MODELLO ORGANIZZATIVO 231

Introduzione

Con il decreto legislativo 8 giugno 2001, n. 231, è stata introdotta nel nostro ordinamento la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle organizzazioni e delle associazioni anche prive di personalità giuridica" per alcuni reati commessi nel loro interesse o a loro vantaggio. Questo decreto è stato emanato sulla base della legge 29 settembre 2000, n. 300, che, nel recepire una serie di atti internazionali e comunitari, delegò il governo a emanare una norma di previsione e disciplina della responsabilità diretta degli enti da reato. In particolare il legislatore con la legge n. 300/2000 ha recepito alcune convenzioni e protocolli internazionali precedentemente sottoscritti dall'Italia:
- la convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea;
- la convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione dei funzionari pubblici della Comunità Europea e degli Stati membri;
- la convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Prima dell'entrata in vigore del decreto legislativo n. 231/2001 era consolidato il principio, di matrice romanistica (*societas delinquere non potest*) e sancito anche dalla costituzione italiana all'articolo 27, secondo il quale la responsabilità penale è personale e quindi gli enti in quanto tali non possono incorrervi.
L'ordinamento italiano prevedeva soltanto agli articoli 196 e 197 del codice penale che sull'ente ricadesse l'obbligazione di pagamento di multe o di ammende in caso di insolvibilità della persona fisica autrice materiale di un fatto accertato come reato commesso dal suo rappresentante legale, oltre a quella di risarcimento del danno.
Il decreto legislativo n. 231/2001, invece, ha introdotto un'assoluta novità nell'ordinamento italiano, ponendo a carico degli enti una responsabilità denominata amministrativa ma con forti analogie con la quella penale; nella relazione ministeriale di accompagnamento si legge infatti che questa responsabilità, " *poiché conseguente da reato e legata alle garanzie del processo penale, diverge in non pochi punti dal paradigma dell'illecito amministrativo"* ; poi la stessa relazione sembra prefigurare un *"tertium genus che coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia"* . Al di là della formale qualificazione giuridica non vi è dubbio che la tipologia di responsabilità delineata dal decreto n. 231/2001 presenti forti analogie con quella penale per diversi motivi: la necessaria derivazione dell'imputazione dell'ente da un fatto materiale di reato, la natura delle sanzioni irrogabili, il richiamo a istituti penalistici sostanziali e processuali, la sottoposizione dell'ente all'accertamento e al giudizio penale con tutte le garanzie previste dal processo penale del nostro ordinamento.

Il decreto legislativo n. 231/2001 prevede infatti a carico degli enti pesanti sanzioni in caso di commissione di reati:
- sanzioni pecuniarie fino a più di un milione e mezzo di euro;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

In ossequio a una specifica tecnica scelta dal legislatore nonché a uno stretto principio di legalità la responsabilità dell'ente non sorge per qualsivoglia fattispecie criminosa ma solo in caso di commissione di specifici reati elencati nello stesso decreto n. 231/2001 o in leggi speciali, sicché sono puniti solo i reati, ancorché in continua crescita, previsti espressamente nel testo originario o introdotti successivamente.

Al momento dell'emanazione del decreto la responsabilità amministrativa degli enti era configurabile solo per le fattispecie di reato di cui agli articoli 24 e 25, relativi ai rapporti con l'amministrazione pubblica, ovvero • malversazione a danno dello Stato o di altro ente pubblico (articolo 316- *bis* cod. pen.);
• indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (articolo 316- *ter* cod. pen.);
• concussione (articolo 317 cod. pen.);
• corruzione per un atto d'ufficio (articolo 318 cod. pen.);
• corruzione per un atto contrario ai doveri d'ufficio (articolo 319 cod. pen.);
• corruzione in atti giudiziari (articolo 319- *ter* cod. pen.);
• istigazione alla corruzione (articolo 322 cod. pen.);
• truffa in danno dello Stato o di altro ente pubblico (articolo 640, comma primo, n. 1 cod. pen.);
• truffa aggravata per il conseguimento di erogazioni pubbliche (articolo 640- *bis* cod. pen.);
• frode informatica in danno dello Stato o di altro ente pubblico (articolo 640- *ter* cod. pen.),
anche se il legislatore aveva già previsto nella relazione di accompagnamento una possibile estensione delle tipologie, sia attraverso una diretta modifica al decreto sia attraverso il rinvio operato da leggi speciali.

Successivamente, infatti, l'articolo 6 della legge 23 novembre 2001 n. 409, recante " *Disposizioni urgenti in vista dell'introduzione dell'euro* ", ha inserito nell'ambito del decreto l'articolo 25- *bis* , che mira a punire il reato di "falsità in monete, in carte di pubblico credito e in valori di bollo". In seguito l'articolo 3 del Decreto Legislativo 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario, ha introdotto il nuovo articolo 25- *ter* del decreto n. 231/2001, estendendo il regime di responsabilità amministrativa degli Enti anche ai cosiddetti reati societari, così come configurati dallo stesso decreto n. 61/2002 (false comunicazioni sociali, false comunicazioni sociali in danno dei soci o dei creditori, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione, impedito controllo, indebita restituzione dei conferimenti,
illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori, illecita influenza sull'assemblea, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, fattispecie poi modificate dalla legge 28 dicembre 2005, n. 262. L'articolo 25- *ter* , comunque, non ha soltanto integrato l'elenco dei reati rilevanti in base al decreto 231/2001, ma ha anche ridisegnato il criterio oggettivo di imputazione della responsabilità amministrativa dell'ente e individuato in modo specifico i potenziali soggetti-autori dei reati presupposto. In deroga, infatti, a quanto previsto dall'articolo 5, D.Lgs. n. 231/2001,

l'articolo 25 ter stabilisce la responsabilità dell'ente " *in relazione ai reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza (...)*" .
Dalla norma emergono due aspetti particolari:
• innanzitutto viene eliminato il requisito del "vantaggio" dell'ente: pertanto, l'ente sarà chiamato a rispondere indipendentemente dal conseguimento di un vantaggio, purché il reato sia stato commesso nel suo interesse;
• in secondo luogo l'individuazione dei potenziali autori del reato-presupposto, pur mantenendo ferma la distinzione dell'articolo 5 tra soggetti "apicali" e "sottoposti", viene limitata a figure particolari, quali amministratori, direttori generali e liquidatori (apicali) e a tutti coloro che siano soggetti alla loro vigilanza (sottoposti).

Dopo l'inserimento dei reati societari l'intervento del legislatore è continuato con la legge 14 gennaio 2003, n. 7 che, ratificando e dando esecuzione alla Convenzione internazionale di New York del 9 dicembre 1999 per la repressione del finanziamento del terrorismo, ha introdotto nel D.Lgs. n. 231/2001 l'articolo **25-quater** relativo ai delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali. Successivamente la legge 11 agosto 2003, n. 228 ha inserito **l'articolo 25-quinquies** che prevede la responsabilità dell'ente per una serie di delitti contro la personalità individuale disciplinati dal codice penale. Nel 2005 la legge comunitaria (legge 18 aprile 2005, n. 62) e la legge sul risparmio (legge 28 dicembre 2005, n. 262) hanno inserito l'articolo 25- *sexies* volto a estendere la responsabilità amministr ativa degli enti ai nuovi reati di abuso di informazioni privilegiate e di manipolazione del mercato. La legge comunitaria 2004 ha inoltre modificato il testo del decreto, introducendo una specifica disposizione, l'articolo 187- *quinquies* , ai sensi della quale l'ente è responsabile del pagamento di una somma pari all'importo della sanzione amministrativa irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (articolo 187- *bis*) e di manipolazione del mercato (articolo 187- *ter*) commessi nel suo interesse o a suo vantaggio da:
a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
La legge 28 dicembre 2005, n. 262 (" *Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari* ") ha poi integrato e modificato sia il testo del decreto sia il codice civile, introducendo tra l'altro il nuovo articolo 2629- *bis* del codice civile relativo al reato di " *Omessa comunicazione del conflitto di interessi* ". Tale reato è stato introdotto, in forza della medesima legge n. 262/2005, nell'articolo 25- *ter* del decreto legislativo n. 231/2001. Con la legge 3 agosto 2007, n. 123, recante "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia" è stato poi introdotto nel decreto l'articolo 25- *septies* , poi sostituito ai sensi dell'articolo 300 del Decreto legislativo 9 aprile 2008, n. 81, che ha esteso il novero dei reati rilevanti ai sensi del decreto a:
• omicidio colposo (articolo 589 cod. pen.);
• lesioni colpose gravi o gravissime (articolo 590 comma 3 cod. pen.) commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.
In seguito il decreto legislativo n. 231/07 di recepimento della direttiva 2005/60/CE, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, ha inserito nel decreto, ai sensi dell'articolo 63 comma 3, l'articolo 25- *octies* che estende l'elenco dei reati a:
• ricettazione (articolo 648 cod.pen.);
• riciclaggio (articolo 648- *bis* cod.pen.);
• impiego di denaro, beni o utilità di provenienza illecita (articolo 648- *ter* cod. pen.).
Infine, per effetto dell'entrata in vigore della legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio di Europa sulla criminalità informatica sottoscritta a Budapest il 23 novembre 2001, è stato introdotto nel decreto l'articolo 24-*bis* che estende l'elenco dei reati a:
• falsità in documenti informatici (articolo 491- *bis* cod. pen.);
• accesso abusivo ad un sistema informatico o telematico (articolo 615- *ter* cod. pen.);
• detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (articolo 615-*quater* cod. pen.);
• diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615- *quinquies* cod. pen.);
• intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617- *quater* cod. pen.);
• installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617- *quinquies* cod. pen.);
• danneggiamento di informazioni, dati e programmi informatici (articolo 635-*bis* cod. pen.);
• danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635- *ter* cod. pen.);
• danneggiamento di sistemi informatici o telematici (articolo 635- *quater* cod. pen.);
• danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635- *quinquies* cod. pen.);
• frode informatica del soggetto che presta servizi di certificazione di firma elettronica (articolo 640- *quinquies* cod. pen.).
Nel 2006 il legislatore è intervenuto con ben tre modifiche al D.Lgs. n. 231/2001. La prima modifica è stata apportata dalla legge 9 gennaio 2006, n. 7, che con il nuovo **articolo 25-quater 1** ha introdotto la responsabilità amministrativa degli enti per l'ipotesi di reato prevista e punita dall'articolo 583- *bis* c.p. (pratiche di mutilazione degli organi genitali femminili). In seguito è stata approvata la legge 6 febbraio 2006, n. 38 contenente nuove norme in materia di lotta contro lo sfruttamento sessuale dei bambini e di contrasto al fenomeno della diffusione della pornografia infantile anche a mezzo internet; fra le novità introdotte, la modifica dell'articolo 25- *quinquies* del decreto n. 231/2001 e l'ampliamento dei reati ivi previsti.
E infine la legge 16 marzo 2006, n. 146, di ratifica della Convenzione e dei protocolli aggiuntivi delle Nazioni Unite contro il crimine transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 ed il 31 maggio 2001, ha esteso la responsabilità amministr ativa degli enti anche ad una serie di reati aventi carattere transnazionale. La tecnica normativa utilizzata dal legislatore è stata diversa rispetto alle precedenti modifiche; anziché integrare il decreto nella parte relativa ai reati- presupposto, esso ha preferito disciplinare direttamente le nuove fattispecie e rinviare al decreto n. 231/2001 la disciplina dei requisiti generali di imputazione della responsabilità all'ente. Il legislatore, al fine di definire l'ambito di applicazione della disciplina in esame, ha formulato una definizione di reato transnazionale, quale illecito punito con una pena della reclusione non inferiore nel massimo a 4 anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

a) sia commesso in più di uno Stato;
b) ovvero sia commesso in uno Stato ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
c) ovvero sia commesso in uno Stato, ma in esso sia impiegato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro. Ai sensi della stessa Legge n. 146/2006, i rati transnazionali rilevanti ai fini della responsabilità amministrativa degli enti sono: reati associativi, traffico di migranti, intralcio alla giustizia (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria e favoreggiamento personale).
La riforma che, però, ha suscitato le maggiori reazioni è stata senz'altro quella attuata con la legge 3 agosto 2007, n. 123, che nel ridisegnare la disciplina in materia di salute e sicurezza sul lavoro, ha previsto la responsabilità degli enti per i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (**articolo 25-septies** del decreto n. 231/2001). La norma ha avuto un impatto estremamente rilevante in quanto tutti gli adempimenti direttamente o indirettamente stabiliti dalla normativa vigente in materia di tutela della salute e sicurezza dei lavoratori (T.U. 81/2008 e non solo) possono oggi rappresentare per gli enti un'area di rischiosità ai sensi dell'articolo 25- *septies* del decreto.

Invece **l'articolo 25-octies** (relativo ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita) è stato inserito dalla legge 21 novembre 2007, n. 231, di attuazione delle direttive 2005/60/CE e 2006/70/CE.
Nel 2008 l'articolo 7 della Legge n. 48 (legge di ratifica ed esecuzione della Convenzione di Budapest del 23 novembre 2001 in materia di criminalità informatica) ha inserito **l'articolo 24-bis** dedicato ai c.d. reati informatici.
Le ultime modifiche al D.Lgs. n. 231/2001 sono state apportate nel 2009 con tre interventi del legislatore:
1) l'articolo 2 della Legge 15 Luglio 2009 n. 94 (Pacchetto sicurezza) ha introdotto **l'articolo 24ter** relativo ai delitti di criminalità organizzata (associazione per delinquere, associazioni di tipo mafioso anche straniere, scambio elettor ale politico-mafioso, sequestro di persona a scopo di estorsione, associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope, illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo).
Invero i delitti contro la criminalità organizzata erano già previsti come potenziali illeciti amministrativi in forza del decreto n. 231/2001 dall'articolo 10 della legge n. 146/2006 ("Ratifica della Convenzione O.N.U. sulla lotta alla criminalità organizzata transnazionale"). L'estensione di tali illeciti anche all'ambito nazionale si inquadra in un più articolato programma di lotta alla criminalità di impresa.
2) L'articolo 15 della Legge 23 luglio 2009 n. 99, tra le altre disposizioni contenute, ha modificato l **'articolo 25- *bis*** (estendendo la sua applicazione anche alla tutela di strumenti o segni di riconoscimento) e inserito **l'articolo 25- *bis* 1** (delitti contro l'industria e il commercio) e **l'articolo 25- *nonies*** (delitti in materia di violazioni del diritto d'autore).
3) L'articolo 4 della legge 3 agosto 2009, n. 116, ha introdotto l **'art 25-novies** (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria) : si tratta di un'apparente sovrapposizione, in quanto esisteva già un articolo 25 *nonies* (delitti in materia di violazione del diritto d'autore).
Deve infine essere precisato che la legge delega n. 300 del 2000 (articolo 11, co. 1, lett. d), prevedeva di estendere la responsabilità amministrativa degli enti ai *"(...) reati in materia di tutela dell'ambiente e del territorio, che siano punibili con pena detentiva non inferiore nel massimo ad un anno anche se alternativa alla pena"* . Tuttavia il legislatore nel 2001 non ha dato adempimento a tale delega ambientale, rinviando a un secondo intervento normativo l'inserimento degli illeciti penali ambientali nel catalogo dei reati ex D.Lgs. n. 231/2001, avvenuto prima della fine del 2010, in quanto la Direttiva 2008/99/CE del Parlamento europeo e del Consiglio, del 18 novembre 2008, sulla tutela penale dell'ambiente, doveva tassativamente essere recepita entro il 26 dicembre 2010.
L'articolo 6 di questa Direttiva dispone che « *gli stati membri provvedono affinché le persone giuridiche possano essere dichiarate responsabili dei reati di cui agli articoli 3 [infrazioni] e 4 [favoreggiamento e istigazione ad un reato] quando siano stati commessi a loro vantaggio da qualsiasi soggetto che detenga una posizione preminente in seno alla persona giuridica, individualmente o in quanto parte di un organo della persona giudica...».*

I destinatari del decreto legislativo 231/2001

L'articolo 1 del decreto legislativo. n. 231 definisce l'ambito di applicazione oggettivo; in particolare la disciplina in questione si applica ai seguenti soggetti:

- enti forniti di personalità giuridica;
- società e associazioni anche prive di responsabilità giuridica.

Non si applica invece:

- allo Stato;
- agli enti pubblici territoriali;
- agli altri enti pubblici non economici;
- agli enti che svolgono funzioni di rilievo costituzionale.

La disciplina si rivolge quindi oltre che alle società, a tutti gli enti dotati di personalità giuridica nonché alle associazioni anche prive della personalità giuridica. In riferimento agli enti pubblici essa ricomprende i soli enti pubblici economici. La scelta del legislatore di utilizzare il termine "ente" anziché "persona giuridica" si giustifica proprio con l'intenzione di voler responsabilizzare anche quegli enti "privati" non dotati di personalità giuridica, che per la loro snellezza di struttura e funzionamento potrebbero facilmente sottrarsi ai controlli pubblici.

Presupposti per l'imputazione della responsabilità all'ente.

L'articolo 5 del decreto elenca una serie di presupposti per l'imputazione della responsabilità all'ente; in particolare è necessario:

1) che la condotta materiale sia stata realizzata: da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (i soggetti apicali); ovvero da soggetti sottoposti alla direzione o alla vigilanza di chi gestisce o controlla l'ente (i soggetti subordinati);
2) che il reato sia stato commesso nell'interesse o vantaggio dell'ente (pertanto quest'ultimo non risponde se le persone fisiche di cui alla lettera a) hanno agito nell'interesse esclusivo proprio o di terzi).

