia necessario);
4. Nel compilare il modulo il responsabile di dipartimento farà esclusivamente riferimento ad un paniere di fornitori preventivamente selezionato dall'Amministrazione - partner ufficiali)
5. Il responsabile di dipartimento mette la data e sottoscrive il modulo;
6. Il modulo va poi validato dal direttore/vice direttore che controlla la conformità dell'ordine al budgete alle necessità dell'Accademia;
7. Per eventuali urgenze (non ve ne dovrebbero essere) va contattata immediatamente Roberta che autorizza in deroga (salvo poi produrre in ogni caso l'ordine di spesa come da punti precedenti);
8. Per il resto procedura identica alla procedura "Area didattica" a partire dal punto 7 e successivi.

Acquisti beni di investimento

Come da deleghe conferite agli amministratori con Cda del 21/10/2019 il PresidenteGianluca Delbarba e gli amministratori delegati Emanuela Zanchetta e Luigi Bracchi hanno potere di autorizzazione disgiunto fino all'importo di Euro 20.000, oltre tale importo è necessaria delibera del Consiglio di Amministrazione.

In ogni caso la procedura è la seguente:

1. Se l'investimento non è ricompreso nei budget annuali di cui ai punti precedenti e sono inferiori ad € 5.000 + IVA vengono autorizzati disgiuntamente da Delbarba o Zanchetta;
2. Nel caso di beni/servizi di valore unitario singolarmente < 5.000 + IVA € ma che si riferiscono ad un unico "progetto" che supera i 5.000 + IVA € è necessaria un'apposita delibera autorizzativa del Cda;
3. Nel caso di beni/servizi di importo superiore a 5.000 + IVA € la spesa deve essere autorizzata dal Cda previa raccolta di idonea documentazione (preventivi, valutazioni di merito etc);
4. Se l'importo della spesa supera i 20.000 € (IVA compresa) essa va autorizzata dal Cda previa idonea istruttoria e relazione in Cda da parte dell'amministratore proponente l'investimento con allegati preventivi e budget economico/finanziario della società aggiornato);
5. Se il progetto approvato è di particolare importanza e complessità (es. fornitura di materialeinformatico su larga scala, ristrutturazione complessa di un immobile etc) il Cda nominerà un "responsabile dei lavori" che può essere un amministratore o un soggetto terzo;

6. Una volta deliberato l'amministratore delegato o a ciò autorizzato dal Cda sottoscrive l'ordine o il contratto di fornitura;
7. Copia del contratto o del preventivo sottoscritto dall'amministratore va consegnato all'ufficio acquisti;
8. Il responsabile amministrativo ha facoltà di aprire nuovo centro di costo in contabilità generale per meglio gestire le spese riferitesi ad un progetto di particolare importanza e spesa;
9. Copia della delibera del Cda e/o della documentazione necessaria, viene trasmessa all'Ufficio acquisti che procede con i vari ordini, eventualmente assistita dal "responsabile dei lavori" nominato al punto 5;
10. Il responsabile dei lavori o, se non nominato, l'ufficio acquisti, controlla la regolare esecuzione dei lavori verificando che le DDT, le fatture accompagnatorie corrispondano a quanto ordinato;
11. I documenti in originale vanno poi consegnati in Amministrazione al responsabile amministrativo;
12. Il responsabile amministrativo aggiorna il budget di spesa autorizzato dal cda e verifica la correttezza della documentazione contabile;

NOTE:

- Poiché in genere gli importi della spesa sono elevati sono necessarie congrue tempistiche per approntare la documentazione necessaria per decidere gli investimenti, non possono esserci urgenze in tale campo. Gli investimenti vanno pianificati.

PROCEDURA VENDITE

- **Fatture vendite (ufficio amministrativo)**

➢ Contratti di servizi con terzi (enti pubblici e/o privati), contratti di service, riaddebito spese, royalty.

- **Generazione fattura elettronica (ufficio amministrativo)**

➢ Generazione della fattura elettronica in uscita con relativo invio, stampa cartacea e salvataggio in PDF.

- **Download certificato di trasmissione**

- **Inserimento contabile (ufficio amministrativo)**

➢ Inserimento nel gestionale di contabilità e assegnazione del relativo conto economico come da piano dei conti

- **Check mensile di verifica (responsabile amministrativa)**

- Verifica mensile della correttezza di tutte le registrazioni in contabilità

PARTE SPECIALE

“G”

Reati informatici

L'articolo 7 della legge 18 marzo 2008 n. 48, recante "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica", ha introdotto nel Decreto l'articolo 24-*bis* rubricato "*Delitti informatici ed illecito trattamento dei dati*".

A. REATI CHE INCIDONO SUI SISTEMI INFORMATICI O TELEMATICI

Articolo *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 è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

****

Considerazioni specifiche

Si tratta di un reato comune, che può essere compiuto da chiunque, ed istantaneo, perché si consuma nel momento dell'introduzione o nella protrazione all'interno del sistema nonostante il dissenso del titolare. Le misure di sicurezza (a cui fa riferimento la norma) da cui è protetto il sistema sono sia le c.d. misure logiche (ad esempio *password*) che le c.d. misure fisiche (armadi chiusi, locali non accessibili a tutti, servizi di controllo e vigilanza). Il reato punisce due diverse condotte: l'introduzione abusiva nel sistema protetto e il mantenersi nello stesso contro la volontà del titolare. A quest'ultimo proposito, va sottolineato che il reato, come ritenuto dalla giurisprudenza, può essere commesso anche da chi, autorizzato all'accesso al sistema per una determinata finalità, non rispetti le condizioni a cui era subordinato l'accesso e lo utilizzi per finalità diverse, abusando dell'autorizzazione concessa.

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

****

Considerazioni specifiche

Il reato può essere commesso con qualsiasi mezzo che sia idoneo a superare la protezione di un sistema informatico (password, codici di accesso o, semplicemente, informazioni che consentano di eludere le misure di protezione). Il possesso abusivo di tali mezzi comporta il pericolo della commissione di un accesso abusivo ad un sistema o della diffusione di tali codici ad altre persone che a loro volta potrebbero accedere abusivamente ad un sistema.

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 euro 10.329.

