

Bozza aggiornata al 21 settembre 2010

CONFCOOPERATIVE

**LINEE GUIDA PER LA PREDISPOSIZIONE DEI MODELLI DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO**

AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001

N. 231

SOMMARIO

<u>SOMMARIO.....</u>	<u>I</u>
Capitolo I: Il quadro normativo e la predisposizione dei modelli di organizzazione e controllo	1
1.1 Introduzione	1
1.2 Soggetti destinatari.....	5
1.3 Presupposti per l'imputazione della responsabilità all'ente.	5
1.4 I Modelli di organizzazione, gestione e controllo.	6
1.5 Le Linee Guida di Confcooperative ex art. 6, comma 3, D.Lgs. n. 231/2001.	7
Capitolo II: Modello Organizzativo – Analisi dei rischi – Protocolli.	9
2.1 Il Modello di organizzazione, gestione e controllo.	9
2.2 Il concetto di rischio accettabile.....	10
2.3 La realizzazione del sistema di analisi, valutazione e gestione dei rischi.	11
2.4 Adozione e diffusione del Modello di organizzazione, gestione e controllo.	18
Capitolo III: Codice etico e sistema disciplinare.	20
3.1 Premessa	20
3.2 Principi generali	20
3.3 Criteri di condotta	24
3.3.1 Criteri di condotta nei rapporti con Pubblica amministrazione, pubblici dipendenti, pubblici ufficiali o incaricati di pubblico servizio.....	24
3.3.2 Criteri di condotta nei rapporti con clienti privati e fornitori.....	25
3.3.3 Criteri di condotta nei rapporti con il personale e i collaboratori.	26
3.3.4 Criteri di condotta nei rapporti con i soci.	27
3.3.5 Criteri di condotta nei rapporti con organizzazioni politiche, sociali, e sindacali.	28
3.3.6 Criteri di condotta nei rapporti con i mass media e diffusione delle informazioni.....	28
3.4 Sistema disciplinare.....	28
3.4.1. Principi generali.....	28
3.4.2. Sanzioni per i lavoratori dipendenti.....	29
3.4.3 Misure nei confronti degli Amministratori.....	29
3.4.4 Misure nei confronti dei soci.....	30
3.4.5 Misure nei confronti di collaboratori, consulenti e fornitori.....	30
Capitolo IV: L'Organismo di Vigilanza.....	31
4.1 Premessa.....	31
4.2 Nomina.....	31
4.3 Requisiti.....	31
4.4 Composizione e configurazione.....	33
4.5 Poteri e funzioni.....	36
4.6 Regolamento di funzionamento.....	37
4.7 Flussi informativi verso l'Organismo di Vigilanza.....	38
4.8 Comunicazioni fra Organismo di Vigilanza e Organi societari.....	39
4.9 Responsabilità.....	40
APPENDICE.....	42

RASSEGNA COMMENTATA DEI REATI PRESUPPOSTO DELLA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI (D.LGS. 8 GIUGNO 2001, N.231; ARTICOLI 24 E SEGUENTI).42

ART. 24 D.LGS 231/2001: INDEBITA PERCEZIONE 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.	45
ART. 24 BIS D.LGS. 231/2001 - DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.	58
ART. 24 TER D.LGS 231/2001 - DELITTI DI CRIMINALITÀ ORGANIZZATA.....	93
ART. 25 D.LGS 231/2001 - CONCUSSIONE E CORRUZIONE.....	106
ART. 25 BIS D.LGS 231/2001 - FALSITA' IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO.....	120
ART. 25 BIS-1 D.LGS 231/2001 - DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO.....	127
ART. 25 TER D.LGS 231/2001 - REATI SOCIETARI.	141
ART. 25 QUATER D.LGS 231/2001 - DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.....	172
ART. 25 QUATER-1 D.LGS 231/2001 - PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI.....	175
ART. 25 QUINQUIES D.LGS 231/2001 - DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE.	178
ART. 25 SEXIES D.LGS. 231/2001 – ABUSI DI MERCATO.....	193
ART. 25 SEPTIES D.LGS. 231/2001 - OMICIDIO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO.	198
ART. 25 OCTIES D.LGS. 231/2001 - RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA.....	206
ART. 25 NOVIES D.LGS 231/2001 - DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE.....	223
ART. 25 NOVIES D.LGS 231/2001 - INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA.....	231
L. 146, 16 MARZO 2006 - REATI TRANSNAZIONALI.....	233

Capitolo I: Il quadro normativo e la predisposizione dei modelli di organizzazione e controllo

1.1 Introduzione

Il decreto legislativo 8 giugno 2001, n. 231 ha introdotto per la prima volta 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 nell'interesse o a vantaggio delle stesse.