In relazione al primo presupposto la distinzione fra figure apicali e soggetti sottoposti non è di poco conto, visto che l'articolo 6 del decreto prevede una differenziata distribuzione dell'onere della prova. In caso di commissione materiale del reato da parte di soggetti apicali, infatti, spetta all'ente offrire la prova dell'adozione del modello organizzativo, della predisposizione di un organismo di vigilanza, dell'elusione fraudolenta del modello stesso e dell'efficace controllo attuato dal citato organo di controllo. In altri termini in caso di commissione del reato da parte di soggetti in posizione apicale sussiste una vera e propria forma di presunzione di responsabilità, che l'ente potrà superare offendo la prova contraria. Occorre precisare, inoltre, che rientrano fra i soggetti apicali anche coloro che di fatto (non solo di diritto), in virtù di poteri originari o delegati, esercitano un penetrante controllo sull'ente ovvero su una sua unità organizzativa dotata di autonomia finanziaria e funzionale. Per quanto riguarda i soggetti sottoposti all'altrui vigilanza l'articolo 6 fa riferimento a tutte le persone che all'interno dell'organizzazione dell'ente si trovano in una posizione di subordinazione rispetto alle figure apicali. Nel caso in cui questi ultimi siano gli autori materiali del reato l'onere di dimostrare che il fatto illecito è stato realizzato eludendo fraudolentemente la direzione e vigilanza dei vertici dell'ente spetta al pubblico ministero. Tuttavia, la stessa norma prevede che il rispetto degli obblighi di direzione e vigilanza possa essere presunto in caso di previa adozione ed efficace attuazione di un adeguato modello di organizzazione, gestione e controllo. Il secondo presupposto necessario per l'imputazione della responsabilità all'ente è l'esistenza di un interesse o vantaggio dello stesso, non necessariamente di tipo economico. Nell'interpretazione delle due locuzioni, in dottrina e giurisprudenza si sono sviluppate tre teorie: la prima ritiene che i due termini (interesse e vantaggio) siano sovrapponibili, come in una sorta di endiadi, ed entrambi riferibili a un generico "interesse oggettivo" dell'ente. Una seconda teoria ritiene che il requisito dell'interesse assorba di fatto quello del vantaggio, che sarebbe una sorta di variante eventuale del primo, anche in analogia con quanto previsto per i reati societari dall'articolo 25-*ter*, del decreto, che fa esclusivo riferimento al criterio dell'interesse). Un ultimo filone interpretativo, prevalente anche in giurisprudenza, segue l'opposto assunto per cui i termini "interessi e vantaggio" sarebbero assolutamente distinti ed alternativi, in ossequio a una lettura sistematica del decreto e al generale principio interpretativo di conservazione delle norme. In conformità alla stessa relazione governativa di accompagnamento al decreto il concetto di "interesse dell'ente" andrebbe interpretato in senso soggettivo, in riferimento cioè alla volontà dell'autore materiale del reato da valutare *ex ante* ; al contrario occorrerebbe leggere il vantaggio in senso oggettivo, facendo riferimento cioè agli effettivi risultati della condotta criminosa, da valutare *ex post*. Resta fermo in ogni caso il principio per cui *"l'ente non risponde se le persone indicate nel comma 1 [ndr soggetti apicali e subordinati] hanno agito nell'interesse esclusivo proprio o di terzi"* (articolo 5, comma 2, del decreto 231/2001).

I modelli di organizzazione, gestione e controllo.

L'articolo 6 del decreto n. 231 prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione dei reati se dimostra di aver adottato ed efficacemente attuato prima della commissione del fatto un " *modello di organizzazione e gestione idoneo a prevenire i reati della specie di quello verificatosi* ", con l'attribuzione del compito di vigilanza ad uno specifico organismo.

Rinviando a quanto si dirà specificatamente in seguito, è bene ricordare che i modelli devono rispondere a cinque specifiche esigenze:

- individuare le attività a rischio di reato;
- prevedere specifici protocolli di formazione e attuazione delle decisioni dell'ente;
- individuare i processi di gestione dei flussi finanziari;
- prevedere un flusso informativo verso l'organismo di vigilanza;
- prevedere ed attuare uno specifico sistema sanzionatorio in caso di mancato rispetto del modello.

Poiché, ai sensi dell'articolo 6, comma 3°, del decreto, i modelli di organizzazione, gestione e controllo possono essere adottati sulla base di "codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire reati".

Il modello organizzativo, l'analisi dei rischi e i protocolli

Il Modello di organizzazione, di gestione e di controllo.

L'articolo 6, comma 1°, del decreto legislativo n. 231/2001, prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione dei reati se dimostra di aver adottato ed efficacemente attuato prima della commissione del fatto un " *modello di organizzazione e gestione idoneo a prevenire i reati della specie di quello verificatosi* ". Il comma 2° dello stesso articolo specifica le esigenze che tale modello organizzativo deve soddisfare:

- individuare attività e processi aziendali esposti al rischio di commissione reati;
- definire specifici protocolli che individuino le modalità di formazione e di attuazione delle decisioni dell'ente;
- individuare modalità di gestione delle risorse finanziarie in grado di prevenire la commissione di reati;

- prevedere idonei sistemi, procedure ed obblighi di comunicazione verso l'organismo di vigilanza;
- introdurre un sistema disciplinare idoneo a sanzionare la violazione delle misure e dei protocolli individuati nel modello.

Lo scopo del modello organizzativo è in altri termini la costruzione di un sistema strutturato e organico di procedure, protocolli, regole e attività di controllo, volto a prevenire e contrastare il rischio di commissione di reati contemplati nel decreto n. 231.
In particolare il modello si propone le finalità di:

- definire il corretto espletamento delle attività che vanno a costituire l'agire dell'ente nell'ambiente economico e sociale in cui opera;
- diffondere la necessaria consapevolezza in tutti coloro che operano in nome e per conto dell'ente di poter incorrere, in caso di violazione delle disposizioni contenute nel modello stesso, in un illecito sanzionabile sul piano penale e amministrativo;
- diffondere la necessaria consapevolezza in tutti coloro che operano in nome e per conto dell'ente che l'eventuale responsabilità personale per uno dei reati previsti dal decreto n. 231/2001 può comportare il sorgere di responsabilità e sanzioni per l'ente stesso;
- sottolineare che tutti i comportamenti difformi ai principi e alle disposizioni del modello adottato sono sistematicamente condannati dall'ente, in quanto contrari ai propri principi etico-sociali prima ancora che alle disposizioni di legge;
- informare tutti gli interessati che la violazione delle prescrizioni contenute nel modello costituisce violazione delle direttive aziendali, e per tale ragione è soggetta all'applicazione di sanzioni, in coerenza con quanto previsto dalla legge, dai contratti nazionali di lavoro, e ogni altro accordo intercorso con l'ente stesso;
- consentire all'ente, grazie a una costante azione di monitoraggio sui "processi a rischio di reato", di intervenire tempestivamente per prevenire e contrastare la commissione dei reati stessi;
- costituire un organo societario terzo, dotato di poteri e risorse adeguate, deputato all'implementazione, aggiornamento e applicazione del modello (organismo di vigilanza).

Il concetto di rischio accettabile.

La costruzione di un modello, in base all'articolo 6, comma 2°, del decreto legislativo n. 231/2001, deve partire da una corretta e completa "mappatura" dei processi/aree aziendali "sensibili", in quanto esposti al rischio di commissione dei reati in esso previsti. A questo fine è necessario un approfondito studio del contesto aziendale per identificare in modo chiaro tutti i possibili "eventi pregiudizievoli" per l'ente e le modalità attraverso le quali si possono verificare. Il processo di autovalutazione che gli interessati devono compiere per catalogare tutti i possibili rischi, comporta l'analisi di elementi caratterizzanti l'azienda medesima, quali per esempio la struttura organizzativa, l'articolazione territoriale, le dimensioni, il settore economico e le aree geografiche in cui essa opera, le specifiche attività, la storia, nonché l'analisi dei singoli reati che si possono collegare a questi elementi.
Una volta identificati i processi/aree aziendali "sensibili" occorre strutturare un sistema di controllo in grado di eliminare i rischi identificati o quanto meno ridurli a un livello *accettabile* . Il concetto di *rischio accettabile* , parametro e premessa fondamentale per la costruzione del sistema di controllo, appare tuttavia di difficile definizione. Una soluzione può essere data legando il concetto di rischio accettabile a quello di *comportamento esigibile* , ossia di condotta che oggettivamente ci si può attendere dall'ente e dalle singole figure che in esso operano. Il comportamento concretamente esigibile è ad esempio, quella condotta che ai sensi dell'articolo 40, comma 2°, del codice penale, ci si può concretamente e ragionevolmente attendere nella situazione concreta al fine di evitare il verificarsi dell'evento lesivo. Lo stesso decreto n. 231/2001 sembra orientarsi in questa direzione quando all'articolo 6, comma 1°, lettera c, esclude la responsabilità dell'ente per i casi in cui le figure apicali autrici del reato abbiano agito con *"elusione fraudolenta del modello"* . L'elusione fraudolenta è proprio la condotta di chi si sottrae con artifizi e raggiri all'applicazione di determinate regole, direttive e procedure; tale circostanza, tuttavia, rileva ai fini della esclusione della responsabilità dell'ente solo se da quest'ultimo oggettivamente *"non prevedibile"* con la diligenza che ci si può ragionevolmente attendere dall'ente in base alla sua attività, struttura, estensione geografica, dimensione eccetera. In sintesi, dunque, il "rischio accettabile" si ridurrà a quel rischio che "residua" in seguito alla corretta definizione e applicazione di procedure, regole e principi previsti dal sistema di controllo aziendale e in seguito a un controllo diligente ed efficace da parte dell'ente (per mezzo dell'organismo di vigilanza e dei vertici aziendali). Questo concetto di rischio accettabile va, però, adattato alle ipotesi di reati colposi (articolo 25-*septies*), in quanto la stessa essenza della colpa (mancanza di volontà) risulta incompatibile con il concetto di elusione fraudolenta. In questo caso il confine di accettabilità del rischio è segnato dalla commissione di atti, non accompagnati dalla volontà, che concretizzino una violazione sostanziale del modello, fermo restando l'efficace e puntuale controllo dell'organismo di vigilanza preposto.

Il processo di analisi si concretizza, quindi, nella definizione per ogni processo o area aziendale di una reale e oggettiva quantificazione del rischio accettabile e del rischio residuo. Per compiere tale percorso, possono venire in ausilio tecniche di analisi dei rischi che normalmente definiscono il rischio residuo come il prodotto di tre fattori:
- gravità del potenziale comportamento scorretto;
- frequenza di esposizione al rischio;
- rilevabilità da parte dell'organizzazione dell'eventuale condotta di reato.

La valutazione quantitativa dei tre fattori può avvenire attraverso un'analisi dei comportamenti delle singole funzioni aziendali, compiuta tramite interviste e raccolta di dati storici aziendali. La metodologia proposta ha valenza generale; può, infatti, essere applicata a varie tipologie di rischi:
operativi (fisico, informatico, di compliance, legale, contabile, fiscale, processo eccetera), di mercato, di credito e così via.

La metodologia consente di utilizzare il medesimo approccio anche qualora i principi del decreto siano estesi ad altri ambiti. Se poi tali ambiti sono regolati da specifica normativa (per esempio adeguamento a standard internazionali previsti dalle norme UNI EN ISO per i sistemi di gestione qualità, ambiente sicurezza, etica eccetera), il modello dovrà integrarsi (non sovrapporsi e sostituirsi) con le regole preesistenti.

La realizzazione del sistema di analisi, valutazione e gestione dei rischi.

Una volta definita la metodologia di rilevazione e quantificazione dei rischi aziendali, occorre procedere concretamente alla realizzazione del sistema di controllo e prevenzione, che si articola in tre attività fondamentali: a) mappatura di aree, processi e funzioni aziendali in cui possono essere commessi reati;
b) analisi delle eventuali carenze rilevate; c) definizione e rafforzamento di adeguati presidi.
Semplificando, queste tre fasi possono essere realizzate cercando di rispondere ad alcuni quesiti di base:
Chi siamo?
A quali norme siamo soggetti?
Cosa facciamo?
Come controlliamo?
Come verifichiamo?
Come rimediamo?
In risposta a questi interrogativi si dovranno considerare i diversi aspetti dell'organizzazione e della struttura aziendale.

Chi siamo.
Dati di partenza: organigramma aziendale, mansionario, sistema di deleghe interne, procure, certificazioni camera di commercio, analisi si poteri e natura di organi aziendali statutari e non, elenco dipendenti e collaboratori ecc.
Attività da svolgere: individuazione degli attori a cui fanno capo le fasi dei processi aziendali.
L'esame dei documenti individuati come dati di partenza mira a definire un quadro chiaro di ruoli e responsabilità, individuando soprattutto i soggetti qualificabili come figure apicali ai sensi dell'articolo 5, comma 1, lett. a, del decreto n. 231/2001, in quanto "*persone che rivestono funzioni di rappresentanza, di amm inistrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale ...[o comunque] persone che esercitano, anche di fatto, la gestione e il controllo dello stesso*".
L'individuazione delle figure apicali è essenziale in quanto esse si trovano di fatto ad essere destinatarie di protocolli ed obblighi specifici previsti nel modello, nonché svolgere un ruolo essenziale per la diffusione e l'efficace applicazione del modello stesso.
Applicazione concreta: mappa delle figure apicali, adeguato sistema di deleghe e procure.

A quali norme siamo soggetti.
Dati di partenza: adempimenti relativi a dettati normativi cogenti, contrattuali, volontari.Attività da svolgere: analisi delle "norme" a cui è soggetta l'azienda. L'azienda è soggetta a diversi vincoli: innanzitutto quelli cogenti dell'ordinamento nazionale e comunitario, poi quelli derivanti dall'adeguamento a standard internazionali (norme ISO per i sistemi di gestione qualità, ambiente sicurezza, etica ecc.) o da espresse richieste contrattuali del cliente. Vanno altresì considerate le disposizioni contenute in atti costitutivi, statuti sociali, regolamenti interni all'ente. Tutti questi documenti e informazioni vengono inseriti e integrati nel modello, che da un lato li recepisce come presidi organizzativi preesistenti, dall'altro li utilizza come strumento di controllo e verifica dei processi aziendali. Applicazione concreta: elenco dei presidi normativi esistenti per ciascun processo o area.

Cosa facciamo.
Dati di partenza: processi, funzioni, attività, aree, istruzioni, regolamenti, procedure, prassi operative aziendali. Esame storico egli eventuali provvedimenti sanzionatori antecedenti all'adozione del modello. Attività da svolgere: descrivere i processi e gli attori delle attività svolte nelle varie aree aziendali, guardando alle potenziali capacità di incorrere in uno dei reati di cui al decreto 231/2001. Ciò significa comprendere l'identità della società, i servizi che offre ai clienti, i punti di forza e di debolezza, gli obiettivi che ne stanno guidando l'evoluzione. Un processo è una sequenza di attività che ha come risultato un prodotto o un servizio per un cliente esterno o interno all'azienda, e viene descritto definendo come le persone, le informazioni e le risorse materiali lavorano e interagiscono per fornire valore al cliente finale. L'analisi dei processi o delle aree aziendali può avvenire secondo approcci diversi (approccio orizzontale, partendo cioè dagli attori per giungere alle attività svolte) o verticale (dalle attività per risalire agli attori). A prescindere dal tipo di approccio prescelto, occorrerà in ogni caso procedere ad un vero e proprio raffronto fra l'elenco dei reati previsti dal decreto n. 231/2001 e le attività poste in essere in ciascuna area aziendale al fine di definire quali soggetti, processi e attività siano esposti al rischio di potenziale realizzazione dei reati medesimi. La descrizione dei processi aziendali è uno dei primi passi per compiere un efficace Business Process Management, un approccio al governo dell'azienda orientato a renderne efficiente il business attraverso la conoscenza, il controllo e il perfezionamento delle sue catene del valore. I processi nella letteratura del (BPM) sono
normalmente suddivisi in quattro categorie:
- Governo: processi di gestione e di funzionamento dell'azienda;
- Business: processi core attraverso i quali la società eroga i suoi servizi;
- Mercato: processi di interazione con il clienti, quali marketing, customer care,...;
- Supporto: processi interni che producono servizi ad altri processi o a unità interne dell'azienda.

L'identificazione dei processi e dei sottoprocessi delle quattro categorie definisce il framework dei processi aziendali, un modello univoco per descrivere il funzionamento della realtà aziendale che permette, da un lato, di «fotografare» la globalità dell'azienda, e, dall'altro, di capitalizzarne la conoscenza mantenendo la coerenza e l'omogeneità delle singole analisi di processo. La definizione del framework dei processi e la successiva rappresentazione per processo delle diverse attività aziendali consente di:
- gestire dinamicamente e con semplicità l'evoluzione dei processi nel tempo, mantenendo aggiornata l'analisi dei rischi a interventi mirati alle sole aree del framework interessate dai cambiamenti;
- disporre di un modello concettuale per l'analisi e l'individuazione delle aree di intervento per il miglioramento delle performance aziendali, in termini di efficacia ed efficienza;
- fornire alle diverse unità organizzative un comune ed organico sistema di interpretazione delle realtà aziendali;
- produrre in modo automatizzato i mansionari delle diverse unità organizzative;
- normalizzare e standardizzare la documentazione aziendale.

Applicazioni concrete: mappa documentata delle potenziali modalità attuative degli illeciti nelle aree a rischio.

Come controlliamo.
Dati di partenza: sistema dei controlli interni esistenti.
Attività da svolgere: verifica dei sistemi di controllo già applicati. Quantificazione del "rischio residuo".
Individuazione di protocolli aggiuntivi.. Una volta individuate le aree "sensibili", occorre verificare i protocolli esistenti, ossia gli eventuali presidi già applicati in azienda e in grado di prevenire la realizzazione degli illeciti. In base a tale analisi sarà possibile procedere alla quantificazione del "rischio residuo" secondo la metodologia sopra proposta.
Qualora poi i protocolli non esistano o comunque appaiano insufficienti o inefficaci, il rischio residuo risulterà superiore alla soglia di accettabilità. A questo punto l'azienda dovrà necessariamente procedere all'implementazione di nuovi protocolli o al rafforzamento di quelli già esistenti, così da abbassare il grado di esposizione al rischio di commissione reati (l'articolo 6, c.2, lett. b, del decreto n. 231/2001 dispone proprio che il modello risponda all'esigenza di *"prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai rati da prevenire"*).
I protocolli hanno la finalità di modulare nel concreto l'agire sociale, andando a richiamare l'osservanza del codice etico (principi di comportamento) e a specificare, sebbene per principi, l'operatività a cui devono ispirarsi i destinatari del modello al fine di prevenire la commissione del singolo reato (principi di attuazione). Possono anche essere previste procedure e istruzioni specifiche per determinati processi/aree sensibili.
I principi generali posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

PRINCIPI ETICI: l'azienda deve diffondere all'interno dell'organizzazione, e nei confronti di tutti gli stakeholders, una tavola dei principi, impegni e responsabilità etici a cui essa ispira la sua attività e delle corrispondenti condotte richieste ai destinatari. La scelta dei principi etici deve trovare una corrispondenza nelle fattispecie di reato previste dal decreto n. 231/2001. Tali principi possono essere inseriti in codici etici di carattere più generale, laddove esistenti, o invece essere oggetto di autonoma previsione.
CHIARA DEFINIZIONE DI RUOLI E RESPONSABILITÀ: l'ente deve definire in documenti formali (organigramma, mansionario, funzionigramma, deleghe e procure, nomine ecc.) le funzioni e i poteri di ciascuna figura aziendale, chiarendo la tipologia di rapporti (gerarchici, di staff, di controllo, di riporto) intercorrenti fra gli stessi. Andranno chiaramente definite le modalità di accesso a determinati ruoli in azienda e gli eventuali sistemi premianti e di gratificazione rivolti al personale (obiettivi, risultati, scatti di anzianità, acquisizione nuovi titoli e competenze).
SEGREGAZIONE DELLE ATTIVITÀ: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla (logica autorizzazione - esecuzione - controllo). Deve essere evitata in ogni caso la concentrazione di poteri e funzioni in un'unica figura, così da assicurare in ogni circostanza l'eventuale controllo da parte di funzioni separate o gerarchicamente sovraordinate.