****

Considerazioni specifiche

Oggetto di tutela sono non solo i 'programmi informatici' ma anche le 'apparecchiature' ed i 'dispositivi'. Dunque, la norma include non solo i *softwares* ma anche l'*hardware*. L'elemento soggettivo è il dolo specifico: il fatto è punibile soltanto laddove sia commesso allo scopo indicato nell'articolo stesso. È un reato comune, che può essere commesso da chiunque.

B. DANNEGGIAMENTO INFORMATICO

B.1. DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI

Art. 635-*bis* del codice penale – Danneggiamento di informazioni, dati e programmi informatici

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

****

Considerazioni specifiche

Si tratta di un reato di evento. Tutte le ipotesi di danneggiamento saranno da considerarsi aggravate: *(I)* quando il danneggiamento è commesso con violenza alla persona o minaccia; *(II)* quando il fatto sia commesso con abuso della qualità di operatore del sistema.

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 la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

****

Considerazioni specifiche

Si tratta di un reato aggravato dall'evento, per cui il fatto sussiste anche in assenza di qualunque effettivo deterioramento o soppressione dei dati, pur essendo necessaria l'idoneità dell'azione a produrre detti effetti.

Le circostanze aggravanti sono le stesse indicate per il reato di cui all'articolo 635-*bis*.

B.2. DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI

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'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge,

danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

****

Considerazioni specifiche

Si tratta di un reato di evento: si richiede espressamente che il sistema venga danneggiato, reso in tutto o in parte inservibile, ovvero ne venga ostacolato gravemente il funzionamento. La fattispecie sarà integrata laddove il danneggiamento del sistema sia cagionato: *(i)* mediante la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi, o *(ii)* mediante l'introduzione o la trasmissione di dati, informazioni o programmi.

La distinzione tra danneggiamento di dati e danneggiamento del sistema è legato alle conseguenze della condotta: quando la soppressione o alterazione di dati, informazioni e programmi renda inutilizzabile o danneggi gravemente il funzionamento del sistema, ricorrerà la fattispecie di cui al presente articolo.

Le circostanze aggravanti sono le stesse indicate per il reato di cui all'articolo 635-*bis* cod. pen.

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 ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

****

Considerazioni specifiche

Si tratta di un reato a consumazione anticipata, che non richiede il verificarsi del danneggiamento, della distruzione o dell'inservibilità, che sono considerate circostanze aggravanti, mentre non è indicato tra le circostanze aggravanti il fatto che il funzionamento del sistema venga gravemente ostacolato.

Al contrario di quanto avviene per il reato di cui all'articolo 635 *ter* cod. pen., non è sufficiente per la sussistenza del reato che i sistemi siano utilizzati dagli enti pubblici, occorrendo che gli stessi siano di pubblica utilità.

C. COMUNICAZIONI INFORMATICHE O TELEMATICHE

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 è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato.

****

Considerazioni specifiche

Il reato, unitamente a quello previsto dal successivo articolo 617-*quinquies*, è volto a tutelare la libertà e la riservatezza delle comunicazioni informatiche, intendendosi per tali qualunque scambio di dati tra due o più sistemi infirmatici. Vi rientrano, quindi, gli scambi di *e-mail*, le *mailing lists*, i *forum*, le *chat*, i *newsgroup*, ecc.

Si può parlare di intercettazione abusiva (fraudolenta) quando la comunicazione è riservata ad un determinato numero di destinatari: per le comunicazioni a carattere pubblico (ad esempio siti web) non è ipotizzabile alcuna riservatezza.

Il reato si verifica quando si prende fraudolentemente cognizione del contenuto di un messaggio in corso di trasmissione. Il reato è escluso se c'è stata autorizzazione esplicita preventiva da parte dei soggetti che partecipano alla comunicazione.

Art. 617-*quinquies* del codice penale – Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

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

****

Considerazioni specifiche

Il reato si verifica si verifica non appena viene fatta cessare, in maniera fraudolenta, una comunicazione in corso. Il reato è escluso se c'è stata autorizzazione esplicita preventiva da parte dei soggetti che partecipano alla comunicazione.

D. FALSITA' INFORMATICA

491-*bis* del codice penale – Documenti Informatici

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

****

Considerazioni specifiche

L'articolo ha esteso alle falsità riguardanti un documento informatico le disposizioni in tema di falso in atto pubblico e falso in scrittura privata.

E. FRODE INFORMATICA

Art. 640-*quinquies* del codice penale – Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

****

Considerazioni specifiche

La frode informatica è già contemplata dall'articolo 640-*quater* del codice penale, che però, per la ricorrenza del reato, richiede alcune condotte che potrebbero non ricorrere nel caso dell'attività di certificazione. La norma introdotta dalla legge 48 del 2008 si potrebbe porre in rapporto di specialità con l'articolo 640 - *quater* ed è incentrata sul necessario fine dell'ingiusto profitto o dell'altrui danno. La condotta incriminata riguarda solo il certificatore c.d. "qualificato", ossia colui che presta servizi di certificazione di firma elettronica qualificata.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** ogni settore della Società dove vengono impiegati strumenti informatici (tutto il personale aziendale).

All'interno delle predette aree, **le operazioni "a rischio**" nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale sono:

- accesso da parte di Soggetti non abilitati e/o autorizzati, ai portali della P.A.;
- alterazione registri informatici della P.A. (es. Agenzia delle Entrate, Anagrafe tributaria, INAIL, ecc.): ad es. per far risultare esistenti condizioni/requisiti, per la successiva produzione di documenti attestanti fatti e circostanze inesistenti, per modificare dati fiscali/previdenziali o reddituali di interesse della Società, ecc.
- messa in condivisione o pubblicazione sul server aziendale di opere protette previo download su reti telematiche.
- installazione sul proprio p.c. di un software antivirus senza acquisto di licenza d'uso
- creazione di keygen per ottenere "chiavi d'accesso"
- modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata.
- download di programmi informatici, attraverso siti web rilevati come potenzialmente pericolosi.
- utilizzo di credenziali di autenticazione per l'accesso ad apparati informatici.

a) immissione di dati, documenti e informazioni nei sistemi informatici aziendali;
b) consultazione *on line* di dati, documenti e informazioni;
c) gestione ed archiviazione di dati, documenti e informazioni in via informatica o telematica;
d) stipulazione e gestione dei contratti con le società installatrici di *software* e con i manutentori dei sistemi.
e) gestione della sicurezza fisica e logica dei sistemi informativi aziendali, in particolare:

gestione dei server aziendali e delle applicazioni in uso c/o la società;

f) gestione della rete telematica
g) manutenzione dei Client assegnati al personale dipendente della Società.
h) gestione e custodia delle credenziali di autenticazione per l'accesso al sistema informatico aziendale e ai portali della P.A.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

In particolare, il titolare della Privacy deve verificare il corretto impiego dei sistemi informatici, delle procedure e chiavi di accesso ed in generale verificare l'assenza di elementi ostativi dettati dalle norme della presente parte speciale.
Inoltre, deve essere verificata l'attendibilità commerciale e professionale dei fornitori e manutentori di software e programmi aziendali.