ESISTENZA DI PROCEDURE/NORME/CIRCOLARI: devono esistere disposizioni aziendali e procedure formalizzate (informatiche e manuali) idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante.
Il rispetto attento delle procedure adottate appare necessario soprattutto per l'area amministrativofinanziaria (l'articolo 6, comma 2°, lett. c, del decreto. n. 231/2001 dispone esplicitamente che il modello deve " *individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati*"). In questo ambito il sistema dei controlli interni potrà essere attuato attraverso strumenti diffusi e riconosciuti: abbinamento firme, riunioni periodiche e frequenti, condivisione dei compiti, previsione di almeno un duplice controllo (operatore e figura apicale), verifica di rispetto del budget, verifica esistenza di adeguata documentazione di supporto e giustificazione (fattura, contratto, ordine, ddt, delibera ecc). Qualora poi determinate operazioni vengano svolte, per scelta aziendale o per eventi eccezionali, al di fuori del sistema di procedure e prassi adottate, sarà importante garantire l'assoluta trasparenza e documentazione dell'attività svolta.
POTERI AUTORIZZATIVI E DI FIRMA: i poteri autorizzativi e di firma devono essere coerenti con le responsabilità assegnate e devono prevedere, ove richiesto, l'indicazione dei limiti di spesa; devono, inoltre, essere chiaramente definiti e conosciuti all'interno della società e all'esterno. Occorre evitare in ogni caso di attribuire poteri illimitati e svincolati dalla verifica a soggetti che sono tenuti ad adottare decisioni che potrebbero comportare la commissione di reati.
TR ACCIABILITÀ e RINTRAC CIABILITÀ: tutte le azioni e le operazioni dell'ente devono essere registrate, coerenti, congrue, verificabili. Per ogni operazione vi deve essere un adeguato supporto documentale al fine di poter procedere in ogni momento all'effettuazione dei controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.
SEGNALAZIONE: ogni attività che mantiene intrinsecamente un rischio residuo elevato deve essere comunicata ad un'entità aziendale deputata alla vigilanza (es. superiore gerarchico, Organismo di Vigilanza, Internal audit). In particolare, il sistema di controllo di gestione deve essere tale da garantire una segnalazione tempestiva di situazioni critiche.
COMUNICAZIONE, FORMAZIONE E ADDESTRAMENTO DEL PERSONALE: deve essere predisposto in azienda un adeguato piano di comunicazione/formazione/addestramento del personale, riferito non solo al contenuto dell'eventuale codice etico adottato, ma anche alla struttura organizzativa aziendale nel suo insieme, alla distribuzione di compiti e poteri, alle procedure, istruzioni e prassi operative applicate, alle disposizioni normative adottate in azienda, ai contenuti generali del modello e ai protocolli previsti a seguito dell'analisi dei rischi, alle decisioni degli organi sociali, alle deliberazioni dell'organismo di vigilanza e degli altri organi di controllo aziendali ecc. Il piano di comunicazione/formazione/addestramento deve essere mirato, adeguato alle capacità e competenze dei destinatari, continuo, rispettoso dei requisiti di veridicità e completezza.
SISTEMA DI GESTIONE DELLA SICUREZZA NEI LUOGHI DI LAVORO: una menzione a parte merita l'aspetto relativo alla sicurezza sui luoghi di lavoro.

Il sistema di gestione della sicurezza deve essere strutturato e gestito mirando ad assicurare la totale conformità normativa alle disposizioni vigenti (ad esempio TU 81/08 e ss.mm.) e l'adozione di tutti i sistemi di prevenzione esistenti e applicabili. Un primo passo fondamentale è l'esplicitazione chiara e la pubblicizzazione, mediante documenti formali (es. codice etico, circolari, istruzioni, procedure ecc.), dei principi e dei criteri fondamentali che sono alla base della gestione aziendale del sistema di salute e sicurezza sul lavoro. È inoltre necessario garantire la corretta individuazione dei responsabili e identificare chiaramente i poteri a essi attribuiti. Occorre, pertanto, un adeguato sistema di procure, deleghe e nomine conformi a quanto previsto dal TU 81/2008 e dalla giurisprudenza esistente in materia e di conseguenza la strutturazione e

diffusione di uno specifico organigramma per la sicurezza, con l'indicazione nominativa dei singoli soggetti (Datore di lavoro, Medico competente, Rappresentante dei lavoratori per la sicurezza, Responsabile del sistema di prevenzione e protezione, Addetti al servizio di protezione e prevenzione, Addetti al primo soccorso, antincendio e gestione delle emergenze, Dirigenti per la sicurezza, Preposti ecc.). A tali soggetti, formalmente individuati, occorre garantire percorsi formativi conformi alle disposizioni normative vigenti in termini di durata, qualifica del formatore, contenuti, verifica dell'efficacia, attestazione finale ecc. Occorre poi predisporre, discutere, approvare, archiviare, aggiornare e diffondere la documentazione richiesta *ex lege* a garanzia della prevenzione e tutela della sicurezza dei lavoratori (documento di valutazione dei rischi, documenti di valutazione rischi interferenziali, nomine, deleghe, procure, attestati, procedure e istruzioni, manuali, progetti, pos, verbali ecc.). La formazione e l'informazione delle risorse umane rappresenta un passaggio fondamentale nella gestione della sicurezza in azienda; informazione e formazione devono essere in ogni caso adeguati agli aggiornamenti normativi, alle conoscenze e alle mansioni del destinatario, alle innovazioni tecnologiche. Soprattutto occorre garantire a tutto il personale periodici incontri dedicati alla gestione della sicurezza sul lavoro.
Accanto a questo sistema di formazione/informazione gestito dal vertici aziendali, occorre prendere atto che le comunicazioni provenienti dalle stesse risorse umane assumono un'importanza fondamentale sia nell'individuazione e valutazione dei rischi sia nell'aggiornamento del sistema in generale. Per esempio i dipendenti e collaboratori possono offrire utili informazioni in merito a mancati incidenti e mancati infortuni, carenze o inefficienze a macchine ed impianti, comportamenti scorretti di collaboratori, fornitori e appaltatori. Un corretto sistema di gestione della sicurezza presuppone inoltre un'attenta gestione dei rapporti di fornitura e appalto; a tale proposito è necessario predisporre un adeguato sistema di selezione, e trasmettere a fornitori ed appaltatori tutte le informazione e documentazioni previste *ex lege* .
Infine un'adeguata gestione della salute e sicurezza sul lavoro dovrebbe prevedere una fase di controllo e valutazione del sistema nel suo complesso e una fase di verifiche ispettive periodiche, rivolte a processi, attività, soggetti specifici, condotte da figure adeguatamente formate e competenti. In seguito a tali verifiche il "sistema sicurezza" nel suo complesso dovrebbe essere sottoposto a un adeguato aggiornamento, nell'ottica del "miglioramento continuo". Il sistema di controllo relativo ai rischi per la salute e sicurezza sul lavoro, così delineato nei suoi aspetti generali, dovrebbe integrarsi con il modello di cui al decreto legislativo n. 231/2001 ed essere congruente con la gestione complessiva dei processi aziendali.

I principi di controllo fin qui indicati rappresentano una mera esemplificazione e necessitano di uno specifico adeguamento alle realtà aziendali in cui sono adottati. In ogni caso essi dovranno essere inseriti in un sistema organico di controlli e presidi, che deve essere efficace nel suo complesso.Quanto appena detto vale soprattutto in relazione agli enti di piccole dimensioni, alle quali è irrealistico imporre l'utilizzo di tutto il complesso bagaglio di strumenti di controllo a disposizione delle grandi organizzazioni. A seconda della scala dimensionale potranno quindi essere utilizzate soltanto alcune componenti di controllo, mentre altre potranno venire escluse (magari perché implicite nel modello aziendale) o essere presenti in termini estremamente semplificati. Tuttavia, è opportuno ribadire che, per tutti gli enti, siano essi grandi, medi o piccoli, il sistema di controlli preventivi dovrà essere tale che lo stesso:

- nel caso di reati dolosi, non possa essere aggirato se non con intenzionalità;
- nel caso di reati colposi, come tali incompatibili con l'intenzionalità fraudolenta, risulti comunque violato, nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito organismo.

Applicazioni concrete: descrizione documentata del sistema dei controlli preventivi attivato, con dettaglio delle singole componenti del sistema, nonché degli adeguamenti eventualmente necessari.

Come verifichiamo.
Dati di partenza: analisi della situazione.
Attività da svolgere: programmazione ed esecuzione di sessioni di analisi dei dati.
La gestione del modello deve prevedere una fase di verifica del suo mantenimento e aggiornamento nonché dell'applicazione ed efficacia dei protocolli adottati.
Le verifiche, eventualmente svolte o disposte dall'organismo di vigilanza, devono essere innanzitutto pianificate e poi eventualmente integrate con le verifiche previste ed attuate da altri enti (es. internal auditing, enti di certificazione terzi, responsabile del sistema di gestione qualità, ambiente, sicurezza, etica ecc.).
Ciascuna verifica deve essere intrapresa previa definizione:
- dei soggetti che le conducono e delle loro competenze;
- delle modalità utilizzate;
- delle aree/funzioni/soggetti coinvolti;
- delle modalità di verbalizzazione e di riporto ai vertici aziendali o all'organismo di vigilanza;

Applicazione concreta: verifica dell'esito delle sessioni di controllo.

Come rimediamo.
Dati di partenza: sessioni di controllo.
Attività da svolgere: gli esiti delle verifiche devono essere tempestivamente comunicati all'organismo di vigilanza, il quale, dopo un attento esame, concorderà con le funzioni competenti la definizione di misure correttive (modifiche e introduzione di protocolli, applicazione di sanzioni, integrazioni a contratti e documenti, intensificazione di momenti formativi, aggiornamento organigramma, informazione ad organi societari ecc.).
In un secondo momento occorrerà in ogni caso verificare l'efficace applicazione delle misure correttive disposte.
Applicazioni concrete: pianificazione degli interventi da effettuare.

Adozione e diffusione del modello di organizzazione, di gestione e di controllo.

Il processo di analisi dei rischi e di definizione dei protocolli di contenimento trova la sua sintesi finale in un documento complessivo, il "modello organizzativo".Questo documento può essere

strutturato in due parti: una "parte generale", che contiene i punti cardine del modello e tratta del funzionamento dell'organismo di vigilanza e del sistema sanzionatorio, e una "parte speciale" il cui contenuto è strutturato sulle diverse tipologie di reato previste dal decreto 231/2001, aventi un'attinenza più specifica all'attività istituzionale della Associazione. Il modello, così strutturato, assume la funzione di vero e proprio manuale aziendale a disposizione delle funzioni interne e dei terzi, affinché tutti sappiano, in particolare, chi ha potere decisionale, di spesa e di controllo, e quali sono le modalità del corretto agire.Risulta quindi evidente che qualsiasi violazione delle regole di condotta delineate dal modello stesso per prevenire i reati di cui al decreto e, in generale, dei protocolli richiamati dal modello o attuativi dello stesso, è suscettibile di sanzione da parte delle funzioni aziendali competenti, in conformità al sistema sanzionatorio adottato. L'applicazione delle sanzioni prescinde, inoltre, dall'effettiva commissione di un reato e, quindi, dall'apertura di un eventuale procedimento penale. In relazione all'adozione ed efficace attuazione del modello l'articolo 6, comma 1°, del decreto legislativo n. 231/2001 dispone che tali attività siano di competenza dell'*organo dirigente*. Una corretta lettura della disposizione porta ad affermare che l'approvazione e l'adozione formale del modello, come ogni successiva integrazione e aggiornamento sostanziale, avvengano con un'apposita delibera del consiglio di amministrazione.
In seguito ad aggiornamenti normativi, cambiamenti nell'organizzazione, nei processi e nelle attività aziendali o al verificarsi di eventi straordinari (gravi violazioni, contestazioni, sanzioni ecc.) possono rendersi necessarie delle modifiche del modello, che è auspicabile giungano all'approvazione del consiglio di amministrazione principalmente per proposta dell'organismo di vigilanza. Dopo la delibera del consiglio sarà compito dell'organismo di vigilanza procedere all'attuazione e alla diffusione delle innovazioni apportate. Per quanto riguarda la gestione del modello le responsabilità sono suddivise fra diversi organi e soggetti aziendali presenti all'interno della Associazione; in particolare:

- L'Organo Amministrativo (il C.d.A.):
- delibera e dispone sulla definizione, sugli ampliamenti e sulle modifiche del modello;
- nomina i membri dell'O.d.V.;
- riceve informazioni periodiche dall'O.d.V. sul funzionamento del modello e sulle sue violazioni.
- L'Organismo di Vigilanza (O.d.V.):
- vigila affinché il modello sia efficace ed idoneo a prevenire la commissione di reati; -vigila affinché il Modello sia costantemente aggiornato e divulgato;
- vigila affinché il modello sia sempre osservato da tutti i soggetti cui è rivolto.
- Il C ollegio Sindacale, ove presente, riceve informazioni periodiche dall'O.d.V. sul funzionamento del modello e sulle sue violazioni.
- I destinatari:
- hanno il dovere di applicare le disposizioni del modello;
- collaborano con l'O.d.V. nel processo di verifica e di monitoraggio e diffusione.

Il codice etico e il sistema disciplinare.

3.1 Premessa

Il codice etico può definirsi il documento che, a partire dalla presentazione dei valori e dalle regole comportamentali cui l'ente intende fare riferimento nell'esercizio della propria attività imprenditoriale, stabilisce le responsabilità etico sociali dei "portatori d'interesse" (Organi Sociali, Soci, Dipendenti, Collaboratori, Consulenti, Fornitori, Clienti, Pubblica Amministrazione, ecc.) nei confronti dell'ente e viceversa, sia in termini di principi generali sia in termini di condotte attese. La finalità del codice etico consiste, di conseguenza, nel raccomandare, promuovere o vietare determinati comportamenti, al di là ed indipendentemente di quanto previsto dall'ordinamento giuridico nazionale e dell'Unione Europea, in linea con la visione aziendale e con la missione mutualistica e/o di utilità sociale (laddove presenti) consacrate nello statuto sociale. L'effettività delle disposizioni del codice etico deve essere assicurata dal regime disciplinare previsto dal modello di organizzazione e gestione, di cui all'articolo 6 del D.Lgs. n.231 del 2001, di cui il codice etico è parte integrante; regime disciplinare al quale spetta di prevedere sanzioni adeguate e proporzionate alla gravità delle eventuali infrazioni commesse, a prescindere dall'eventuale rilevanza penale dei comportamenti assunti e/o dell'instaurazione di un procedimento penale ove ricorra un reato. Il codice etico è voluto ed adottato dall'Organo Amministrativo, il quale deve promuovere la sua diffusione ed effettiva conoscenza fra tutti i destinatari. Di seguito è proposta un'indicazione dei principi generali e dei principali criteri di condotta comportamentale che possono rappresentare il punto di partenza per la costruzione *ex novo* di un codice etico ovvero per l'ampliamento di un codice etico eventualmente già esistente.

3.2 Principi generali

Diseguito si richiamano sinteticamente i principi etici cui le Associazioni ispirano le proprie scelte e le proprie norme di comportamento.

Rispetto delle norme previste dell'ordinamento giuridico
Il movimento associazionistico ha come principio imprescindibile il rispetto di leggi e regolamenti vigenti in tutti i paesi in cui esso opera. Pertanto ogni soggetto che compone l'organigramma aziendale dell'ente deve impegnarsi al rispetto delle leggi e dei regolamenti vigenti in tutti i
paesi in cui l'ente agisce. Tale impegno dovrà valere anche per i consulenti, fornitori ,clienti e chiunque abbia rapporti con l'ente. Quest'ultimo non inizierà o proseguirà nessun rapporto con chi non intende allinearsi a questo principio. L'ente dovrà assicurare un adeguato programma di formazione e di sensibilizzazione continua sulle problematiche attinenti al codice etico con particolare riguardo al rispetto delle norme di legge e regolamentari vigenti.

Onestà negli affari ed imparzialità
Ogni soggetto che compone l'organigramma aziendale dell'ente deve assumere un atteggiamento corretto ed onesto sia nello svolgimento delle proprie mansioni sia nei rapporticon gli altri componenti della Società evitando di perseguire scopi illeciti o illegittimi per procurarsi un indebito vantaggio proprio o di terzi. Tale impegno dovrà valere anche per i consulenti, fornitori, clienti e per chiunque abbia rapporti con la Associazione. In nessun caso l'interesse o il vantaggio dell'ente può indurre o giustificare

un comportamento disonesto. L'ente opera con imparzialità, evitando in ogni circostanza trattamenti di favore. Pertanto, l'ente esige che tutti i suoi componenti agiscano nei confronti dei vari portatori di interesse in modo da non compromettere l'indipendenza di giudizio e l'imparzialità propria e degli stessi. Al fine di garantire la piena attuazione dei principi di onestà ed imparzialità, non è ammessa alcuna forma di regalo o di omaggio, anche solo promessa, che possa essere intesa come eccedente le normali pratiche commerciali o di cortesia, o comunque finalizzata ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società.

Correttezza nella gestione societaria e nell'utilizzo delle risorse
L'ente persegue il proprio oggetto sociale, oltre che nell'imprescindibile rispetto della legge, anche nel rispetto scrupoloso dello Statuto e dei Regolamenti sociali, assicurando il corretto funzionamento degli organi sociali e la tutela dei diritti patrimoniali e partecipativi dei propri soci, salvaguardando l'integrità del capitale sociale e del patrimonio aziendale.

Trasparenza e completezza dell'informazione
L'ente riconosce il valore fondamentale della corretta informazione ai soci, agli organi ed alle funzioni competenti, in ordine ai fatti significativi concernenti la gestione societaria e contabile ed in alcun modo giustifica azioni dei propri collaboratori che impediscano il controllo da parte degli enti od organizzazioni preposte. L'ente favorisce un flusso di informazioni continuo, puntuale e completo fra gli organi sociali, le diverse aree aziendali, le varie figure apicali, gli organi ed enti di vigilanza, e, ove necessario, verso le Pubbliche Autorità. In ogni caso e informazioni trasmesse all'esterno e all'interno dell'organizzazione stessa sono rispettose dei requisiti di veridicità, completezza e accuratezza, anche in relazione a dati economici, finanziari e contabili.