Dovrà inoltre essere garantita:

- la formazione/informazione del personale;
- la professionalità ed affidabilità degli amministratori di sistema;
- il controllo costante degli interventi effettuati e del rispetto delle misure di sicurezza adottate dalla società.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione dei dati, informazioni e documenti informatici (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano ricostruibili le autorizzazioni all'uso e le responsabilità in materia di codici di accesso, chiavi elettroniche, password e misure di sicurezza in genere;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- siano effettuati i necessari controlli sull'integrità di dati, informazioni e documenti informatici;
- sia impedita la divulgazione e l'appropriazione abusiva di codici di accesso, chiavi elettroniche, password e misure di sicurezza in genere;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione informatica da parte degli organi a ciò deputati;
- siano effettuate con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalle procedure interne, dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale ed adeguate all'evoluzione della tecnologia; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PROCEDURA AREA TECNICA

1. Il Piano di Sicurezza Informatica

1.1. Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dall'Accademia per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati. Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs 196/2003, "Codice in materia di protezione dei dati personali" e del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza". Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo dell'Accademia un adeguato livello di sicurezza.

1.2. Obbiettivi

Scopo del presente documento è descrivere la strategia che l'Accademia intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- *Confidenzialità*: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.
- *Integrità*: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).

- *Disponibilità*: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.
- *Accountability (Tracciabilità)*: tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento. Il Piano per la sicurezza informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice dell'Accademia.

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

1.3. Responsabilità (figure coinvolte)

L'Ente predispone il Piano per la sicurezza informatica ai sensi dell'art.12 del DPCM 13 novembre 2014. Tale piano risulta essere comprensivo del Piano per la sicurezza informatica dei documenti di cui all'art. 4 del DPCM 3 dicembre 2013, relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, predisposto dal Responsabile della gestione documentale nel rispetto del D.Lgs 196/2003 e del relativo Allegato B, d'intesa con il Responsabile del trattamento dei dati personali.

2. Il Sistema Informativo dell'Accademia

2.1. Tipologia di servizi offerti

Il Sistema Informativo dell'Accademia è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze "interne" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza della popolazione residente esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi strettamente Accademici, oppure tramite un sistema esterno, reso disponibile da altri enti e all'Accademia stessa accessibile con le opportune modalità.

2.2. Servizio Informativo

2.2.1. Organizzazione

Nel contesto del Sistema Informativo ogni utente dell'Accademia deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia di Utenti	Compiti/Responsabilità	Note
Addetti Assistenza Informatica Esterna	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, ecc.). Verifiche sull'attuazione delle politiche.	
Dipendenti della Segreteria	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati.	Si faccia riferimento al mansionario specifico.
Responsabili	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati. Vigilanza sul comportamento dei dipendenti e degli addetti esterni.	Si faccia riferimento ad Organigramma
Amministratore di Rete Amministratore di Sistema	Verifica su attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche. Verifica su politiche di sicurezza informatiche, fisiche e sociali. Reporting e certificazione regolari sullo stato della struttura	Andrea Gianfreda

2.2.2. Addetti

Nel contesto del Sistema Informativo ogni dipendente dell'Accademia è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto

concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica è incaricata una figura interna con la consulenza di una società esterna specializzata in tale settore, la quale svolge anche attività di assistenza hardware e software.

2.3. Infrastruttura Tecnologica

2.3.1. Generalità

L'Infrastruttura Tecnologica dell'Accademia può essere schematizzata come segue:

Tipologia di Apparati	Descrizione
Apparati Server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà dell'Accademia o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso il locale CED del distaccamento di Via Cefalonia 58 – Brescia (BS).
Apparati Server esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società esterne o da Enti esterni (MIUR, etc), in virtù di contratti stipulati con l'Accademia.
Apparati di rete	Indichiamo in questa categoria tutti gli apparati (router, switch, hub, …) che concorrono alla connettività fra le sedi dell'Accademia (connettività interna), da e verso Internet (connettività pubblica verso l'esterno).
Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli apparati che concorrono specificatamente alla sicurezza (storage per backup, apparati firewall).
Infrastruttura di comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano, per ogni sede, la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet.
Apparati client	In questa categoria raggruppiamo tutti gli apparati (PC, Portatili, …) utilizzati dall'utenza interna per l'utilizzo dalle sedi territoriali o in connettività mobile dei servizi dell'Accademia

2.3.2. Struttura Fisica

Il sistema informatico dell'Accademia è così costituito:

- Server SRV-DC1 - Windows Server 2019 – con funzioni di Domain Controller Primario
- Server SRV-DC2 - Windows Server 2019 – con funzioni di Domain Controller di Backup
- Server SHARE - Windows Server 2019 – con funzioni di File Server
- Server Gestionale – Windows Server 2012 – con funzioni di service provider per l'uso del gestionale interno e deposito della relativa banca dati
- Server Business – Windows Server 2019 – con funzione di service provider per l'uso del gestionale Amministrativo e deposito della relativa banca dati
- Server Management – Windows Server 2016 – con funzioni di management dei precedenti
- NAS di rete utilizzato come unità di storage per tutti i dati cartacei relativi alla didattica (come dispense, programmi ecc.)
- NAS di rete utilizzato come unità di backup per il precedente
- Server "Microsoft" esterno utilizzato per la gestione del dominio, del servizio di posta elettronica e di una serie di applicazioni rivolte al personale interno.