Tracciabilità delle operazioni
Tutte le azioni e le operazioni dell'ente devono avere una registrazione adeguata e deve essere possibile la verifica del processo di decisione, autorizzazione e di svolgimento. Per ogni operazione vi deve essere un adeguato supporto documentale al fine di poter procedere in ogni momento all'effettuazione dei controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

Riservatezza delle informazioni
L'ente assicura la riservatezza delle informazioni in proprio possesso, l'osservanza della
normativa in materia dei dati personali e si astiene dal ricercare dati riservati attraverso mezzi illegali. Ogni soggetto che compone l'organigramma aziendale che a qualsiasi titolo entri in possesso di informazioni di interesse aziendale o relativamente a qualsiasi portatore d'interesse, in nessuna maniera si deve sentire autorizzato a diffonderla o utilizzarla al di fuori degli scopi operativi per cui è stato autorizzato dalle direzioni aziendali.

Prevenzione e gestione dei conflitti di interesse
L'ente previene o gestisce eventuali conflitti di interesse fra i propri soci, dipendenti, amministratori, collaboratori e la Pubblica Amministrazione, che coinvolgano l'attività stessa dell'ente. Al fine di prevenire e gestire correttamente eventuali situazioni di conflitto di interesse, anche solo potenziali, al momento di assegnazione dell'incarico o di avvio del rapporto di lavoro richiede ai propri amministratori, dipendenti e collaboratori a vario titolo di sottoscrivere un'apposita dichiarazione che esclude la presenza di condizioni di conflitto di interesse tra singolo e Società, o, in caso di esistenza di tali condizioni, ne chiarisca la natura.

Valore delle Risorse Umane
Si intendono come Risorse Umane tutti i componenti dell'organigramma aziendale (comprensivo di collaboratori continuativi), i consulenti, i soci, gli amministratori e tutti coloro che prestano la loro opera o partecipano a qualunque titolo alla scambio mutualistico o siano destinatari delle attività dell'ente in forme contrattuali diverse da quella del lavoro subordinato.
L'ente riconosce la centralità del portatore d'interesse "Risorse Umane" e l'importanza di stabilire e mantenere relazioni basate sulla lealtà e sulla fiducia reciproca, valorizzando quanto possibile le aspirazioni e le capacità del singolo. Ritiene, inoltre, di primaria importanza l'informazione e la formazione continua di tali Risorse, anche al fine di mantenere in capo a queste le competenze adeguate allo svolgimento delle massoni previste dall'organigramma aziendale. Per quanto riguarda i lavoratori, siano essi soci o meno, l'ente garantisce in ogni momento condizioni di lavoro rispettose della dignità individuale ed ambienti di lavoro sicuri ed applica ai propri dipendenti la legislazione ed i contratti di lavoro vigenti. Nella gestione dei rapporti gerarchici e disciplinari l'autorità è esercitata con equità, imparzialità e correttezza, evitando ogni abuso che possa ledere la dignità e la professionalità della persona.
E' vietata qualsiasi forma di favoritismo, clientelismo, nepotismo sia nella gestione che nella selezione del personale che deve essere scelto tenendo conto esclusivamente delle esigenze aziendali e del profilo professionale.

Spirito di servizio
Tutti i componenti dell'ente, nell'adempimento delle proprie funzioni, considerano costantemente propria la missione di fornire un bene di alto valore economico e sociale alla collettività; tale considerazione deve informare sempre la condotta dell'ente e di ciascun socio, amministratore, dipendente o collaboratore.

Responsabilità sociale
L'ente si impegna ad operare ricercando un continuo equilibrio fra i diversi interessi coinvolti, come lo sviluppo economico, il benessere sociale e della collettività, il rispetto dell'ambiente, la cultura della sicurezza e della prevenzione dei rischi. La responsabilità sociale dell'impresa porta al riconoscimento della pluralità di gruppi o categorie di interessi anche con riferimento alle conseguenze ed all'esternalità prodotta dall'attività di impresa.

Attenzione al territorio

L'ente è consapevole degli effetti della propria attività sul contesto di riferimento, sullo sviluppo economico e sociale e sul benessere generale della collettività e pone di conseguenza attenzione, nel proprio operato, a contemperare tali interessi. L'ente si impegna pertanto ad operare ricercando un continuo equilibrio fra i diversi interessi coinvolti,

come lo sviluppo economico, il benessere sociale e della collettività, il rispetto dell'ambiente, la cultura della sicurezza e della prevenzione dei rischi. L'ente considera altresì di elevata rilevanza le tematiche connesse all'ambiente, assicurando il pieno rispetto della normativa nazionale e comunitaria vigente in ogni fase produttiva. L'ente ritiene che il dialogo con i soggetti della società civile ed economica del territorio su cui opera sia di importanza strategica per un corretto sviluppo della propria attività e instaura, ove possibile, un canale stabile di dialogo con questi , allo scopo di cooperare nel rispetto dei reciproci interessi. L'ente è aperto all'interazione con le imprese sociali e del terzo settore in una logica dei valori dell'economia sociale, della promozione della persona ed del miglioramento della qualità di vita nei territori in cui opera.

Qualità e sicurezza dei prodotti
L'ente si impegna a persegue la propria missione attraverso l'offerta di servizi o prodotti di qualità, a condizioni competitive e nel rispetto di tutte le norme cogenti.
Lo stile di comportamento dell'ente nei confronti dei clienti è improntato alla disponibilità, al rispetto e alla cortesia, nell'ottica di un rapporto collaborativo e di elevata professionalità. In particolare, nella comunicazione con i clienti, l'ente assicura completezza, correttezza e chiarezza di tutte le informazioni inerenti caratteristiche, contenuti, natura e provenienza dei prodotti. L'ente assicura l'immissione nel mercato di servizi o prodotti conformi alle leggi nazionali e comunitarie in materia, attivando tutti i controlli necessari a garantire ai consumatori sicurezza e qualità.

3.3 Criteri di condotta

3.3.1 Criteri di condotta nei rapporti con Pubblica amministrazione, pubblici dipendenti, pubblici ufficiali o incaricati di pubblico servizio.

I rapporti attinenti all'attività dell'ente intrattenuti con pubblici ufficiali od incaricati di pubblico servizio (che operino per conto della Pubblica Amministrazione, centrale e periferica, o di organi legislativi, delle istituzioni comunitarie, di organizzazioni pubbliche internazionali e di qualsiasi Stato estero), con la magistratura, con le Autorità pubbliche di vigilanza e con altre Autorità indipendenti, nonché con *partners* privati concessionari di un pubblico servizio, devono essere intrapresi e gestiti nell'assoluto e rigoroso rispetto delle leggi e delle normative vigenti in modo da non compromettere l'integrità e la reputazione di entrambe le particolo L'ente vieta, ai propri dipendenti, collaboratori, soci, amministratori o rappresentanti e, più in generale, a tutti coloro che operano nel suo interesse, in suo nome o per suo conto, di promettere od offrire, anche indirettamente, denaro, doni, beni, servizi, prestazioni o favori non dovuti (anche in termini di opportunità di impiego), in relazione a rapporti intrattenuti con pubblici ufficiali, incaricati di pubblico servizio o dipendenti, in genere, della Pubblica Amministrazione o di altre Pubbliche Istituzioni, o anche con soggetti privati, al fine di influenzarne le decisioni, in vista di trattamenti più favorevoli o prestazioni indebite o per qualsiasi altra finalità. Sono consentiti doni di modico valore nei limiti delle normali pratiche commerciali o di cortesia, che non possano in alcun modo influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'ente. I doni di modico valore devono essere comunque documentati in modo adeguato per consentire le verifiche alla funzione competente. Qualsiasi dipendente, collaboratore, socio, amministratore che riceva, direttamente o indirettamente, richieste di denaro o di favori di qualunque tipo (ivi compresi omaggi o regali di non modico valore) formulate da pubblici funzionari, incaricati di pubblico servizio o dipendenti in genere della Pubblica Amministrazione (italiana o di altri paesi esteri) o di altre Pubbliche Istituzioni, o da soggetti privati (italiani o esteri), deve immediatamente riferire alla funzione competente per l'assunzione dei provvedimenti conseguenti. Ogni rapporto con le istituzioni dello Stato o internazionali deve, pertanto, essere riconducibile esclusivamente a forme di comunicazione ed interazione volte ad attuare l'oggetto sociale dell'ente, a rispondere a richieste o ad atti di sindacato ispettivo, o comunque a rendere nota la posizione o situazione dell'ente.

A tal fine, l'ente:
- opera esclusivamente attraverso i canali di comunicazione a ciò preposti con gli interlocutori Istituzionali a livello nazionale e internazionale, comunitario e territoriale;
- non sollecita o cerca di ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe la parti;
- rappresenta i propri interessi e posizioni in maniera trasparente, rigorosa e coerente, evitando atteggiamenti di natura collusiva;
- impedisce falsificazioni e/o alterazioni dei rendiconti o dei dati documentali al fine di ottenere un indebito vantaggio o qualsiasi altro beneficio;
- compie uno scrupoloso controllo dei dati contenuti nelle dichiarazioni rivolte agli enti pubblici;
- persegue il pieno rispetto delle condizioni e delle tempistiche previste nel contratti stipulati con la Pubblica Amministrazione.

Gestione Appalti e Contratti Pubblici
L'ente, nella partecipazione a gare di appalto o a negoziazioni per contratti di lavoro, forniture e servizi della Pubblica Amministrazione, adotta condotte improntate ai principi di buona fede, correttezza professionale, lealtà, e legalità verso gli enti pubblici e verso gli altri soggetti concorrenti. Nella gestione e partecipazione ad appalti pubblici o comunque a contratti e convenzioni con la Pubblica Amministrazione, l'ente opera nel pieno rispetto della normativa vigente italiana ed europea. L'ente si astiene dal tener comportamenti anticoncorrenziali, cioè comportamenti ingannevoli, fraudolenti o sleali contrari alla libera concorrenza, e censura qualsiasi tentativo volto a influenzare chi opera per conto della Pubblica Amministrazione al fine di ottenere un atteggiamento di favore nei confronti dell'ente stesso.

3.3.2 Criteri di condotta nei rapporti con clienti privati e fornitori.
Lo stile di comportamento dell'ente nei confronti dei clienti e dei fornitori è improntato alla disponibilità, al rispetto ed alla cortesia, nell'ottica di un rapporto collaborativo e di elevata professionalità. L'ente persegue la propria missione attraverso l'offerta di servizi di qualità, a condizioni competitive e nel rispetto di tutte le norme poste a tutela della leale concorrenza tra imprese. La selezione dei fornitori e la determinazione delle condizioni di acquisto avvengono sulla base di parametri obiettivi quali la qualità, la convenienza, il prezzo, la capacità, l'efficienza, l'eticità, il rispetto della legge. L'acquisto di prodotti o di servizi deve in ogni caso risultare conforme ed essere giustificato da concrete e motivate esigenze aziendali, nell'ottica di garantire la massima trasparenza ed efficienza del processo

di acquisto; l'ente predispone un'adeguata rintracciabilità delle scelte adottate. La condivisione del codice etico adottato dall'ente rappresenta presupposto necessario per l'instaurazione e il mantenimento del rapporto di fornitura. E' fatto espresso divieto ai componenti dell'ente di richiedere o pretendere dai fornitori favori, doni o altre utilità, ovvero di dare o promettere loro analoghe forme di riconoscimento, ancorchè finalizzate ad una ottimizzazione del rapporto con l'ente. Quanto sopra si applica anche ai rapporti con consulenti esterni ed *outsourcers* .

3.3.3 Criteri di condotta nei rapporti con il personale e i collaboratori.

Tutela della dignità
L'ente è impegnato nel garantire a tutti i suoi componenti la tutela della dignità e dell'integrità psicofisica nel rispetto dei principi di pari opportunità e di tutela della *privacy* , con speciale riguardo ai soggetti svantaggiati e disabili.

Selezione e assunzione del personale
La valutazione del personale da assumere è effettuata in base alla corrispondenza dei profili dei candidati rispetto alle esigenze dell'ente, nel rispetto dei principi di imparzialità e di pari opportunità per tutti i soggetti interessati. Tutto il personale viene assunto con regolare contratto di lavoro nelle forme previste; non è consentita alcuna forma di lavoro irregolare , nè da parte dell'ente né da parte di Società controllate, fornitori, subappaltatori, collaboratori. Nel momento in cui inizia la collaborazione, il dipendente/collaboratore riceve esaurienti informazioni riguardo alle caratteristiche delle mansioni e della funzione assegnata, riguardo agli elementi normativi e retributivi, alle normative ed ai comportamenti per la gestione dei rischi connessi alla salute personale, ed infine riguardo ai comportamenti eticamente accettati e richiesti dall'ente, tramite consegna del Codice Etico.

Gestione del rapporto
E' proibita qualsiasi forma di discriminazione nei confronti delle persone. Tutte le decisioni prese nell'ambito della gestione e dello sviluppo delle risorse umane sono basate su considerazioni di profili di merito e/o corrispondenza tra profili attesi e profili posseduti dai dipendenti /collaboratori. Nella gestione dei rapporti gerarchici l'autorità è esercitata con equità e correttezza, evitandone ogni abuso. Tutti i dipendenti/collabor atori si impegnano ad agire lealmente al fine di rispettare gli obblighi assunti col contratto di lavoro e quelli contemplati nel Codice Etico, assicurando le prestazioni che sono loro richieste e rispettando gli impegni assunti.

Divieto di accettare / promettere doni o altre utilità

Tutti coloro i quali operano per conto dell'ente non sono autorizzati ad offrire, accettare o promettere, per se per altri, alcuna forma di dono, compenso, utilità o servizio di qualsiasi natura rivolta ad influenzare o comunque realizzare trattamenti di favore nel corso dello svolgimento delle proprie mansioni.

Conflitti di interesse
Ogni dipendente e collaboratore dell'ente è tenuto ad evitare tutte le situazioni e tutte le attività in cui si possa manifestare un conflitto con gli interessi dell'ente o che possano comunque interferire con la propria capacità di assumere, in modo imparziale, decisioni nel migliore interesse dell'impresa e nel pieno rispetto delle norme del Codice Etico.

Deve, inoltre, astenersi dal trarre vantaggio personale da atti di disposizione dei beni sociali o da opportunità d'affari delle quali è venuto a conoscenza nel corso dello svolgimento delle proprie funzioni. Ogni situazione che possa costituire o determinare un conflitto di interesse deve essere tempestivamente comunicata da ogni dipendente o collaboratore al proprio superiore o referente aziendale.

Salute e Sicurezza sul lavoro
L'ente deve esplicitare chiaramente e rendere noti mediante un documento formale i principi ed i criteri fondamentali in base ai quali vengono prese le decisioni di ogni tipo e da ogni livello in materia di salute e sicurezza sul lavoro; tali principi e criteri possono così individuarsi:

- evitare i rischi,
- valutare i rischi che non possono essere evitati,
- combattere i rischi alla fonte,
- adeguare il lavoro all'uomo, in particolare per quanto concerne la scelta dei luoghi, delle attrezzature e dei metodi di lavoro e produzione, al fine di eliminare ogni effetto nocivo del lavoro sulla salute;
- tenere conto del grado di evoluzione della tecnica;
- sostituire ciò che è pericoloso con ciò che non è pericoloso o che lo è meno;
- programmare la prevenzione mirando ad un complesso coerente che integri nella medesima la tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro;
- dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale;
- impartire adeguate istruzioni ai lavoratori.

Tali principi sono utilizzati dall'impresa per prendere le misure necessarie per la protezione della sicurezza e salute dei lavoratori, comprese le attività di prevenzione dei rischi professionali, di informazione e formazione, nonché l'approntamento di una organizzazione e dei mezzi necessari. L'azienda sia ai livelli apicali che a quelli operativi deve attenersi a questi principi, in particolare quando devono essere prese delle decisioni o fatte delle scelte e in seguito quando le stesse devono essere attuate.

3.3.4 Criteri di condotta nei rapporti con i soci.
L'ente crea le condizioni affinché la partecipazione dei soci alle decisioni di loro competenza sia diffusa e consapevole, garantendo la completezza di informazione, la trasparenza e l'accessibilità ai dati ed alla documentazione, secondo i principi di legge ed in particolare operando per la concreta attuazione del principio democratico proprio delle Associazioni. L'ente

promuove ed attua la parità di trattamento tra i soci e tutela il loro interesse alla migliore attuazione e valorizzazione dello scambio mutualistico. L'ente vigila affinché i soci non si pongano in contrasto con gli interessi sociali, perseguendo interessi propri o di terzi estranei o contrari all'oggetto sociale, od operando in modo antitetico e confliggente con esso.

3.3.5 Criteri di condotta nei rapporti con organizzazioni politiche, sociali, e sindacali.
L'ente, nel fornire eventuali contributi a partiti, movimenti, comitati ed organizzazioni politiche e sindacali, a loro rappresentanti e candidati, adotta procedure e forme documentate, tracciate e conformi alla normativa vigente. In ogni caso tali contributi sono slegati da qualsiasi interesse, diretto o indiretto, dell'ente ad ottenere agevolazioni, turbative, trattamenti di favore. In nessun caso i suddetti contributi saranno elargiti in un'ottica di reciprocità, escludendosi dunque ogni forma di scambio politico.

3.3.6 Criteri di condotta nei rapporti con i mass media e diffusione delle informazioni.
I rapporti con la stampa, i mezzi di comunicazione ed informazione e, più in generale, con gli interlocutori esterni, devono essere tenuti solo da soggetti espressamente a ciò delegati, in conformità alle procedure e politiche adottate dall'ente. Le comunicazioni verso l'esterno seguono i principi guida della verità, correttezza, trasparenza, prudenza e sono volte a favorire la conoscenza delle politiche aziendali e dei programmi e dei progetti della Società.

3.4 Sistema disciplinare.

3.4.1. Principi generali.

L'efficacia e l'effettività del Modello Organizzativo e del Codice Etico, sono strettamente connesse alla predisposizione di un adeguato sistema sanzionatorio cui affidare una duplice funzione:

- sanzionare in termini disciplinari, *ex post*, le violazioni del Codice Etico e delle procedure previste dal Modello Organizzativo;
- stigmatizzare e quindi prevenire la realizzazione di condotte inosservanti, attraverso la minaccia della sanzione disciplinare.