Nel locale CED situato nel distaccamento di Via Cefalonia sono presenti le macchine fisiche:

- Dell PowerEdge R640 – 10 x Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz – 64GB RAM -1TB HDD – 256GB SSD
- Dell PowerEdge R430 – 8 x Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz – 48GB RAM - 3TB HDD
- Dell – Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz – 16GB RAM - 2TB HDD

Le sedi dell'Accademia sono poi dotate di due connettività al fine di garantire la navigazione Extranet ed Intranet dei loro utenti. Le connessioni ricadono sotto le seguenti categorie:

- FTTH (Fiber To The Home) 100: rappresenta la connettività backbone dedicata alle VPN, alla navigazione e in generale ogni operazione svolta dagli uffici.
- FFTC (Fiber To The Cabinet) 100/20: rappresenta la connettività di riserva dedicata principalmente alla navigazione degli studenti e dei docenti.

2.3.3. Architettura Applicativa

Nel presente paragrafo descriviamo i principali software applicativi ed utilità in uso presso l'Accademia esplicitandone le caratteristiche salienti. Dal punto di vista della architettura applicativa possiamo distinguere le seguenti categorie:

- Software centralizzati: trattasi di applicativi in uso a livello di Accademia, installati in unica posizione, su server presso la sede, o in uno degli ambienti virtuali disponibili, oppure resi disponibili da enti esterni e usufruibili dall'Accademia via Web. Quasi sempre la architettura elaborativa è a 3 livelli, composta da un database server, da un

application (e web) server con accesso dei client via Web tramite la Intranet ed Extranet dell'Accademia.
- Software stand-alone: in questa categoria intendiamo software installati localmente sulle postazioni di lavoro, essenzialmente ai fini della produttività personale.

2.3.4. Sistema di Conservazione

I dati trattati dall'Accademia sono salvati e protetti come indicato nell'apposita sezione del GDPR Aziendale. Le tipologie di dati possono essere così riassunte:

- Dati Anagrafici e Accademici: le informazioni anagrafiche dei soggetti che transitano in LABA, così come le informazioni relative alla loro carriera Accademica, vengono salvate all'interno di un Database SQL interrogato dal software Gestionale interno.
- Dati Economico-Amministrativi: le informazioni di carattere economico-amministrativo, come dati anagrafici, coordinate bancarie, situazione contabile ecc. degli studenti e dei fornitori LABA sono salvate all'interno di un Database SQL interrogato dal software Business Cube.
- Le mail istituzionali di studenti, docenti e personale interno e avanti dominio laba.edu, vengono interamente gestite dai server esterni di Microsoft Office 365.
- Il materiale realizzato dagli studenti (e raccolto dai Docenti durante l'anno accademico) viene salvato e conservato nell'archivio OneDrive di un account istituzionale dedicato.
- Le registrazioni delle lezioni vengono salvate, se d'accordo con il Docente relatore, nell'account Steam del registrante o all'interno del canale relativo alla materia del Docente stesso.

3. Politiche Organizzative della Sicurezza

3.1. Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno dell'Accademia richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo. L'applicazione delle politiche di sicurezza all'interno dell'Accademia richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.

Attualmente, l'individuazione della politica di sicurezza determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1. Backup

I dati, in qualunque modo elaborati dai sistemi informatici dell'Accademia, sono salvati nella memoria centrale del Server Microsoft Windows 2019. Al fine di salvaguardarne l'integrità è stato attivato un sistema di duplicazione e memorizzazione giornaliero dei dati informatici che effettua il backup delle macchine virtuali ove sono salvati tali dati. Per ridurre ancor più la probabilità di eventuali disservizi il piano di disaster recovery prevede che questa copia abbia carattere ridondante e venga distribuita sui due NAS di rete a disposizione; ad oggi non è pianificato un backup dei dati in Cloud ma non se ne esclude la possibilità di una prossima implementazione.

3.2. Sicurezza Logica

3.2.1. Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi, in modo tale da garantirne la fruibilità nel tempo, che deve essere al contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2. Sistema di Autenticazione

La credenziale di autenticazione consiste in un indirizzo e-mail atto all'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo.

Le credenziali di autenticazione sono affidate al controllo del Server Microsoft Windows 2019 che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di Microsoft Active Directory ("insieme di servizi di rete - account utente, account computer, cartelle condivise, stampanti, etc. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei client") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione).

Tramite tecnologia SSO (Single Sign-On) tali credenziali verranno poi utilizzate per unificare gli accessi degli utenti ai vari servizi messi a disposizione dell'Accademia come la navigazione wi-fi all'interno degli spazi condivisi, l'ingresso ai servizi Microsoft O365 e al nuovo gestionale di prossima implementazione.

Ad integrare la protezione sul sistema informativo, i software dell'Accademia e gli applicativi web sono dotati di apposite procedure di accesso tramite username ("nome con il quale l'utente viene riconosciuto da un computer, da un programma o da un server") e password ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo username è un identificativo che, insieme alla password, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.3. Antivirus e Similari

Il sistema informatico dell'Accademia e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-quinquies del Codice Penale ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"), mediante l'attivazione:

- ***software antivirus*** stand-alone installato sui singoli elaboratori. La posta elettronica è invece protetta mediante l'antivirus integrato nel Server di posta elettronica di Microsoft O365 ("software atto a rilevare ed eliminare virus informatici o altri programmi dannosi");
- ***software antispyware*** installato sui singoli elaboratori ("programma il cui scopo è quello di cercare ed eliminare dal sistema, tramite un'apposita scansione, i software che raccolgono informazioni riguardanti l'attività on-line di un utente - siti visitati, acquisti eseguiti in rete etc. - senza il suo consenso per farne un uso illegittimo");
- ***software antispam*** integrato nel Server di posta elettronica di Microsoft O365 ("software che individua messaggi di posta elettronica indesiderati generalmente commerciali e/o pubblicitari").