La previsione di una sanzione disciplinare per un determinato comportamento deve rispondere ad esigenze di proporzionalità connesse alla concreta gravità del fatto. E' chiaro che deve esservi, comunque, un riscontro in termini di effettività. Anche nel caso di violazioni poco rilevanti, deve essere comunque prevista una sanzione dotata di un'adeguata efficacia deterrente. L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia e indipendente dalla tipologia di illecito che le violazioni del Modello possano determinare. In caso di accertata violazione del Modello o del Codice Etico, l'Organismo di Vigilanza (O.d.V.) riporta la segnalazione e richiede l'applicazione di eventuali sanzioni ritenute necessarie all'Organo Amministrativo ed alla direzione aziendale, quando esistente ed investita di corrispondete delega. Deve essere inoltre informato il Collegio Sindacale, quando costituito. L'Organo Amministrativo e la competente funzione aziendale approvano i provvedimenti da adottare, anche a carattere sanzionatorio, secondo le normative in vigore, ne curano l'attuazione e riferiscono l'esito all'Organismo di Vigilanza. Qualora non venga comminata la sanzione proposta dall'Organismo di Vigilanza, l'Organo Amministrativo ne dovrà dare adeguata motivazione all'Organismo stesso ed al Collegio Sindacale, quando costituito. L'ente, insieme al Codice Etico ed al Modello,deve adeguatamente pubblicizzare anche il sistema disciplinare, affinché tutti i portatori di interesse abbiano piena conoscenza delle conseguenze connesse al compimento di condotte vietate dal Codice Etico o difformi rispetto alle procedure stabilite nel Modelli Organizzativo.

3.4.2. Sanzioni per i lavoratori dipendenti.
I comportamenti tenuti dai lavoratori dipendenti, siano o meno essi soci, in violazione delle singole regole comportamentali dedotte nel Codice Etico e nel Modello, sono da intendersi come illeciti disciplinari; tali regole vanno pertanto espressamente inserite nel regolamento disciplinare aziendale, se esistente, o comunque formalmente dichiarate vincolanti per tutti i lavoratori nonché esposti, così come previsto dall'articolo 7 della Legge 30 maggio 1970, n. 300(Statuto Lavoratori); esse andranno affisse in luogo accessibile a tutti evidenziando esplicitamente le sanzioni collegate alle diverse violazioni. In relazione alla tipologia delle sanzioni è opportuno fare riferimento all'apparato sanzionatorio previsto nei Contratti Collettivi Nazionali vigenti e applicabili all'ente. Qualsiasi provvedimento deve rispettare le procedure previste dal citato articolo 7 della legge n.300 del 1970 e /o normative speciali applicabili.

3.4.3 Misure nei confronti degli Amministratori.
In caso di violazione del Modello da parte di singoli Amministratori della Società, l'Organismo di Vigilanza ne informerà l'Organo Amministrativo ed il Collegio Sindacale, ove esistente, i quali, valutata la segnalazione in un'apposita adunanza da convocarsi nel più breve tempo possibile, provvederanno ad assumere le opportune iniziative avendo come riferimento la vigente normativa societaria nonchè lo Statuto Sociale. Quando la società è amministrata da un Amministratore Unico, l'Organismo di Vigilanza potrà procedere ad informare, oltre al Collegio Sindacale laddove esistente, anche i singoli soci affinché adottino le opportune iniziative previste dallo Statuto e dalla vigente normativa societaria.

3.4.4 Misure nei confronti dei soci.

In caso di violazione del Modello da parte dei soci della Società, l'Organismo di Vigilanza ne informerà l'Organo Amministrativo il quale provvederà ad assumere le opportune iniziative previste dalla vigente normativa e dallo Statuto Sociale, ivi compresa l'esclusione da socio.

3.4.5 Misure nei confronti di collaboratori, consulenti e fornitori.
Ogni comportamento posto in essere dai collaboratori, consulenti o fornitori in contrasto con le

linee di condotta indicate dal Modello e dal Codice Etico, tale da comportare il rischio di commissione di un reato sanzionato dal D.Lgs. n. 231/2001, potrà determinare, mediante l'attivazione di opportune clausole, la sospensione del rapporto contrattuale e delle attività conseguenti, nonché l'applicazione di eventuali penali conseguenti alla sospensione dell'attività, fino a giungere alla risoluzione dei contratti e fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento siano derivati danni concreti all'ente, come nel caso di applicazione da parte del Giudice delle misure previste dal Decreto. L'Organismo di Vigilanza curerà l'elaborazione, l'aggiornamento e l'inserimento nelle lettere di incarico o, più in generale, negli accordi con i collaboratori e *partners*, delle succitate specifiche clausole contrattuali.

Capitolo IV: L'Organismo di Vigilanza

4.1 Premessa.

L'articolo 6 del D.Lgs. n. 231/2001 affida il compito di vigilare sul funzionamento e l'osservanza dei modelli organizzativi e di curare il loro aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (articolo 6, lett. *b*, D.Lgs. n. 231/2001). L'esistenza di un tale organismo è condizione necessaria, insieme all'efficace adozione ed applicazione del Modello Organizzativo, affinché l'ente goda dell'esonero dalla responsabilità conseguente alla commissione dei reati di cui al Decreto. Si sottolinea che l'organismo in parola non deve essere inteso come un nuovo organo sociale (al pari dell'Organo Amministrativo o del Collegio Sindacale), bensì quale parte integrante del sistema di controllo interno all'impresa.

4.2 Nomina.

L'Organismo di Vigilanza è istituito con delibera dell'Organo Amministrativo e, tenuto conto della dimensione e complessità organizzativa della singola realtà aziendale, può essere a composizione plurisoggettiva o monocratica. Fatto salvo il rispetto dei requisiti di autonomia, indipendenza, professionalità, continuità d'azione ed onorabilità, possono essere chiamati a far parte dell'Organismo sia componenti esterni che interni all'ente. Negli enti di piccole dimensioni le funzioni dell'Organismo di Vigilanza possono essere svolte direttamente dall'Organo Amministrativo. La delibera deve prevedere come contenuto minimo: la determinazione della composizione dell'Organismo e dei requisiti soggettivi dei suoi componenti (fornendo un'adeguata motivazione delle scelte operate), la durata dell'incarico, l'eventuale compenso per i componenti, l'elencazione dei compiti e dei poteri affidati, le cause di ineleggibilità e decadenza dall'incarico, i meccanismi di sostituzione dei componenti in caso di decadenza o dimissioni, nonché uno specifico ed autonomo potere di spesa che garantirà l'autonomia d'azione. Quest'ultimo aspetto, che potrebbe apparire soprattutto per le Associazioni di piccole dimensioni un ostacolo all'istituzione dell'O.d.V. , può essere circoscritto con la definizione di un budget prefissato. Resta inteso che l'Organismo di Vigilanza non è obbligato ad attingervi, ma deve essere posto nella condizione di gestire il budget prefissato qualora necessiti dell'apporto di consulenti o professionisti esterni al fine di svolgere la propria attività di controllo, o ancora per acquisire eventuali pareri da personale esperto. E' ovvio che quanto più sono i soggetti (e le professionalità) presenti nell'O.d.V. , tanto più remota diviene la necessità di incaricare professionisti esterni per consulenze *ad hoc* .

4.3 Requisiti.

In base a quanto disposto dagli articoli 6, comma 1, lett. *b)* e 7, commi 3 e 4 del D.Lgs. n. 231/2001, l'Organismo di Vigilanza deve possedere requisiti di: autonomia e indipendenza, professionalità, continuità d'azione e onorabilità. Autonomia: deve essere assicurata all'O.d.V. completa autonomia, intesa come libera capacità decisionale, di autodeterminazione e di azione, on pieno esercizio della discrezionalità tecnica nell'esercizio delle proprie funzioni. Tale autonomia va esercitata soprattutto rispetto ai vertici societari, nel senso che l'Organismo dovrà rimanere estraneo a qualsiasi forma di interferenza e pressione da parte dei vertici stessi e non dovrà in alcun modo essere coinvolto nell'esercizio di attività di gestione che esorbitino dai compiti specificamente assegnati in funzione della propria attività. Il requisito va inteso in senso sostanziale e non meramente formale, ed è pertanto dimostrato dall'attribuzione di specifici poteri e funzioni nonché di una certa autonomia patrimoniale (ad esempio, come sopra detto, con la dotazione iniziale diun budget preventivamente deliberato dall'Organo Amministrativo). L'autonomia comporta infine la possibilità per l'organismo di vigilanza di autodeterminarsi fissando le proprie regole comportamentali e procedurali per il tramite di un regolamento dallo stesso adottato.

Indipendenza: La posizione dell'Organismo di Vigilanza deve essere quella di un organismo terzo gerarchicamente collocato al vertice della linea di comando, libero da legami di sudditanza rispetto al vertice aziendale, capace di adottare provvedimenti ed iniziative insindacabili. Nel caso di O.d.V. a composizione plurisoggettiva, i singoli componenti non dovrebbero svolgere funzioni operative all'interno della società e, se questo si verifica, si devono individuare soluzioni che garantiscano comunque l'autonomia in senso collegiale dell'Organismo. Nell'ipotesi di O.d.V. monocratico, e qualora sia nominato un componente interno all'ente, l'assenza di situazioni di conflitto di interesse dovrebbe essere scrupolosamente valutata sia con riguardo alla titolarità di compiti operativi che di eventuali funzioni di controllo già esercitate nell'ambito dell'ente.

Professionalità: Il requisito della professionalità assume connotati prettamente soggettivi, che andranno verificati per ciascun componente, con una preventiva analisi del *curriculum vitae* e delle concrete esperienze lavorative di ognuno di essi. In particolare, secondo la giurisprudenza prevalente, occorre che l'O.d.V. sia composto da soggetti dotati di specifiche conoscenze in materia di metodologie ed attività di controllo, valutazione e gestione dei rischi, organizzazione aziendale, finanza, revisione e gestione, pratica professionale legale, oltre che capacità specifiche in relazione all'attività ispettiva e consulenziale.

Continuità d'azione: La continuità d'azione va intesa in termini di effettività dell'attività di vigilanza e controllo ed in termini di costanza temporale dello svolgimento delle funzioni dell'O.d.V. Pertanto, per parametrare il requisito in parola si dovrà fare riferimento alla dimensione e complessità organizzativa della singola realtà aziendale, non escludendo che nelle realtà di grandi dimensioni si renda necessaria la presenza di una struttura dedicata
esclusivamente ed a tempo pieno all'attività di vigilanza sul Modello.

Onorabilità: I componenti dell'Organismo di Vigilanza, visto il ruolo che sono chiamati a ricoprire, devono presentare necessariamente un profilo etico di indiscutibile valore; in particolare, il regolamento di disciplina del funzionamento dell'O.d.V. deve prevedere

specifiche cause di ineleggibilità e decadenza, che, secondo la giurisprudenza, non possono risolversi solamente nella condanna con sentenza passata in giudicato per aver commesso uno dei reati di cui al D.Lgs 231/2001 ovvero nella la condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche o delle imprese. Limitando le cause di ineleggibilità o decadenza a tali ipotesi estreme, si arriverebbe alla conseguenza logica di poter nominare quale membro dell'organo di vigilanza *"un soggetto condannato – seppure con sentenza non irrevocabile - per corruzione, per truffa aggravata ai danni di ente pubblico, per frode fiscale ovvero un soggetto nei confronti del quale sia stata emessa sentenza di patteggiamento divenuta irrevocabile ad esempio per gravi fatti corruttivi".*

4.4 Composizione e configurazione.

Alla luce di quanto sopra rilevato si deve escludere che, al di fuori dell'ipotesi di enti di piccole dimensioni, le funzioni di O.d.V. possano essere svolte dall'Organo Amministrativo (sia esso Consiglio di Amministrazione o Amministratore Unico) o dalle funzioni aziendali interne come quella di amministrazione o di direzione del personale, o dall'ufficio legale interno, o, ancora, del controllo di qualità, in quanto queste tutte difettano dei requisiti di autonomia e indipendenza. Parimenti la dottrina maggioritaria esclude (o quanto meno reputa fortemente inopportuno) che il Collegio Sindacale possa esercitare le funzioni di O.d.V. , non potendo esso soddisfare il requisito della continuità d'azione. Inoltre il Collegio Sindacale è un organo non obbligatorio nelle realtà societar ie di piccole o medie dimensioni. Con particolare riguardo alle Associazioni, si rileva che stante quanto previsto dall'articolo 2543 del codice civile la nomina del collegio è obbligatoria nei soli casiprevisti dal secondo comma e terzo comma dell'art 2477 (vale a dire se il capitale sociale non è inferiore a quello minimo stabilito per le società per azioni, attualmente 120.000 euro, ovvero se per due esercizi consecutivi siano stati superati due dei limiti indicati dal primo comma dell'articolo 2435 *bis:* 1) totale dell'attivo dello stato patrimoniale superiore ai 4.400.000 euro;
2) ricavi delle vendite e delle prestazioni: superiori agli 8.800.000 euro;
3) dipendenti occupati in media durante l'esercizio superiori alle 50 unità).

In ogni caso, il Collegio Sindacale resta uno degli interlocutori privilegiati dell'Organismo di Vigilanza, essendo esso istituzionalmente investito del compito di vigilare sull'adeguatezza del sistema amministrativo, organizzativo e contabile della società e sul suo corretto funzionamento. Pertanto il Collegio, ove presente, dovrà essere sempre informato dell'eventuale commissione di reati, così come di eventuali carenze del Modello. E in presenza di casi rientranti nella patologia aziendale , l'O.d.V. potrà chiedere al Collegio di attivare i poteri allo stesso riconosciuti dalla legge. Problema diverso è quello relativo alla possibilità che dell'O.d.V. in composizione plurisoggettiva faccia parte un membro del Collegio Sindacale. Accogliendo una prassi diffusa si ritiene che a tale eventualità non si frapponga in linea di principio alcun ostacolo in quanto i singoli Sindaci dovrebbero essere in possesso, *ex lege* , dei requisiti di professionalità e onorabilità. Sulla base delle considerazioni sopra esposte appare evidente l'opportunità di nominare quale Organismo di Vigilanza, negli enti che non possono definirsi di piccole dimensioni, un soggetto giuridico *ad hoc* che sia caratterizzato nel suo complesso dai requisiti di autonomia e indipendenza, professionalità, continuità d'azione ed onorabilità. Come anticipato la configurazione di questo soggetto giuridico può essere monocratica ovvero plurisoggettiva. La giurisprudenza ha chiarito in più occasioni che la composizione dell'O.d.V. va determinata in base alla organizzazione ed alle dimensioni aziendali.
L'opzione per la composizione monocratica pare praticabile in enti che si caratterizzano per:
a) ridotta articolazione della struttura organizzativa e societaria,
b) processi aziendali non numerosi e di semplice monitoraggio,
c) profili rischio reato, accertati nel processo di mappatura delle aree sensibili, non altamente differenziati.

In presenza di tali condizioni può essere valutata la nomina di un Organismo di Vigilanza monocratico. Tale scelta comporta necessariamente un'attenta valutazione da parte dell'Organo Amministrativo circa il possesso in capo all'incaricato dei requisiti di autonomia, indipendenza, onorabilità e professionalità nonché della continuità d'azione. In particolare, è in ogni caso opportuno prevedere che l'Organismo di Vigilanza monocratico si avvalga strutturalmente sia di consulenti esterni, per integrare gli aspetti di professionalità, sia di funzioni aziendali interne all'ente che ne supportino in via continuativa l'azione fornendo altresì l'indispensabile conoscenza dell'ente stesso. In tutti i casi i cui l'ente, in virtù della maggiore complessità sotto il profilo della struttura organizzativa e dei profili di rischio reato nelle aree sensibili ovvero per semplice preferenza, si orienti verso un Organismo plurisoggettivo, la composizione potrà essere:
a) di soggetti completamente esterni oppure,
b) preferibilmente, mista, che raccolga cioè al tempo stesso figure interne all'organizzazione (con particolare riguardo ai titolari di funzioni aziendali in grado di assicurare adeguata conoscenza su organizzazione, processi e funzionamento dell'ente) e soggetti esterni (necessari a garantire l'indispensabile indipendenza, autonomia e competenza sulle problematiche legate all'applicazione del modello) ed eventualmente, ove presenti, Amministratori indipendenti, nel senso che non intrattengano direttamente o indirettamente con la Società o con gli Amministratori esecutivi relazioni economiche di rilevanza tale da condizionare la loro autonomia di giudizio. In particolare, la maggioranza dei componenti dovrà essere costituita da professionisti esterni ed Amministratori indipendenti (laddove presenti), e ciò come precondizione necessaria ad assicurare l'idoneità stessa della composizione dell'O.d.V . Ovviante dovrà esser garantita, non solo formalmente ma anche sostanzialmente, in capo all'Organismo nel suo complesso, la sussistenza dei requisiti di autonomia ed indipendenza nonché in capo a ciascun componente la presenza dei requisiti di professionalità e di onorabilità.
Una particolare disciplina è riservata dall'articolo 6 comma quarto del Decreto n. 231/2001 agli enti di "piccole dimensioni" nei quali la funzione di Organismo di Vigilanza può essere svolta direttamente dall'Organo dirigente. Con questa norma, di difficile interpretazione, il legislatore ha voluto venire incontro alle esigenze di enti che si caratterizzano per una struttura elementare e che difficilmente potrebbero sostenere la complessità ed i costi normalmente conseguenti all'adozione di un organismo di vigilanza *ad hoc*, anche se in configurazione monocratica, con le caratteristiche sopra individuate.

E' necessario sottolineare come l'adozione di una struttura estremamente elementare, in enti a base societaria aperta come le Associazioni con una base sociale tendenzialmente
più ampia rispetto alle società commerciali non quotate, debba sempre trovare una precisa giustificazione in relazione all'aspetto dimensionale dell'ente, nel senso che deve essere adeguata rispetto alle concrete esigenze organizzative ed amministrative,

all'ambito operativo ed al relativo livello reddituale. Ciò comporta che laddove sia presente un Organo Amministrativo collegiale, questo dovrà periodicamente effettuare una valutazione dell'adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società, ai sensi dell'articolo 2381 terzo comma del codice civile. In termini operativi, nel caso in cui sia presente un Organo Amministrativo collegiale, l'ente di piccole dimensioni che volesse avvalersi della facoltà in discorso potrebbe costituire un O.d.V. formato da uno o più degli Amministratori non esecutivi, vale a dire senza deleghe né formali né di fatto, e dove possibile, indipendenti. In questo caso, come nel caso che l'O.d.V. coincida con l'Amministratore unico, tenuto conto delle molteplici responsabilità ed attività cui quotidianamente l'Organo dirigente deve dedicarsi, è auspicabile ritenere che, nell'assolvimento di questo ulteriore compito, esso si avvalga di professionisti esterni, ai quali affidare l'incarico di effettuare periodiche verifiche sul rispetto e l'efficacia del modello. E' necessario chiarire che i compiti delegabili al consulente esterno sono quelli relativi allo svolgimento di tutte le attività di carattere tecnico, fermo restando l'obbligo dei professionista esterno di riferire all'Organo dell'ente. E' evidente,infatti, che l'affidamento di questo tipo di delega non fa venir meno la responsabilità di tale Organo in ordine alla funzione di vigilanza ad esso conferita dalla legge.

4.5 Poteri e funzioni.

A norma dell'articolo 6 del D.Lgs. n. 231/2001 l'O.d.V. ha *"il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento"*. A uesta breve affermazione corrispondono in realtà una serie articolata di funzioni e poteri che l'Organismo di Vigilanza si vede attribuiti direttamente dall'Organo Amministrativo. In particolare, sul piano generale, all'Organismo di Vigilanza vengono affidati i seguenti compiti:

- vigilare sulla corretta attuazione del Modello da parte dei destinatari;
- verificare l'adeguatezza e l'efficacia del Modello, con particolare attenzione all'identificazione delle aree "a rischio" reato, e dalla idoneità delle procedure adottate ai fini della prevenzione dei reati rilevanti per il D.Lgs. n. 231/2001;
- promuovere ed assicurare un'adeguata diffusione e conoscenza del Modello nei confronti dei destinatari dello stesso;
- verificare lo stato di aggiornamento del Modello, segnalando con tempestività all'Organo Amministrativo la necessità di procedere alle integrazioni ed agli aggiornamenti da eseguire a seguito della modificazione della normativa di riferimento e/o della struttura aziendale.

Tali compiti generali si declinano, poi, nell'attribuzione all'Organismo di Vigilanza di specifiche funzioni:

- condurre ricognizioni delle attività aziendali ai fini della "mappatura" aggiornata delle aree di attività a rischio nell'ambito del contesto aziendale;
- attivare leprocedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al *management* operativo e forma parte integrante del processo aziendale;
- promuovere adeguate iniziative per la diffusione dellaconoscenza e della comprensione del Modello e predisporre la documentazione organizzativa interna necessaria, contenente istruzioni, chiarimenti o aggiornamenti relativi al Modello stesso;
- instaurare e mantenere canali di comunicazione costanti con le diverse figure apicali delle aree a rischio;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di attività a rischio;
- raccoglier e, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere allo stesso Organismo di Vigilanza obbligatoriamente trasmesse o tenute a sua disposizione;
- coordinarsi con le altre funzioni aziendali, anche attraverso apposite riunioni, per migliorar il monitoraggio delle attività nelle aree di rischio nonchè per i diversi aspetti attinenti l'attuazione del Modello (definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, etc.); • controllare la presenza, l'effettività e la regolare tenuta della documentazione richiesta in conformità a quanto previsto dalle procedure operative che entrano a far parte del Modello o che siano da esso richiamate. In particolare devono essere messi a disposizione dell'O.d.V. tutti i dati possibili al fine di consentire l'effettuazione dei controlli;
- condurre le indagini interne per l'accertamento di presunte violazioni alle prescrizioni del Modello e del Codice Etico;
- verificare che gli elementi previsti dal Modello siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a fornire indicazioni di indirizzo per un corretto aggiornamento degli elementi stessi;
- in presenza di violazioni del Modello, o suo mancato adeguamento, da parte dei destinatari o dei responsabili delle funzioni aziendali competenti, così come in presenza di mancato adeguamento alle prescrizioni indicate dall'O.d.V. , procedere alla segnalazione all'Organo Amministrativo per l'adozione degli opportuni provvedimenti.

4.6 Regolamento di funzionamento.

L'Organismo di Vigilanza, per svolgere al meglio i propri compiti, dovrà dotarsi di apposito Regolamento che ne disciplini il concreto funzionamento. ale Regolamento dovrà prevedere l'obbligo dell'O.d.V. di riunirsi periodicamente ed in modo continuativo, ad esempio con cadenza mensile o bimestrale, salvo esigenze straordinarie. Vanno definite inoltre le modalità di convocazione (scritta, via fax, via mail, con un minimo di giorni di anticipo ecc.), ed i soggetti abilitati a richiederla in via straordinaria, segnatamente l'Organo Amministrativo ed il Collegio Sindacale, sia collegialmente sia da parte dei suoi singoli componenti. Le convocazioni dovranno avvenire in forma scritta e contenere l'ordine del giorno della riunione stilato in maniera concordata tra i membri dell'O.d.V. o dal preposto alla Presidenza dell'O.d.V. stesso. Tali convocazioni potranno essere inviate per conoscenza anche alla Presidenza dell'Organo Amministrativo ed alla Presidenza del Collegio Sindacale. Andranno inoltre regolamentate le condizioni di validità delle riunioni (es, presenza della maggioranza dei componenti) e delle votazioni (es. maggioranza con attribuzione di un voto a ciascun membro). L'attività svolta durante le riunioni dell'Organismo di Vigilanza deve essere registrata e formalizzata tramite verbali approvati entro lasuccessiva riunione, al fine di conservare sempre traccia delle tematiche affrontate e delle eventuali decisioni deliberate. Tutti i verbali approvati andranno conservati presso la sede aziendale unitamente a tutta la documentazione necessaria a dare evidenza oggettiva dell'attività espletata. E' importante garantire la massima riservatezza delle informazioni pervenute o raccolte dall'Organismo, e delle discussioni instaurate durante le riunioni, ciò a tutela della *privacy* dei soggetti eventualmente coinvolti e della assoluta autonomia e professionalità dell'Organismo stesso. E' necessario, inoltre, stabilire un obbligo

di relazione da parte dell'O.d.V. nei confronti dell'Organo Amministrativo e del Collegio Sindacale, ove esistente, sulla propria attività. Tali relazioni dovranno avere una frequenza almeno semestrale, in base a specifiche indicazioni provenienti dalla giurisprudenza. Altri *reports* sull'attività ell'O.d.V. potranno essere redatti su specifica richiesta dell'Organo Amministrativo, del Collegio Sindacale, o delle rispettive Presidenze. Nel Regolamento, tenuto conto di quanto previsto nel Modello Organizzativo, occorrerà infine dettagliare i flussi in formativi da e verso l'Organismo di Vigilanza.

4.7 Flussi informativi verso l'Organismo di Vigilanza.

Nel declinare i compiti dell'O.d.V. occorre chiarire che, per assolvere al mandato che a legge gli assegna, ed al fine di ottenere un Modello efficace, l'Organismo di Vigilanza deve avere garantito il più ampio accesso alle informazioni aziendali e alle dinamiche di gestione operativa E'stato già posto in rilevo, come *ex* articolo 6, comma 2, lett. *d)* del D.Lgs.n. 231/01, i Modelli Organizzativi debbano prevedere specifici obblighi di informazione nel confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza degli stessi. La finalità, evidentemente, è di agevolare l'attività di vigilanza sull'efficacia del modello e di accertare *ex post* le cause che hanno reso possibile il verificarsi di un reato. Deve qui evidenziarsi la necessità di prevedere un sistema di relazioni a vari livelli che permetta una circolazione di informazioni idonea a ridurre il rischio reati. L'obbligo di relazionar e all'Organismo di controllo, con cadenza periodica che deve essere fissata nel Modello, è rivolto alle funzioni aziendali a rischio-reato e riguarda:

•1 i risultati dei controlli effettuati periodicamente dalle funzioni sul modello tramite prospetti riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi ecc.

• 2 le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili.

In particolare, tutti i dipendenti, dirigenti e tutti coloro che cooperano al perseguimento dei fini dell'ente, sono tenuti ad informare l'Organismo di Vigilanza, sia nelle relazioni periodiche che devono essere previste dal Modello, sia tempestivamente al verificarsi dell'evento, in ordine ad ogni violazione del Modello e del Codice Etico, nonché in ordine alla loro inidoneità, inefficacia e ad ogni altro aspetto potenzialmente rilevante. Pertanto, tutti i soggetti di cui sopra sono tenuti a trasmettere all'Organismo di Vigilanza le informazioni concernenti:

- eventi che potrebbero ingenerare responsabilità della Società ai sensi del Decreto;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti;
- rapporti predisposti dal responsabili delle funzioni aziendali nell'ambito della attività di controllo svolte, dal quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle indicazioni di cui al Decreto;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, evidenzianti i procedimenti disciplinari avviati e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nel confronti dei dipendenti), ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari;
- richiesta di assistenza legale avanzate dai soci, Amministratori, dirigenti o dipendenti a seguito di procedimenti aperti per la commissione di reati rilevanti ai sensi del Decreto;
- comunicazioni in ordine alla variazione della struttura organizzativa, alla variazione delle deleghe e dei poteri;
- variazioni delle aree a rischio, realizzazione di operazioni a rischio o comunque idonee ad alterare il rischio predeterminato nel Modello di Organizzazione;
- partecipazione ad appalti o a procedure finalizzate alla conclusione di contratti con la Pubblica Amministrazione;
- richieste di fondi e contributi pubblici e loro utilizzo; -informazioni relative ai clienti e ai fornitori della Società indagati per reati sanzionati dal Decreto;
- copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

L'Organismo di Vigilanza è destinatario anche delle segnalazioni aventi ad oggetto il funzionamento e l'aggiornamento del Modello, ossia l'adeguatezza dei principi del Codice Etico e delle procedure aziendali. Tali segnalazioni dovranno essere effettuate in forma scritta, anche via e-mail. Non sono ammesse segnalazioni anonime. L'Organismo agisce in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì l'anonimato del segnalante. I componenti dell'Organismo sono tenuti al segreto in ordine alle notizie ed alle informazioni acquisite nell'esercizio delle loro funzioni e in nessun caso potranno venir meno ai limiti posti dalla normativa sulla *privacy* e sulla tutela delle informazioni, come peraltro previsto anche dai recenti reati inseriti nell'elenco che lo stesso D.Lgs. n. 231/2001 oggi sanziona .

4.8 Comunicazioni fra Organismo di Vigilanza e Organi societari.

L'Organismo di Vigilanza deve riferire con apposito *report* scritto, periodicamente, ecomunque su base almeno semestrale, nei confronti degli Organi sociali,in merito all'attuazione del Modello, alle attività di verifica e controllo compiute e all'esito delle stesse, segnalando eventuali criticità e proponendo le modifiche al Modello ritenute opportune onecessarie. L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento dagli Organi sociali. A propria volta, l'Organismo di Vigilanza ha il dovere di richiedere al Presidente dell'Organo Amministrativo (o all'Amministratore Unico) ed al Presidente del Collegio Sindacale, ove presente, la convocazione degli Organi da essi presieduti, affinché l'O.d.V. possa ad essi riferire in merito a fatti che possano dar luogo a responsabilità amministrativa a carico dell'ente ponendo così tali Organi in condizione di adottare le misure di rispettiva competenza.

Ogni anno, in tempo utile rispetto all'assemblea convocata per l' approvazione del bilancio di esercizio, l'Organismo di vigilanza trasmetterà inoltre all'Organo Amministrativo ed al Collegio Sindacale, ove presente, una relazione consuntiva avente ad oggetto l'attività svolta nell'adempimento dei propri doveri, nonché il proprio programma di attività per l'anno successivo. Tale relazione dovrà essere comunicata all'assemblea dei soci unitamente allo schema del bilancio di esercizio.

4.9 Responsabilità.

Il legislatore, al momento dell'emanazione del D.Lgs. n. 231/2001, non ha ritenuto opportuno assoggettare ad una specifica disciplina la responsabilità dei componenti dell'Organismo di Vigilanza. Per quanto riguarda la responsabilità penale, ad oggi si può affermare che l'O.d.V. è senz'altro depositario di un obbligo di vigilanza attribuito direttamente dalla legge; tuttavia il medesimo Organismo non riveste un ruolo di garante che si traduce nel dovere di prevenzione di eventuali reati da parte delle figure aziendali apicali e dei subordinati. L'Organismo di Vigilanza non ha alcuna posizione di garanzia

rilevante *ex* articolo 40 comma, 2, c.p., visto che non è titolare di specifici poteri impeditivi ma solo di un generico dovere di sorveglianza e controllo. Infatti, la gestione dell'ente e le scelte strategiche sono e restano prerogativa dell'imprenditore e degli organi societari statutari. Resta inteso che i membri dell'Organismo di Vigilanza potrebbero incorrere in una responsabilità penale in caso di concorso omissivo, quando cioè contribuiscano dolosamente e con comportamenti omissivi coscienti alla condotta di reato posta in essere da un altro soggetto. Sussiste solamente un rischio di responsabilità penale dei componenti dell'O.d.V. : è il caso relativo all'inosservanza degli obblighi in tema di prevenzione dell'attività di riciclaggio. Infatti, il D.Lgs. n. 231/2007, artt. 52 e 55, attribuisce esplicitamente all'O.d.V. l'obbligo di comunicare *"a) senza ritardo alle autorità di vigilanza di settore tutti gli atti o i fatti di cui vengano a conoscenza nell'esercizio dei propri compiti che possano costituire una violazione delle disposizioni emanate ai sensi dell'articolo 7, c.2; b)...senza ritardo al titolare dell'attività o al legale rappresentante o a un suo delegato, le infrazioni all'articolo 41 di cui abbiano notizia; c).... entro trenta giorni, al Ministero dell'Economia e delle Finanze le infrazioni alle disposizioni di cui al'articolo 49..e 50 di cui abbiano notizia; d)... entro trenta giorni, all'Autorità di Vigilanza di settore le infrazioni alle disposizioni contente nell'articolo36 di cui abbiano notizia".* Tali disposizioni, dunque, attribuiscono all'Organismo di Vigilanza un obbligo di doppia comunicazione/denuncia: interno, alla proprietà/rappresentanza legale della società, ed esterno, alle Autorità di Vigilanza ed al Ministero dell'Economia e delle Finanze. L'omissione dolosa delle dovute comunicazioni è sanzionata con la responsabilità penale dei componenti dell'O.d.V. (reclusione fino ad un anno e multa da 100 a 1.100 euro). Per quanto riguarda la responsabilità civile dell'Organismo di Vigilanza nei confronti di terzi, va precisato che l'Organismo *de quo* non è qualificabile come Organo della società in senso stretto, ed in capo ad esso non è ravvisabile una posizione autonoma di garanzia e tutela degli interessi collettivi o di terzi (come ad esempio avviene per il Collegio Sindacale). L'Organismo previsto dall'articolo 6 D.Lgs. n. 231/2001 è una funzione organizzativa dell'impresa, facoltativa ed indipendente. I suoi poteri, se pur ampi ed effettivi, non si traducono mai in interventi di impedimento di comportamenti potenzialmente illeciti o in applicazioni dirette di sanzioni disciplinari. Di conseguenza non ricorrono lecondizioni affinchè l'O.d.V. risponda dei danni patiti da terzi a seguito di accertamento della responsabilità amministrativa dell'ente.

Diversa l'ipotesi della responsabilità contrattuale *ex* articolo 1218 c.c. dei singoli componenti dell'Organismo di Vigilanza verso la Società che li nomina, per *culpa in vigilando* o per negligente adempimento dell'incarico. In caso di colpa dei membri dell'Organismo di Vigilanza, questi saranno tenuti a risarcire il pregiudizio subito dall'ente a seguito delle sanzioni irrogate al medesimo per la commissione di reati di cui al Decreto. In ogni caso, l'attribuzione di tale responsabilità all'O.d.V. o ad un suo componente dovrà sempre basarsi sulla colpa per violazione dell'obbligo di diligenza nello svolgimento delle funzioni di vigilanza e sul nesso causale tra l'inadempimento ed il danno in concreto subito. A fronte di tale rischio appare opportuno, a tutela degli stessi interessi della società, prevedere nella delibera di nomina dell'O.d.V. l'estensione a ciascun membro di adeguata copertura assicurativa per responsabilità civile, sia per danni verso la Società e terzi, sia per spese legali anche di difesa, con gli stessi massimali di quelli previsti per gli amministratori della Società.

APPENDICE

RASSEGNA COMMENTATA DEI REATI PRESUPPOSTO DELLA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI (D. LGS. 8GIUGNO 2001, N. 231; ARTICOLI 24 E SEGUENTI).

Nella presente appendice vengono descritte per ciascun reato previsto dal D.Lgs 231 del 2001 e successive modifiche alcune condotte esemplificative, le aree/processi aziendali a maggior rischio, e alcuni protocolli finalizzati alla prevenzione del reato. Come già evidenziato le presenti Linee Guida hanno l'obiettivo di fornire indicazioni generali, non potendo prevedere ipotesi, situazioni e casistiche applicabili a qualsivoglia Associazione aderente e a tutte le tipologie di rischio di commissione di reato. Si tratta, quindi, di mere esemplificazioni che, oltre a non avere assolutamente la pretesa di essere esaustive, vanno poi adattate, di volta in volta, alla concreta realtà aziendale di riferimento, in base alla natura dell'ente, alle dimensioni, all'organizzazione, alle attività tipiche e alla storicità.
Pertanto, quanto contenuto nella seguente parte necessita di uno specifico adeguamento alle singole realtà aziendali in cui viene adottato il modello e di una verifica della congruità con le caratteristiche dimensionali e organizzative della stessa . In particolare, si sottolinea che i protocolli indicati devono essere inseriti in un sistema organico di controlli e presidi, che deve essere efficace nel suo complesso. Quanto appena detto vale soprattutto in relazione agli enti di piccole dimensioni, così come precedentemente definiti, e ai quali è irrealistico imporre l'utilizzo di tutto il complesso bagaglio di protocolli e strumenti di controllo appropriati in organizzazioni diversamente strutturate e dimensionate.
In questa tipologia di imprese l'organismo di Vigilanza potrà valutare l'opportunità dell'applicazione dei controlli preventivi e dei protocolli suggeriti in forma estremamente semplificata. A seconda della scala dimensionale potranno, quindi, essere utilizzate soltanto alcune componenti di controllo, mentre altre potranno venire escluse o essere presenti in termini estremamente semplificati. Tuttavia, è opportuno ribadire che, per tutti gli enti, siano essi grandi, medi o piccoli, il sistema dei protocolli e dei controlli preventivi dovrà essere tale che lo stesso:
- nel caso di reati dolosi, non possa essere aggirato se non con intenzionalità;
- nel caso di reati colposi, come tali incompatibili con l'intenzionalità fraudolenta, risulti comunque violato, nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito Organismo.

Di seguito si procede alla rassegna commentata dei reati presupposto della responsabilità amministrativa degli enti che allo stato delle modifiche fino ad ora introdotte risulta composto dai seguenti reati:

Articolo 24. *Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.*

Articolo 24bis. *Delitti informatici e trattamento illecito di dati.*

Articolo 24ter. *Delitti di criminalità organizzata.*

Articolo 25. *Concussione e corruzione.*

Articolo25bis. *Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.* Articolo25bis- 1. *Delitti contro l'industria e il commercio.*Articolo25ter. *Reati societari.* Articolo25quater. *Delitti con finalità di terrorismo o di eversione dell'ordine democratico.* Articolo25quater-1. *Pratiche di mutilazione degli organigenitali femminili.* Articolo25quinquies. *Delitti contro la personalità individuale.* Articolo25sexies. *Abusi di mercato.*Articolo25septies. *Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.*

Articolo25octies. *Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.*

Articolo25novies. *Delitti in materia di violazione del diritto d'autore.*
Articolo25novies. *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.*

L. 146, 16 marzo 2006. *Reati transnazionali.*

ARTICOLO 24 D.LGS 231/2001: INDEBITA PE RCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE, FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO.