I sistemi operativi degli elaboratori e dei Server sono periodicamente aggiornati automaticamente mediante Windows Update con le opportune patch di sicurezza ("programma o parte di programma che aggiorna e corregge un software"). Regolarmente e costantemente il Responsabile aggiorna, vigila e controlla.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

Al fine di prevenire intrusioni dall'esterno è stato installato e configurato un firewall hardware e su ciascun elaboratore è stato attivato il firewall software integrato nel sistema operativo "Microsoft Windows". Periodicamente sono stati eseguiti e verranno effettuati, nei tempi previsti dalla normativa, gli aggiornamenti sui sistemi di protezione.

4. Documenti e Banche Dati

4.1. Sistema di Gestione Informatica dei Documenti

Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti". Tale sistema è attivato dall'Istituto su tutte le postazioni di lavoro degli uffici afferenti all'AOO e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili individuati all'interno dell'AOO (Responsabile della gestione documentale, Responsabile dei sistemi informativi).

Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'Accademia si faccia riferimento alle indicazioni contenute nel GDPR Aziendale, così come anche per i seguenti argomenti:

- Protocollo informatico
- Formazione dei documenti
- Formati adottati
- Sottoscrizioni
- Validazione temporale
- Metadati
- Trasmissione dei documenti
- Conservazione

5. Trattamento dei Dati Personali – Analisi e Gestione dei Rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando al GDPR Aziendale.

5.1. Gestione dei Rischi

Al fine di minimizzare i rischi di corruzione, perdita, alterazione, furto dei dati, l'Istituto adotta le seguenti politiche di sicurezza.

5.1.1. Configurazione dei Sistemi

I sistemi in utilizzo sulla rete sono installati in configurazioni standard con software di comprovata stabilità e sicurezza. Il personale dipendente dell'Accademia è informato sui rischi dovuti all'installazione e all'utilizzo di software non conformi alle politiche di sicurezza o quantomeno non sufficientemente testati. Il Responsabile che materialmente esegue le installazioni dei sistemi provvede a disattivare tutti i servizi non necessari e a chiudere le porte TCP/UDP non necessarie al corretto funzionamento degli applicativi.

5.1.2. Sicurezza

L'Amministratore di rete certifica di essere:

- abbonato a servizi offline/online in materia di sicurezza informatica e a servizi offline/online di alert in materia di cyberattacchi, sicurezza informatica, virus
- in possesso delle certificazioni che gli consentono di operare sui software applicativi in uso nella rete LAN senza invalidarne le garanzie dei produttori

PARTE SPECIALE

“H”

Violazione del diritto d’autore

L'articolo 15, c. 7, della legge 23 luglio 2009 n. 99, recante "*Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*", ha introdotto l'articolo 25 *novies*, rubricato "Delitti in materia di violazione del diritto d'autore".

Si tratta, in particolare, dei seguenti reati:

Art. 171 legge 633/1941 – Messa a disposizione del pubblico, in un sistema di reti telematiche, di un'opera dell'ingegno protetta o di parte di essa.

Comma 1 lett. a) *bis*
Salvo quanto previsto dall'art. 171-bis e dall'art. 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:
omissis
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;

Comma 3
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 un'opera altrui non destinata alla pubblicazione, 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.

****

Art. 171-*bis* legge 633/1941

1. 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.

2. 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.

****

Considerazioni specifiche

Il bene giuridico protetto riguarda gli interessi patrimoniali dei titolari del diritto di sfruttamento economico del *software*. Costituisce reato la condotta di abusiva duplicazione di programmi anche in assenza di una finalità di natura patrimoniale. È configurabile il reato di cui alla norma ogniqualvolta i programmi informatici illegalmente detenuti abbiano concretamente favorito l'attività imprenditoriale esercitata dall'autore del fatto, venendo impiegati per attività funzionali all'impresa, come l'archiviazione dei dati relativi ai fornitori o ai clienti, l'elencazione delle scadenze contabili o la gestione delle fatturazioni. L'indicazione del comportamento vietato viene operata dall'articolo facendo riferimento ai vari diritti di utilizzazione economica dell'opera dell'ingegno.

Art. 171-*ter* legge 633/1941

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a

disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti commessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

****

Art. 171-*septies* legge 633/1941

La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

****

Art. 171-*octies* legge 633/1941

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove,

installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

****

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** ogni settore della Società dove vengono impiegati strumenti informatici (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano in generale l'utilizzo del sistema informatico.
Il rischio, in questo caso, potrebbe essere rappresentato dall'utilizzo abusivo di programmi informatici, anche per uso endo aziendale, senza acquisto della relativa licenza.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono:

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le

norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.

- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.
- I Destinatari interessati devono inoltre assicurarsi che nei contratti di acquisto di prodotti interessati da un diritto di proprietà industriale altrui sia prevista la licenza di utilizzo di tali diritti di proprietà industriale.

Dovrà inoltre essere garantita:

- la formazione specifica del personale delle aree interessate in materia di proprietà industriale, mirata a rendere consapevoli i destinatari riguardo ai problemi giuridici connessi alla gestione dei relativi diritti;
- la definizione di regole relative alla promozione dei prodotti ed ai rapporti con i concorrenti ed i clienti;
- la sensibilizzazione degli esponenti aziendali circa il corretto utilizzo delle risorse aziendali altrui in tema di proprietà industriale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono:

A. attuare un controllo preventivo e continuativo delle attività connesse con, o che implicano, l'utilizzo di diritti di proprietà industriale di terzi;
B. effettuare i necessari controlli sui contratti di cessione o licenza di diritti di proprietà industriale di terzi nonché sui procedimenti e/o i prodotti su cui esiste un diritto di proprietà industriale di terzi;
C. mantenere una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
D. segnalare tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolare ogni forma di controllo da parte di quest'ultimo;
E. garantire la costante formazione ed aggiornamento del personale dipendente e dei collaboratori esterni (agenti, collaboratori, ecc.) che operano nelle aree aziendali a rischio per i reati di cui alla presente parte speciale;

F. non porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione informatica da parte degli organi a ciò deputati;
G. effettuare con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalle procedure interne, dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.

Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"I"

Reati di criminalità organizzata

L'articolo 2, comma 29, della legge 15 luglio 2009 n. 94, recante "*Disposizioni in materia di sicurezza pubblica*", ha introdotto nel Decreto l'articolo 24-*ter*, rubricato "Delitti in materia di criminalità organizzata".

Si tratta, in particolare, dei seguenti reati:

Art. 416, 6° comma - Associazione per delinquere

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602*, nonché all'*articolo 12, *comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al* decreto legislativo 25 luglio 1998, n. 286, *si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.*

Art. 416-*bis* del codice penale – Associazione di tipo mafioso

Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni.

Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma.

L'associazione si considera armata quanto i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.

Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

**articolo così modificato dall'articolo 5 della legge 69 del 27 maggio 2015.*

****

Considerazioni specifiche

Come già evidenziato nella predetta parte speciale, attraverso lo strumento del reato associativo vi è il concreto rischio che alcune fattispecie illecite finora escluse dal novero di quelle considerate dal Decreto possano rientrare in questo ambito.

Art. 416-*ter* del codice penale - Scambio elettorale politico-mafioso

La pena stabilita dal primo comma dell'articolo 416-bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416-bis in cambio della erogazione di denaro.

****

Considerazioni specifiche

Vista l'attività della Società, si tratta di reato ben difficilmente configurabile in seno alla stessa.

Art. 630 del codice penale - Sequestro di persona a scopo di rapina o di estorsione

Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da venticinque a trenta anni.

Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta.

Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.

Al concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà, senza che tale risultato sia conseguenza del prezzo della liberazione, si applicano le pene previste dall'articolo 605. Se tuttavia il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da sei a quindici anni.

Nei confronti del concorrente che, dissociandosi dagli altri, si adopera, al di fuori del caso previsto dal comma precedente, per evitare che l'attività delittuosa sia portata a conseguenze ulteriori ovvero aiuta concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di prove decisive per l'individuazione o la cattura dei concorrenti, la pena dell'ergastolo è sostituita da quella della reclusione da dodici a venti anni e le altre pene sono diminuite da un terzo a due terzi.

Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma.

I limiti di pena preveduti nel comma precedente possono essere superati allorché ricorrono le circostanze attenuanti di cui al quinto comma del presente articolo

Considerazioni specifiche

Si tratta di reato ben difficilmente configurabile in seno alla Società.

Art. 74 DPR 9 ottobre 1990, n. 309 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope.

Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 70, commi 4, 6 e 10, escluse le operazioni relative alle sostanze di cui alla categoria III dell'allegato I al regolamento (CE) n. 273/2004 e dell'allegato al regolamento n. 111/2005, ovvero dall'articolo 73, chi promuove, costituisce, dirige, organizza o finanzia l'associazione è punito per ciò solo con la reclusione non inferiore a venti anni.

Chi partecipa all'associazione è punito con la reclusione non inferiore a dieci anni.

La pena è aumentata se il numero degli associati è di dieci o più o se tra i partecipanti vi sono persone dedite all'uso di sostanze stupefacenti o psicotrope.

Se l'associazione è armata la pena, nei casi indicati dai commi 1 e 3, non può essere inferiore a ventiquattro anni di reclusione e, nel caso previsto dal comma 2, a dodici anni di reclusione. L'associazione si considera armata quando i partecipanti hanno la disponibilità di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

La pena è aumentata se ricorre la circostanza di cui alla lettera e) del comma 1 dell'articolo 80.

Se l'associazione è costituita per commettere i fatti descritti dal comma 5 dell'articolo 73, si applicano il primo e il secondo comma dell'articolo 416 del codice penale.

Le pene previste dai commi da 1 a 6 sono diminuite dalla metà a due terzi per chi si sia efficacemente adoperato per assicurare le prove del reato o per sottrarre all'associazione risorse decisive per la commissione dei delitti.

Quando in leggi e decreti è richiamato il reato previsto dall'articolo 75 della legge 22 dicembre 1975, n. 685, abrogato dall'articolo 38, comma 1, della legge 26 giugno 1990, n. 162, il richiamo si intende riferito al presente articolo.

****

Considerazioni specifiche

Si tratta di reato ben difficilmente configurabile in seno alla Società, presupponendo, come è stato sottolineato dalla giurisprudenza, la presenza di tre elementi fondamentali: *(I)* l'esistenza di un gruppo, i membri del quale siano aggregati consapevolmente per il compimento di una serie indeterminata di reati in materia di stupefacenti; *(II)* l'organizzazione di attività personali e di beni economici per il perseguimento del fine illecito comune, con l'assunzione dell'impegno di apportarli anche in futuro per attuare il piano permanente criminoso; *(III)* sotto il profilo soggettivo, l'apporto individuale apprezzabile e non episodico di almeno tre associati, che integri un contributo alla stabilità dell'unione illecita.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come aree "a rischio" ogni settore della Società (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano, in generale, la gestione delle attività sensibili riportate nell'analisi dei rischi per le quali sono previste ipotesi di reato qualificabili come delitti in forma associativa.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.
Per ciascuna delle aree a rischio sopra individuate, i Destinatari devono assicurarsi che:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;

- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia garantito, anche da parte dei subappaltatori e dei terzi in genere che espletino servizi o producano beni per conto della Società, il rispetto della normativa vigente in materia di immigrazione e di lavoro, ivi incluso per ciò che attiene al profilo della costituzione del rapporto lavorativo;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non giustificati in relazione al tipo di incarico effettuato ed alla prassi ed alle eventuali tariffe vigenti;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati;
- siano effettuate con tempestività, regolarità, correttezza e buona fede tutte le comunicazioni, le segnalazioni periodiche e gli invii di documenti, informazioni e dati previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza o richiesti dalle stesse, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza dalle medesime esercitate e prestando la massima collaborazione all'espletamento degli accertamenti.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale; pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure adottate, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente l'Organismo di Vigilanza della deroga attuata.
Sono fatte salve le procedure di maggior tutela eventualmente già vigenti a livello az

PARTE SPECIALE

"L"

Delitti di impiego di lavoratori stranieri irregolari

L'articolo 2 del D.lgs. 16 luglio 2012, n. 109 (recante "*Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare*") ha introdotto nel Decreto l'articolo 25-*duodecies*, rubricato "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*". Si tratta delle ipotesi aggravanti del reato di cui all'articolo 12 del D.lgs. 286/1998, relativo all'impiego di lavoratori stranieri irregolari, ipotesi aggravanti che ricorrono:

- se i lavoratori occupati sono in numero superiore a tre;
- se i minori occupati sono minori in età non lavorativa;
- se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-*bis* del codice penale.