In relazione alla commissione dei delitti di cui agli articoli 316 bis, 316 ter, 640, comma 2, n. 1, 640 bis e 640 ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o e' derivato un danno di particolare gravità; si applica la sanzione pecuniaria da duecento a seicento quote.

Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

***

Articolo 316 *bis* c.p. Malversazione a danno dello Stato o dell'Unione europea. ***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, punito con la reclusione da sei mesi a quattro anni.***

Osservazioni
La malversazione è reato comune (potendo essere commesso da "chiunque") che si configura nel caso in cui, dopo aver ricevuto finanziamenti, contributi o sovvenzioni da parte dello Stato italiano o dell'Unione europea, non si proceda all'utilizzo delle somme ottenute per gli scopi/attività cui erano destinate, anche se tale distrazione riguardi solo parte della somma erogata, e l'attività programmata si sia realmente svolta. Si differenzia dalla truffa aggravata in quanto nella malversazione il bene è conseguito legittimamente, ma il suo uso è distorto, invece nella truffa gli artifizi e i raggiri sono funzionali all'ottenimento del beneficio, il cui ottenimento diventa così illegittimo. Finalità della norma è quella di reprimere le frodi successive al conseguimento di prestazioni pubbliche distraendole dallo scopo tipico individuato dal precetto che autorizza l'erogazione. Presupposto della condotta è che la prestazione pubblica si sostanzi in attribuzioni pecuniarie a fondo perduto (sovvenzioni o contributi) o in atti negoziali ad onerosità attenuata (finanziamenti). Consumazione del reato ed esecuzione della condotta criminosa coincidono, pertanto il reato può configurarsi anche in relazione a finanziamenti o agevolazioni ottenuti in passato e non destinati alla prefissate finalità.

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque trattasi di reato comune	Il reato si consuma con la condotta. Erogazione ed ottenimento di contributi, sovvenzioni o finanziamenti pubblici	Mancata destinazione dei fondi o delle agevolazioni pubbliche allo scopo tipico previsto ed entro i termini previsti	Dolo generico: coscienza e volontà di dare alla prestazione pubblica ricevuta una destinazione diversa da quella stabilita o concordata.	Reclusione da sei mesi a quattro anni. Sanzione ecuniaria da 100 a 500 quote; Sanzione pecuniaria da 200 a 600 quote, se dal reato l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; Sanzioni interdittive.

Trattandosi di reato di pura omissione, il momento fondi o delle agevolazioni consumativo è individuato nella scadenza del termine entro il quale il finanziamento va utilizzato.

Relativamente a questa fattispecie per le Associazioni sussiste una considerevole rischiosità, vista la partecipazione a procedure pubbliche per l'ottenimento di finanziamenti, contributi o erogazioni da parte di enti pubblici locali, statali o comunitari.

Aree aziendali esposte a rischio:

- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici;
- Gestione finanziaria-contabile, controllo di gestione, internal auditing, rendicontazione;
- Gestione investimenti ambientali, produttivi, e per ricerca e sviluppo tecnologico;
- Gestione finanziamenti per lo sviluppo dell'occupazione, la qualificazione e riqualificazione del personale.

Protocolli per il contenimento o l'eliminazione del rischio:

- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi coinvolti nella gestione di contributi, sovvenzioni o finanziamenti pubblici;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti per la redazione dei progetti, delle comunicazioni e delle rendicontazioni destinate agli enti pubblici eroganti;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a contributi, sovvenzioni o finanziamenti pubblici (entità, ente erogante, data di ottenimento del finanziamento, figure aziendali che si sono occupate del progetto e della gestione dell'agevolazione, destinazione finale dell'agevolazione stessa);
- Incontri periodici e/o audit fra O.d.V. e funzioni aziendali esposte al rischio *de quo* ;
- Documentazione, archiviazione e tracciabilità degli atti e delle operazioni inerenti eventuali contributi, sovvenzioni o finanziamenti pubblici;
- Segregazione e separazione delle funzioni fra chi gestisce l'attività di progettazione, chi verifica e chi appone la firma finale;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione di contributi, sovvenzioni o finanziamenti pubblici, con esplicitazione delle fasi e delle tipologie di controlli attuati.

Articolo 316 *ter* c.p. Indebita percezione di erogazioni in danno dello Stato o dell'Unione europea. ***Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a 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.***

Osservazioni

Tale reato si configura in caso di indebito ottenimento -mediante utilizzo o presentazione di dichiarazioni o documenti materialmente o ideologicamente falsi, ovvero mediante l'omissione di informazioni dovute- di contributi, finanziamenti, mutui agevolati o altre erogazioni dallo Stato, da altri enti pubblici o dall'Unione europea. Il momento consumativo in tale fattispecie, rispetto al reato di malversazione (articolo 316bis c.p.), è anticipato alla fase di ottenimento del contributo, a prescindere dal successivo utilizzo delle somme ottenute.

La condotta dell'agente si deve inserire in un procedimento amministrativo teso ad ottenere erogazioni da parte dello Stato e può esplicarsi in senso commissivo (presentazione dichiarazioni o documenti falsi o attestanti cose non vere) o omissivo (c.d. silenzio antidoveroso). Si tratta di una fattispecie criminosa residuale e sussidiaria rispetto al reato di truffa aggravata per il conseguimento di erogazioni pubbliche (articolo 640 bis c.p.), in quanto nei suoi elementi costitutivi non è inclusa l'induzione in errore del soggetto passivo (da ultimo Cass. Pen. Sez. II, 45845 del 11/12/08). Pertanto, qualora l'erogazione consegua alla mera presentazione di una dichiarazione mendace, senza accompagnarsi ad ulteriori artifizi e raggiri finalizzati all'induzione in errore, ricorrerà la fattispecie di cui all'articolo 316 ter c.p. L'ipotesi di reato de quo si configura come speciale e residuale anche nei confronti del reato di truffa in danno dello Stato (articolo 640, c.2, n.1 c.p.), rispetto al quale l'elemento specializzante -oltre che dalla mancanza di artifizi e raggiri- è dato dal tipo di profitto, generico e di qualsiasi natura. Ad esempio, concretizza la fattispecie di indebita percezione: la presentazione di fatture indicanti un prezzo maggiorato per l'acquisto di beni con contributi pubblici; il conseguimento di finanziamenti con dichiarazioni attestanti un reddito imponibile non corrispondente a quello reale; l'ottenimento di indennità assistenziali per propri dipendenti esponendo dati anagrafici e contabili non veritieri o incompleti; l'attestazione da parte di un dipendente di circostanze non vere, ma conformi a quanto richiesto dalla Pubblica Amministrazione, che faccia ottenere alla società un finanziamento pubblico.

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque estraneo allapubblica amministrazione ; trattasi di reato comune	Conseguimento indebito del di erogazioni pubbliche a fondo perduto o agevolate,	La condotta può essere tanto commissiva (impiego o presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere) quanto omissiva	Dolo specifico (fine di conseguire l'erogazione indebita).	Reclusione da sei mesi a tre anni. Sanzione pecuniaria da 200 a 600 quote, se dal reato l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; Sanzioni interdittive.

Aree maggiormente esposte a rischio risultano essere le seguenti:
- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi
- Gestione finanziaria-contabile, controllo di
- Gestione investimenti ambientali, produttivi, parimenti non sussistente qualora l'erogazione pubblica, e per ricerca e sviluppo tecnologico;
- Gestione finanziamenti pe lo viluppo dell'occupazione, la qualificazione e pertanto potersi considerare come percepita riqualificazione del personale.

Protocolli per il contenimento o l'eliminazione d**el rischio:**
- Diffusione e accettazione del Codice Etico, interdittive. del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti *ex* D.Lgs 231/2001 e successive modifiche;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi aziendali finalizzati alla percezione di contributi, finanziamenti, mutui agevolati o altre erogazioni dallo Stato, da altri enti pubblici o dall'Unione europea;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti per la redazione dei progetti, delle comunicazioni e delle rendicontazioni destinate agli enti pubblici eroganti;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche (entità, ente erogante, dati identificativi della richiesta, data di ottenimento del finanziamento, figure aziendali che si sono occupate della progettazione e della gestione dell'agevolazione, destinazione finale dell'agevolazione stessa);
- Incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo* ;
- Vigilanza, anche attraverso audit dedicati, da parte dell'O.d.V. sui processi/funzioni esposti al rischio individuato;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti eventuali contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche (dalla presentazione della richiesta alla rendicontazione);
- Segregazione e separazione delle funzioni fra chi gestisce l'attività di progettazione, chi verifica e chi appone la firma finale;
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione di contributi, sovvenzioni o finanziamenti pubblici e soprattutto all'individuazione del responsabile finale del processo, con esplicitazione dei momenti e delle tipologie di controlli attuati.

Articolo 640, c. 2 n. 1 c.p. Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea. ***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:***
- ***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;***
- 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.

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

Osservazioni
La condotta di reato consiste nel porre in essere artifizi o raggiri per indurre in errore o per arrecare un danno allo Stato, ad altro ente pubblico, o all'Unione Europea, al fine di realizzare un ingiusto profitto. Gli artifizi o raggiri possono consistere in una qualsiasi simulazione o dissimulazione posta in essere per indurre in errore, compreso il silenzio maliziosamente serbato. Si tratta di un reato istantaneo e di danno, che si realizza con il concreto conseguimento del profitto e l'effettivo danno per il soggetto passivo pubblico. Tuttavia, per giurisprudenza univoca, la natura pubblica o privata dell'attività dell'ente in cui la condotta di reato si inserisce è irrilevante; infatti la circostanza aggravante di cui al comma 2, n. 1 sussiste per il solo fatto che danneggiato della condotta truffaldina sia lo Stato o altro ente pubblico. Costituiscono ad esempio condotte i reato: il rilascio di cambiali firmate con false generalità; la dazione di un assegno accompagnata da assicurazioni circa la copertura e la solvibilità; presentazione per il rimborso di note di spese non dovute; l'alterazione di cartellini segnatempo per percepire retribuzioni maggiori; la predisposizione di documenti o dati per la partecipazione a procedure di gara contenenti informazioni non veritiere, al fine di ottenere l'aggiudicazione della gara stessa, qualora la Pubblica Amministrazione proceda all'aggiudicazione della gara proprio alla società; l'omessa comunicazione all'ente pubblico di circostanze che si ha l'obbligo di comunicare (es. perdita di condizioni legittimanti un atto/permesso/autorizzazione della Pubblica Amministrazione); le condotte costituenti truffa contrattuale a danno di enti pubblici (es. Condotta dell'impresa che nella stipula/esecuzione di contratti con ASL, Comuni, Regioni ed altri enti pubblici, nasconde circostanze che, se conosciute dagli enti medesimi, avrebbero condotto ad una mancata sottoscrizione o ad una risoluzione dei contratti stessi - Cass. 5585, 8/05/1987); l'alterazione di registri e documenti che l'impresa periodicamente deve trasmettere agli istituti assicurativi e previdenziali; la compensazione illecita nel Modello F24 di credito imposta (tribunale di Cosenza n. 1342 del 03/12/08, dep. 2/03/09).

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque; trattasi di reato comune	La condotta consiste nell'induzione in errore della vittima mediante l'impiego di artifizi o raggiri; rilevano anche la menzogna, il silenzio e la reticenza. Non è richiesta l'idoneità	L'evento consiste nel conseguimento di un profitto ingiusto (momento di consumazione del reato) in corrispondenza di un altrui danno patrimoniale.	Dolo specifico (intento ingannatorio diretto al conseguimento dell'ingiusto profitto)	Reclusione da uno a cinque anni e multa da euro 309 ad euro 1549.

	ingannatoria astratta dei mezzi impiegati dal reo rilevando, esclusivamente, che questi abbiano conseguito l'effetto concreto dell'induzione in errore.			

Il reato di truffa aggravata ai danni dello Stato è quello che espone le Associazioni alla maggiore rischiosità, sia in termini di pena edittale prevista, sia in termini di numero e tipologia di processi/aree aziendali potenzialmente idonei a far incorrere l'organizzazione nel reato in questione.

In particolare **le aree aziendali esposte a rischio** risultano essere:
- Negoziazione, stipulazione ed esecuzione di contratti con la Pubblica Amministrazione;
- Gestione autorizzazioni, licenze ed adempimenti verso la Pubblica Amministrazione;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici;
- Gestione investimenti ambientali, produttivi, e per ricerca e sviluppo tecnologico;
- Gestione finanziamenti per lo sviluppo dell'occupazione, la qualificazione e riqualificazione del personale,
- Gestione finanziaria- contabile, controllo di gestione, internal auditing, rendicontazione;
- Gestione contenziosi giudiziali e stragiudiziali relativi all'esecuzione di contratti stipulati con soggetti pubblici;
- Gestione degli adempimenti relativi ai diritti di proprietà industriale ed intellettuale;
- Contatto con enti Pubblici per gestione adempimenti, verifiche, ispezioni, riguardanti anche la sicurezza nei luoghi di lavoro *ex* T.U. 81/08;
- Gestione rapporti con enti pubblici per assunzione personale appartenente a categorie protette;
- Gestione adempimenti di legge in materia previdenziale ed assistenziale del personale;
- Gestione di beni mobili registrati relativi all'attività aziendale;
- Gestione degli adempimenti tributari.

Protocolli per il contenimento o l'eliminazione del rischio:

- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari; • Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 e in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.; • Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili della gestione di rapporti con lo Stato, altri enti pubblici o Unione europea;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti per la redazione dei progetti, delle comunicazioni e delle rendicontazioni destinate agli enti pubblici eroganti;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito ai rapporti intrattenuti con rappresentanti di enti pubblici (identificazione dell'ente, tipologia del rapporto, oggetto e datazione di eventuali incontri, figure aziendali che si sono occupate della gestione del rapporto medesimo);
- Incontri periodici e/o audit fra O.d.V. e funzioni aziendali esposte al rischio *de quo* ;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti i rapporti tenuti con enti pubblici anche a distanza (es. per via telematica);
- Segregazione e separazione delle funzioni fra chi predispone, che controlla, chi firma e chi invia le comunicazioni ufficiali ricolte ad enti pubblici;
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con enti pubblici, e soprattutto all'individuazione del responsabile finale del processo, con esplicitazione dei momenti e delle tipologie di controlli attuati.

Articolo 640 *bis* c.p. 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.

Osservazioni
In questa fattispecie la truffa è posta in essere per conseguire indebitamente erogazioni pubbliche. Rispetto alla truffa aggravata (articolo 640, c.2, n.1 c.p.) l'elemento specializzante è costituito dall'oggetto materiale, ossia:

-contributi e sovvenzioni: erogazioni a fondo perduto;
-finanziamenti: cessioni di credito a condizioni vantaggiose per impieghi determinati;
-mutui agevolati: cessioni di credito vantaggiose e con ampi tempi di restituzione;
-altre erogazioni dello stesso tipo: categoria aperta in grado di ricomprendere qualsiasi altra attribuzione economica agevolata erogata dallo Stato, altri enti pubblici o Comunità europee. Per la realizzazione di tale fattispecie è necessario che al mendacio si accompagni una specifica attività fraudolenta (artifizi e raggiri per indurre in errore), che vada ben oltre la semplice esposizione di dati falsi, così da vanificare o rendere meno agevole l'attività di controllo richiesta da parte delle autorità preposte: es. predisposizione di documenti o dati per la partecipazione a bandi di erogazione finanziamenti pubblici con inserimento di informazioni supportate da documentazione artefatta; p resentazioni di fatturazioni false o gonfiate per ottenere il rimborso delle relative somme dall'ente pubblico; presentazione di attestazioni false, dissimulanti o rappresentanti una realtà distorta; falsificazione di dati contabili per l'ottenimento di mutui o altri finanziamenti statali agevolati; false dichiarazioni per ottenere indebite prestazioni economiche dall'INPS a titolo di disoccupazione involontaria, indennità di maternità, sussidi per lavori socialmente utili; artifizi e raggiri per procurarsi elargizioni della CEE nel settore agricolo; false dichiarazioni per ottenere un contributo straordinario dalla Regione per l'abbattimento di capi di bestiame affetti da malattie; presentazione di rendiconti non veritieri per la percezione di contributi pubblici finalizzati all'organizzazione di corsi professionali (Cass. Sez. VI, 15/10/2004); La differenza tra il reato de quo e quello previsto e punito dall'articolo 316 ter c.p. (indebita percezione di erogazioni pubbliche) consiste appunto nell'inclusione tra gli elementi costitutivi della prima fattispecie della induzione in errore del soggetto passivo: pertanto, qualora l'autore non si limiti a rendere dichiarazioni

mendaci, ma predisponga una serie di artifici in grado di indurre in errore il soggetto pubblico, ricorrerà il reato di truffa aggravata ex articolo 640 bis c.p. (Cass.3055/2007).

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque; trattasi di reato comune	L'evento consiste nell'ottenimento (indebito) non di un generico profitto, bensì di provvidenze pubbliche non dovute	La condotta è identica a quella del reato previsto dall'art.640: impiego di artifizi e raggiri ed induzione in ingannatorio inteso all'indebita percezione delle erogazioni.	Dolo specifico (intento ingannatorio diretto al conseguimento dell'ingiusto profitto)	Reclusione da uno a sei anni.

Anche relativament a questa fattispecie le Associazioni risultano esposte ad una considerevole rischiosità;

Le aree aziendali esposte a rischio coprono la totalità dei processi aziendali:

- Gestione autorizzazioni, licenze ed adempimenti verso la Pubblica Amministrazione;
- Acquisizione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie da parte di enti pubblici, anche europei;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione investimenti ambientali;
- Selezione e gestione del personale, formazione finanziata;

Protocolli per il contenimento o l'eliminazione del rischio:

- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi aziendali finalizzati alla percezione di contributi, finanziamenti, mutui agevolati o altre erogazioni dallo Stato, da altri enti pubblici o dall'Unione europea;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti per la redazione dei progetti, delle comunicazioni e delle rendicontazioni destinate agli enti pubblici eroganti;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche (entità, ente erogante, dati identificativi della richiesta, data di ottenimento del finanziamento, figure aziendali che si sono occupate della progettazione e della gestione dell'agevolazione, destinazione finale dell'agevolazione stessa);
- Incontri periodici e/o audit fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delleoperazioni inerenti eventuali contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche (dalla presentazione della richiesta alla rendicontazione);
- Segregazione e separazione delle funzioni fra chi gestisce l'attività di progettazione, chi verifica e chi appone la firma finale;
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione di contributi, sovvenzioni o finanziamenti pubblici e soprattutto all'individuazione del responsabile finale del processo, con esplicitazione dei momenti e delle tipologie di controlli attuati.