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** le seguenti aree:

A. Consiglio di Amministrazione
B. Ufficio personale (relativamente all'individuazione e selezione dei lavoratori ed alla stipula dei successivi contratti nonché alla gestione del rapporto di lavoro).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale sono:

i) selezione ed assunzione di personale;
j) verifica iniziale e periodica della documentazione di lavoratori stranieri (regolare possesso e validità da parte del lavoratore straniero di regolare permesso di soggiorno);
k) implementazione delle procedure autorizzative connesse al rapporto di lavoro.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.

- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

In particolare, l'Ufficio personale deve selezionare ed assumere esclusivamente personale in regola con la normativa in materia di immigrazione e deve altresì controllare la regolarità della documentazione presentata dai dipendenti e collaboratori da assumere, con particolare riferimento al possesso di un regolare e valido permesso di soggiorno.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.

In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.

Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"M"

Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali

L'articolo 25-quater del D. Lgs. 231/2001 non richiama specificatamente una serie di reati, bensì fa un generico riferimento ai "Delitti con finalità di terrorismo o di eversione dell'ordine democratico" previsti dal codice penale e dalle leggi speciali, nonché all'articolo 2 della Convenzione Internazionale del terrorismo fatta a New York il 9 dicembre 1999.

Di seguito quanto riportato dall' art. 2 della Convenzione Internazionale:

1. Commette reato ai sensi della presente Convenzione ogni persona che, con qualsiasi mezzo, direttamente o indirettamente, illecitamente e deliberatamente fornisce o raccoglie fondi nell'intento di vederli utilizzati, o sapendo che saranno utilizzati, in tutto o in parte, al fine di commettere: a) un atto che costituisce reato ai sensi e secondo la definizione di uno dei trattati enumerati nell'allegato; b) ogni altro atto destinato ad uccidere o a ferire gravemente un civile o ogni altra persona che non partecipa direttamente alle ostilità in una situazione di conflitto armato quando, per sua natura o contesto, tale atto sia finalizzato ad intimidire una popolazione o a costringere un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere, un atto qualsiasi.
3. Affinché un atto costituisca reato ai sensi del paragrafo 1, non occorre che i fondi siano stati effettivamente utilizzati per commettere un reato di cui ai commi a) o b) del paragrafo 1 del presente articolo.
4. Commette altresì reato chiunque tenti di commettere reato ai sensi del paragrafo 1 del presente articolo.
I trattati richiamati dall'articolo sono numerosi e fanno riferimento a diverse convenzioni internazionali aventi l'obiettivo di reprimere gli atti di terrorismo. (A titolo esemplificativo si riportano: Protocollo per la repressione di atti illeciti diretti contro la sicurezza delle installazioni fisse sulla piattaforma continentale - Roma, 10 marzo 1988, Convenzione internazionale per la repressione degli attentati terroristici con esplosivo, adottata dall'Assemblea generale delle Nazioni Unite il 15 dicembre 1997, ecc.).

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio**" le seguenti aree:

C. Consiglio di Amministrazione
D. Direzione amministrativa
E. Ufficio personale

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale sono :

- Procedure di assunzione : selezione/assunzione personale, verifica preliminare sui requisiti del candidato.

- Procedure di gestione utenza : corretto adempimento degli obblighi in materia di antiterrorismo previsti dalla normativa vigente.

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.
- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- La Società garantisce la conformità dell'operatività alle disposizioni vigenti in materia di antiterrorismo/antiriciclaggio, avvalendosi di specifici applicativi in grado di consultare le basi dati dei nominativi sospetti di finanziamento al terrorismo.
- Gli uffici preposti, in conformità alle vigenti prescrizioni di legge ed al ruolo rivestito nei rapporti con i fornitori e/o clienti, approntano e consultano le liste antiterrorismo predisposte dagli organismi ufficiali.

- La Società garantisce controlli automatici sui nominativi sospetti di terrorismo e provenienti da Paesi con cui è vietato dalla normativa operare (Black List).
- siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;
- non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.
In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.
Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.

PARTE SPECIALE

"N"

Delitti contro la personalità individuale

L'art. 5 della Legge 11 agosto 2003, n. 228 ha introdotto, nel corpo del D. Lgs. 231/2001 (di seguito, 'Decreto'), l'art. 25-quinquies, il quale prevede la responsabilità degli enti per i delitti contro la personalità individuale, commessi dai propri soggetti apicali o subordinati nell'interesse e/o vantaggio della società stessa. Segnatamente, l'articolo in questione prevede:

"In relazione alla commissione dei delitti previsti dalla sezione I del capo III del titolo XII del libro II del codice penale si applicano all'ente le seguenti sanzioni pecuniarie:

a) per i delitti di cui agli articoli 600, 601 e 602, la sanzione pecuniaria da quattrocento a mille quote;

b) per i delitti di cui agli articoli 600-bis, primo comma, 600-ter, primo e secondo comma, anche se relativi al materiale pornografico di cui all'art. 600-quater, 1, e 600-quinquies, la sanzione pecuniaria da trecento a ottocento quote;

c) per i delitti di cui agli articoli 600-bis, secondo comma, 600-ter, terzo e quarto comma, e 600-quater, anche se relativi al materiale pornografico di cui all'art. 600-quater, 1, la sanzione pecuniaria da duecento a settecento quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1, lettere a) e b), si applicano le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non inferiore ad un anno.

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3."

Di seguito vengono riportate la fattispecie incriminatrici richiamate dal Decreto.

Riduzione o mantenimento in schiavitù o in servitù (art. 600, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque eserciti su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduca o mantenga 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. La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta venga attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Prostituzione minorile (art. 600 bis, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque recluti o induca alla prostituzione una persona di età inferiore agli anni diciotto oppure ne favorisca, sfrutti, gestisca, organizzi e controlli la prostituzione ovvero altrimenti ne tragga profitto. Tale norma sanziona, inoltre, chiunque compia atti sessuali con un minore di età

compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi.