Articolo 640 *ter* c.p. Frode informatica in danno dello Stato o di altro ente pubblico.*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. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.*

Osservazioni
Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico, o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altri enti pubblici. La struttura e gli elementi costitutivi della fattispecie sono gli stessi della truffa (articolo 640 c.p.), tuttavia l'attività fraudolenta dell'agente non investe direttamente la persona del soggetto passivo pubblico, ma il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Il momento consumativo si realizza con il conseguimento dell'ingiusto profitto con relativo danno patrimoniale all'ente pubblico. Si pensi ai flussi informativi obbligatori verso la PA, come le dichiarazioni fiscali all'Agenzia delle Entrate (Modello Unico, Modello 770, comunicazioni IVA, F24, ecc.), le comunicazioni alla Camera di Commercio, l'invio di denunce e dati previdenziali ad INAIL ed INPS (es. DM10). Si pensi anche a Associazion che nella partecipazione a procedure ad evidenza pubblica, o nell'esecuzione di contratti con soggetti pubblici, debbano effettuare delle comunicazioni telematiche con i soggetti stessi o inserire dati in registri telematici pubblici (es. inserimento in sistema informatico di un importo relativo ad un finanziamento pubblico superiore a quello ottenuto legittimamente).

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque;	Reato di danno. Alterazione o danneggiamento di un sistema informatico; manipolazione di dati o informazioni; intrusione	Conseguimento di un profitto ingiusto (momento di consumazione del reato) in corrispondenza di un danno	Dolo specifico	Reclusione da uno a cinque anni e multa da 309 a 1.549 euro.

	Illegittima in programmi *software* .	patrimoniale patito dallo Stato o da altro ente pubblico.		

Aree aziendali esposte a rischio:
- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie;
- Gestione Sistemi Informativi, ed in particolare gestione di SW pubblici o forniti da terzi per conto di enti pubblici;
- Gestione sistema privacy;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione investimenti ambientali;
- Acquisizione e gestione di finanziamenti per lo sviluppo dell'occupazione, la qualificazione e riqualificazione del personale.

Protocolli per il contenimento o l'eliminazione del rischio:
- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativie di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali autorizzate ad accedere a sistemi informatici o telematici ed in possesso delle relative password;
- Incontri periodici e/o audit fra O.d.V. e funzioni aziendali esposte al rischio *de quo* ;
- Documentazione, archiviazione, tracciabilità degliatti e delle operazioni effettuate su sistemi informatici e telematici, specie se di pubblica rilevanza;
- Diffusione di prassi e procedure interne finalizzate al corretto accesso a sistemi informatici o telematici della Pubblica Amministrazione (attribuzione nominativa delle password, controlli automatici su corretto utilizzo delle credenziali di accesso, rispetto del D.P.S. e della normativa privacy, ecc.);
- Applicazione dei protocolli previsti in prevenzione dei reati informatici (articolo 24bis D.Lgs 231/2001);
- Predisposizione di automatismi di controllo della legittimità degli accessi ai sistemi informatici o telematici e di segnalazione di operazioni non autorizzate (cancellazioni, tentativi di accesso non autorizzati, abusiva duplicazione, alterazione della funzionalità del sistema ecc.);
- Diffusione ed accettazione di specifico regolamento per corretto accesso a sistemi informatici o telematici della Pubblica Amministrazione per le Associazioni che gestiscono, sviluppano e realizzano i suddetti sistemi in base a contratti o accordi con enti pubblici.

ARTICOLO 24 BIS D.LGS. 231/2001 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.

In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

***

Articolo 491 *bis* c.p. Falsità in un documento informatico pubblico o avente efficacia probatoria. ***Se alcuna delle falsità previste dalpresente capo [ndr Falsità in atti] 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.***

Articolo 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici.
Articolo 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative.
Articolo 478. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti.
Articolo 479. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici.
Articolo 480. Falsità ideologica ommessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative.
Articolo 481. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità.
Articolo 482. Falsità materiale commessa dal privato.
Articolo 483. Falsità ideologica commessa dal privato in atto pubblico.
Articolo 484. Falsità in registri e notificazioni.
Articolo 485. Falsità in scrittura privata.
Articolo 486. Falsità in foglio firmato in bianco. Atto privato.
Articolo 487. Falsità in foglio firmato in bianco. Atto pubblico.
Articolo 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali.
Articolo 489. Uso di atto falso.
Articolo 490. Soppressione, distruzione e occultamento di atti veri.]

NOTA: il **documento informatico** è, secondo la definizione data dall'articolo 1, lett. *p)* del Decreto legislativo n. 82 del 7 marzo 2005, il c.d Codice dell'Amministrazione Digitale, "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". Sul punto, la relazione al disegno di legge originario n. 2807) annota: " *...in considerazione della*

sopravvenuta inadeguatezza della definizione di documento informatico, inteso come 'supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli, si è deciso di accogliere, anche ai fini penali, la più ampia e corretta nozione di documento informatico, già contenuta nel regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, come 'rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti'."

Osservazioni
La fattispecie in questione punisce le condotte di falsità di cui agli artt. 476-493 c.p. aventi ad oggetto documenti informatici pubblici o privati aventi efficacia probatoria. La norma punisce sia la falsità c.d. materiale che la falsità ideologica; nel primo caso si fa riferimento all'ipotesi di un documento contraffatto nell'indicazione del mittente o nella firma stessa, o ancora all'ipotesi di alterazione del contenuto dopo la sua formazione. L'ipotesi di falsità ideologica attiene, invece, alla non veridicità delle dichiarazioni contenute nel documento stesso.

Le realtà Associazione potrebbero incorrere in tali reati ad esempio attraverso:
il falso materiale commesso con un uso illegittimo della firma elettronica altrui, la redazione di un falso atto informatico destinato ad essere inserito in un pubblico archivio la cui gestione operativa sia affidata ad una società privata come appunto una Associazione, la cancellazione di dati considerati sensibili o rischiosi al fine di controllare o deviare eventuali ispezioni o controlli.
Nel caso specifico, ad esempio durante la procedura di richiesta di un'autorizzazione il soggetto che presiede la richiesta, trasmette su supporto informatico, utilizzando un sistema informativo interno o messo a disposizione da un ente pubblico, un documento falso.

Aree aziendali esposte a rischio:
- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie;
- Gestione Sistemi Informativi, ed in particolare gestione di SW pubblici o forniti da terzi per conto di enti pubblici;
- Gestione finanziaria- contabile, controllo di gestione, rendicontazione;
- Gestione investimenti ambientali;

Protocolli per il contenimento o l'eliminazione del rischio:
- Individuazione della funzione deputata rappresentare la società nei confronti della P.A. concedente, cui conferire apposita delega e procura;
- Definizione, chiara e precisa di ruoli e compiti della funzione responsabile del controllo sulle fasi di ottenimento e gestione delle concessioni e/o autorizzazioni, con particolare riguardo ai presupposti di fatto e di diritto per la presentazione della relativa richiesta;
- Adozione e diffusione di Manuale Informatico (MI) e/o Regolamento informatico e/o policy aziendale;
- Formalizzazione della procedura, prevedendo specifici sistemi di controllo (ad es., la compilazione di schede informative, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo, per verificare la veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la concessione e/o autorizzazione;
- Flussi informativi all'ODV: comunicare su base annuale l'elenco delle richieste inoltrate e delle autorizzazioni ottenute, specificando le PA concedenti e i referenti contattati per la gestione della pratica (scheda di evidenza);
- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.;
- Adeguato sistema di pro cure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi aziendali a rischio;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Previsione di specifiche clausole per terzi/outsourcer per il rispetto del Codice etico e Modello;
- Stesura del Manuale Informatico (MI);
- Utilizzo di applicativi informatici dedicati atti a configurare le abilitazioni all'accesso alla rete, a tracciare tali accessi ed a impedire condotte illecite;
- Previsione di una procedura interna per la gestione delle abilitazioni ai sistemi informativi (associazione di ogni utente ad un profilo abilitativo coerente con ruolo aziendale);
- Predisposizione e mantenimento del censimento degli applicativi che si interconnettono con la Pubblica amministrazione o con Autorità di Vigilanza e loro specifici software in uso;
- Previsione di distinti ruoli e responsabilità di gestione della sicurezza delle informazioni (segregazione dei compiti per ambiti di sicurezza, progettazione, implementazione, manutenzione);
- Adeguamento alle procedure e istruzioni riportate nel Documento di Protezione e Sicurezza (DPS) per la protezione delle informazioni con particolare riferimento al trattamento dei dati sensibili;
- Adozione di soluzioni di continuità operativa, tecnologica e infrastrutturale che assicurino continuità anche in situazioni di emergenza;
- Protezione e controllo delle aree fisiche (perimetri e zone riservate);
- Tracciabilità e archiviazione delle attività effettuate sui sistemi informatici e patrimonio informativo (sia a sistema che documentale);
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Segnalazione tempestiva all'O.d.V. di eventuali incidenti relativi alla sicurezza dei dati;
- Formazione periodica sui reati informatici e sulle procedure aziendali in essere.

Articolo 615 *ter* c.p. 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: 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; - se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;***

- ***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.***

Osservazioni
La fattispecie di reato prevede e punisce chi si introduce o permane abusivamente in un sistema informatico o telematico protetto. Per sistema informatico ai sensi dell'art 1 della Convenzione di Budapest del 23 novembre 2001 sulla criminalità informatica, si intende "qualsiasi apparecchiatura o rete di apparecchiature interconnesse o configurate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati". Per "sistema telematico" si deve intendere qualsiasi rete di telecomunicazione sia pubblica che privata, locale, nazionale o internazionale, operante da o per l'Italia. Fondamentale per la configurabilità del reato è che il sistema attaccato (anche se adibito ad un uso individuale) risulti protetto da "misure di sicurezza", che devono intendersi anche come misure genericamente di carattere organizzativo, che cioè disciplinino semplicemente le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo. Possono rilevare, esemplificando, la sistemazione dell'impianto all'interno di un locale munito di serrature, la prescrizione di una *password* di accesso, l'esclusione del personale impiegatizio, attraverso la rete interna del sistema, dall'accesso ai comandi centrali per intervenire sui dati, ecc. Si prescinde dall'accertamento del fine specifico di lucro o di danneggiamento del sistema. E ' prevista la punibilità di due tipologie di condotte:
- introduzione abusiva (cioè senza il consenso del titolare dello *ius excludendi*) in un sistema informatico o telematico munito di sistemi di sicurezza;
- la permanenza in collegamento con il sistema stesso, continuando a fruire dei relativi servizi o ad accedere alle informazioni ivi contenute, nonostante vi sia stato il dissenso anche tacito del titolare (che è dimostrato anche dalla predisposizione di misure di protezione del sistema nel senso sopra descritto).

Soggetti attivi	Elemento oggettivo:	Condotta	Elemento soggettivo	Pena
Chiunque;	Reato di danno. Alterazione o danneggiamento di un sistema informatico;manipolazione di dati o informazioni; intrusione illegittima in programmi *software*.Reato di pericolo (funzione di tutela anticipata). Accesso abusivo (non autorizzato) ad un sistema informatico protetto; permanenza in tale sistema nonostante l'ingiunzione o i tentativi di estromissione del proprietario, gestore otitolare del sistemastesso.	-Fatto commesso, con abuso dei poteri o in violazione dei doveri, da pubblicoufficiale o incaricato dipubblico servizio, dainvestigatore privato o daoperatore del Aggravantisistema; -fatto commesso con uso di violenza su cose opersone ovvero conimpiego di armi; -fatto cui consegue ladistruzione o il anneggiamentodel sistema, l'interruzionedel suo funzionamento,ovvero la distruzione o ildanneggiamento di dati,informazioni o programmiin esso contenuti;-fatto commesso susistemi di interessemilitare, ovvero relativiall'ordine o alla sicurezzapubbliche, allasanità, alla protezione civile o comunque diinteresse pubblico.	Dolo generico (volontarietà della condotta con consapevolezza del carattere abusivo e illegittimo di questa).	Reclusione fino a tre anni nell'ipotesi base (a querela). Reclusione da uno a cinque anni nelle ipotesi di cui ai nn. 1,2 e 3 (d'ufficio). Reclusione da uno a cinque anni, e da tre a otto anni, nelle ipotesi di cui al n.4 (d'ufficio).

Si tratta di una fattispecie perseguibile a querela della persona offesa, salvo che non si verifichino le aggravanti di cui al comma 2 (danneggiamento/distruzione di dati, di programmi o del sistema; interruzione totale o parziale del funzionamento del sistema; abuso della funzione di pubblico ufficiale, investigatore, operatore del sistema; utilizzo di violenza; accesso a sistemi di interesse pubblico). Le condotte criminose configurabili si ricollegano ad ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale dell'ente, soci o consulenti:
- accedano abusivamente ad un sistema informatico protetto (interno e/o esterno alla società): ad esempio utilizzo di nome utente e di parola d'accesso di terzi per visualizzare e riprodurre documenti senza autorizzazione;
- ottengano, riproducano, diffondano, comunichino o divulghino codici di accesso a sistema informatici protetti: ad esempio comunicare credenziali per accedere alle caselle mail di terzi al fine di controllarne l'operato, anche nell'interesse dell'azienda;
- intercettino, impediscano o interrompano comunicazioni relative ad un SI/telematico o intercorrenti tra più sistemi: ad esempio introduzione di *virus* o installazione di *software* non autorizzati aventi effetto di rallentare la comunicazione telematica;
- ottengano, producano, riproducano, mettano a disposizione apparecchiature dispositivi o programmi lesivi dell'integrità dei dati dei sistemi informativi: ad esempio introduzione di *virus* , programmi contenenti le c.d. "bombe logiche" etc;
- installino mezzi volti ad intercettare, blocchino o interrompano comunicazioni esempio utilizzo di apparecchiature capaci di copiare i codici per via informatica/telematica: addi accesso degli utenti al SI;
- 1 distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità;
- 2 distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui;
- 3 distruggano, danneggino sistemi informatici/telematici altrui tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi;

-distruggano o danneggino sistemi informatici/telematici di pubblica utilità;
-violino gli obblighi previsti dalla legge per il rilascio di un certificato qualificato di firma elettronica.
Le condotte di cui sopra, sia che l'acceso abusivo riguardi un sistema interno ovvero esterno alla società cui appartiene l'agente, possono tradursi in operazioni che portano un interesse o vantaggio per la società stessa, ad esempio: diminuzione del credito dei clienti, maggiorazione dei costi dei servizi erogati, fatturazione di servizi non richiesti, accesso abusivo nel sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione alla gara di appalto o al fine di conoscere il portafoglio clienti oppure le strategie commerciali, ovvero l'elenco dei soci e dei dipendenti/collaboratori o i dati relativi ai loro compensi.

Aree aziendali esposte a rischio:

- Utilizzo della rete aziendale intranet ed extranet;

gestione dei sistemi informativi; gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici;

- Attività aziendali svolte tramite l'uso di sistemi informativi, della posta elettronica, dell'accesso ad Internet;
- Gestione e manutenzione dei sistemi informativi aziendali, della piattaforma aziendale IT, e della sicurezza informatica aziendale;
- Gestione e trasmissione di comunicazioni ed informazioni con la PA per via telematica;
- Gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie;
- Gestione sistema privacy;
- Gestione gare, appalti e finanziamenti pubblici;
- Gestione finanziaria- contabile, controllo di gestione, rendicontazione;
- Gestione documenti informatici;
- Gestione dati riservati e sensibili;
- Gestione credenziali e certificati digitali;
- Gestione credenziali e certificati digitali per comunicazioni a uffici pubblici;
- Processi di pagamento;
- Accesso a sistemi di banche e istituzioni finanziarie;
- Accesso a sistemi di clienti e partner commerciali;
- Accesso a sistemi esterni;
- Gestione credenziali e certificati digitali per accesso a gare e processi di *eprocurement* ;
- Gestione credenziali e certificati digitali per comunicazioni a uffici pubblici (es. dichiarazione al registro INES – EPER ["emissioni inquinanti industriali"]);
- Presidio e protezione fisica infrastrutture ICT (*information communication technology*);
- Presidio e protezione logica sistemi ICT (*information communication technology*);
- Gestione credenziali di accesso ai sistemi ICT (*information communication technology*) interni, esterni;
- Gestione procedure di profilazione utenti.

Protocolli per il contenimento o l'eliminazione del rischio:

- Utilizzo di applicativi informatici dedicati atti a configurare le abilitazioni all'accesso alla rete, a tracciare tali accessi ed a impedire condotte illecite;
- Adozione e diffusione di Manuale Informatico (MI) e/o Regolamento informatico e/o policy aziendale;
- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;
- Realizzazione di percorsi formativi e di aggiornamento dedicati al Codice Etico, al Modello 231 ed in generale alla responsabilità degli enti ex D.Lgs 231/2001 e ss.mm.;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi aziendali;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Previsione di specifiche clausole per terzi/outsourcer per il rispetto del Codice etico e Modello;
- Predisposizione di rendiconti periodici all'O.d.V.;
- Previsione di una procedura interna per la gestione delle abilitazioni ai sistemi informativi (associazione di ogni utente ad un profilo abilitativo coerente con ruolo aziendale);
- Predisposizione e mantenimento del censimento degli applicativi che si interconnettono con la Pubblica amministrazione o con Autorità di Vigilanza e loro specifici *software* in uso;
- Previsione di distinti ruoli e responsabilità di gestione della sicurezza delle informazioni (segregazione dei compiti per ambiti di sicurezza, progettazione, implementazione, manutenzione, etc.);
- Adeguamento alle procedure e istruzioni riportate nel Documento di Protezione e Sicurezza (DPS) per la protezione delle informazioni con particolare riferimento al trattamento dei dati personali;
- Adozione di soluzioni di continuità operativa, tecnologica e infrastrutturale che assicurino continuità anche in situazioni di emergenza;
- Protezione e controllo delle aree fisiche (perimetri e zone riservate);
- Tracciabilità e archiviazione delle attività effettuate sui sistemi informatici e patrimonio informativo (sia a sistema che documentale);
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Segnalazione tempestiva all'O.d.V. di eventuali incidenti relative alla sicurezza dei dati;
- Formazione periodica sui reati informatici e sulle procedure aziendali in essere.