Pornografia minorile (art. 600 ter, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, sfruttando minori di anni diciotto, realizzi esibizioni o spettacoli pornografici o produca materiale pornografico ovvero chiunque recluti o induca minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli ne tragga altrimenti profitto. La fattispecie punisce anche chiunque faccia commercio del materiale pornografico e chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisca, divulghi o pubblicizzi il materiale pornografico di cui al primo comma, ovvero distribuisca o divulghi notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto; ovvero chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente ceda ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto. Infine, tale norma sanziona chiunque assista a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto.

Detenzione di materiale pornografico (art. 600 quater, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, al di fuori delle ipotesi previste nell'articolo 600 ter, cod. pen., consapevolmente si procuri o disponga di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto.

Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque organizzi o propagandi viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività.

Tratta di persone (art. 601, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque commetta tratta di persona che si trova nelle condizioni di cui all’articolo 600, cod. pen., ovvero, al fine di commettere i delitti di cui al medesimo articolo, la induca mediante inganno o la costringa mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno. 5

Acquisto e alienazione di schiavi (art. 602, cod. pen.)

Tale ipotesi di reato si configura nei confronti di chiunque, fuori dei casi indicati nell'articolo 601, cod. pen., acquisti o alieni o ceda una persona che si trova in una delle condizioni di cui all'articolo 600, cod. pen. Per quanto attiene ai reati sopra considerati, va tenuto presente che possono essere ritenuti responsabili degli stessi non solo i soggetti che direttamente realizzino le fattispecie criminose, ma anche i soggetti che consapevolmente agevolino, anche solo finanziariamente, la medesima condotta. Di conseguenza, potrebbero rientrare nell'ipotesi di reato sopra considerate, le eventuali erogazioni di risorse economiche in favore di soggetti terzi, effettuate da parte dell'Ente con la consapevolezza che le erogazioni stesse possano essere utilizzate da tali soggetti per finalità criminose

PRINCIPI GENERALI DI COMPORTAMENTO

All'interno della Società sono state individuate come **aree "a rischio"** ogni settore della Società (tutto il personale aziendale).

All'interno delle predette aree, le **operazioni "a rischio"** nelle quali possono essere ipoteticamente commessi i reati di cui alla presente parte speciale riguardano l'utilizzo del sistema informatico (es. rischio di download da siti web classificati come pericolosi e non attinenti all'attività lavorativa aziendale; salvataggio su pc aziendali di materiale pornografico tramite memorie esterne come pen drive).

La presente parte speciale indica le regole di condotta che gli amministratori, i procuratori, i dirigenti, i dipendenti, i collaboratori ed i terzi che abbiano rapporti con la Società e che agiscono nelle "aree" a rischio sopra indicate (i "Destinatari"), devono osservare, al fine di impedire il verificarsi dei reati in questione.

I Destinatari devono :

- Astenersi dal porre in essere, collaborare o dare causa a comportamenti che integrino le fattispecie di reato sopra considerate o che, pur non costituendo di per sé dette fattispecie di reato, possano potenzialmente diventarlo.
- Qualora vengano a conoscenza di operazioni sospette o movimenti da segnalare, i Destinatari devono darne tempestiva notizia all'Organismo di Vigilanza e trasmettere allo stesso ogni documentazione pertinente.
- I documenti riguardanti l'attività d'impresa nelle suddette aree a rischio dovranno essere conservati a cura della funzione competente con modalità tali da non poter essere modificati, se non con apposita

evidenza, e l'accesso agli stessi potrà essere consentito solamente al soggetto competente, secondo le norme aziendali interne, o ad un suo delegato, nonché all'Organismo di Vigilanza ed al Collegio Sindacale.

- I Destinatari devono rendere edotti i terzi, che a vario titolo entrano in contatto con la Società, delle misure adottate per la prevenzione dei reati di cui alla presente parte speciale.

La documentazione raccolta deve essere conservata agli atti per eventuali controlli da parte dell'Organismo di Vigilanza.

Per ciascuna delle aree a rischio sopra individuate i Destinatari devono attenersi a specifiche procedure, in forza delle quali:

- Siano utilizzati strumenti informatici costantemente aggiornati ed elaborati da reputate imprese del settore che impediscano l'accesso e/o ricezione di materiale relativo alla pornografia minorile (strumenti di "content filtering");
- Nel rispetto delle normative vigenti, siano svolti periodici controlli volti ad impedire l'abuso dei sistemi informativi aziendali o la commissione di reati attraverso il loro utilizzo;
- Siano effettuati richiami netti e inequivocabili volti al corretto uso degli strumenti informatici in possesso dei dipendenti;
- Sia svolta una attenta valutazione di possibili partnership commerciali con società operanti in settori quali la comunicazione telematica di materiale relativo alla pornografia minorile e il turismo nelle aree geografiche richiamate al punto precedente;
- Siano ricostruibili la formazione degli atti (attraverso la tracciatura dei singoli passaggi e l'identificazione dei soggetti che partecipano agli stessi) ed i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- Siano effettuati i necessari controlli sull'assenza di circostanze ostative in relazione alle fattispecie dei reati della presente parte speciale;
- Sia mantenuta una condotta trasparente e collaborativa con le Pubbliche Autorità, in particolare con la magistratura inquirente e giudicante, mediante la comunicazione di tutti i dati, le informazioni e le notizie che fossero richieste, nel rispetto della normativa in materia di protezione dei dati personali;
- Siano segnalate tempestivamente all'Organismo di Vigilanza eventuali situazioni anomale ed agevolata ogni forma di controllo da parte di quest'ultimo;

- Non siano posti in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, le funzioni di controllo della gestione sociale da parte degli organi a ciò deputati.

L'Organismo di Vigilanza di LABA curerà che le procedure attuate siano idonee al rispetto delle prescrizioni della presente parte speciale e, pertanto, ove necessario, proporrà le modifiche e le integrazioni delle prescrizioni stesse e delle relative procedure di attuazione.
In caso di particolare urgenza nella formazione e nell'attuazione delle decisioni o in caso di temporanea impossibilità di osservare le procedure suddette, sono ammesse eventuali deroghe alle procedure stesse, sotto la piena responsabilità di chi le pone in essere e salvo, comunque, l'obbligo di riferire immediatamente all'Organismo di Vigilanza della deroga attuata.

Sono ovviamente fatte salve le procedure di maggior tutela eventualmente già vigenti a livello aziendale.