Il D.Lgs. n. 231/2001 è stato emanato sulla base della Legge 29 settembre 2000, n. 300 che, nel recepire una serie di Atti internazionali e comunitari, delegava il Governo ad emanare una norma di previsione e disciplina della responsabilità diretta degli enti da reato.

In particolare, il legislatore con la Legge n. 300/2000 recepiva alcune convenzioni e protocolli internazionali precedentemente sottoscritti dall'Italia:

-Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea;

-Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione dei funzionari pubblici della Comunità Europea e degli Stati membri;

-Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Fino all'introduzione del D.Lgs. n. 231/2001, l'art. 27 della Costituzione (“la responsabilità penale è personale”), impediva che detta responsabilità potesse investire le organizzazioni in quanto persone giuridiche. Il principio *societas delinquere non potest*, unanimemente riconosciuto fino al 2001, lasciava gli enti indenni da eventuali conseguenze sanzionatorie, salvo l'eventuale risarcimento del danno, qualora riconosciuto. Gli articoli 196 e 197 c.p., infatti, riversano sull'ente l'obbligazione di pagamento di multe o ammende in caso di insolvibilità della persona fisica autrice materiale del fatto. Tuttavia, si tratta solo di un'obbligazione civile di garanzia della persona giuridica per l'ipotesi in cui colui che ne abbia la rappresentanza o l'amministrazione commetta un reato.

Il D.Lgs. 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 responsabilità penale; nella Relazione ministeriale di accompagnamento si legge, infatti, che tale 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 D.Lgs. 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 ad istituti penalistici sostanziali e processuali,

la sottoposizione dell'ente all'accertamento ed al giudizio del giudice penale, con tutte le garanzie previste dal processo penale del nostro ordinamento.

Il D.Lgs. n. 231/2001 prevede 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 ad una specifica tecnica scelta dal legislatore nonché ad 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 D.Lgs. n. 231/2001 o in leggi speciali. In altre parole, il D.Lgs. n. 231/2001 contiene un catalogo di reati aperto ed in continua espansione, come dimostrano le integrazioni che dal 2001 ad oggi si sono susseguite.

Al momento dell'emanazione del D.Lgs. n. 231/2001, la responsabilità amministrativa degli enti era configurabile solo per le fattispecie di reato di cui agli **artt. 24 e 25** dello stesso Decreto (Indebita percezione di contributi o altre erogazioni da parte di un ente pubblico, Truffa in danno dello Stato o di altro ente pubblico, Truffa aggravata per il conseguimento di erogazioni pubbliche, Frode informatica in danno dello Stato o di altro ente pubblico, Corruzione, Concussione); tuttavia, il legislatore già prevedeva nella Relazione di accompagnamento una possibile estensione delle tipologie, sia attraverso una diretta modifica al Decreto sia attraverso il rinvio operato da leggi speciali.

Dopo appena cinque mesi dall'entrata in vigore del decreto 231, il legislatore introduceva l'art. **25 bis**, relativo alle falsità in monete, carte di pubblico credito e in valori di bollo (art. 6, L. 23 novembre 2001, n. 409).

L'anno successivo, con l'approvazione della riforma del diritto societario, il legislatore introduceva anche l'art. **25-ter** relativo ai reati societari (art. 6, D.Lgs. 11 aprile 2002, n. 61), fattispecie poi modificate dalla Legge 28 dicembre 2005, n. 262.

L'art. 25-ter, tuttavia, non si limitava ad integrare l'elenco dei reati rilevanti ex D.Lgs. n. 231/2001, ma ridisegnava il criterio oggettivo di imputazione della responsabilità amministrativa dell'ente ed individuava in modo specifico i potenziali soggetti-autori dei reati presupposto.

In deroga, infatti, a quanto previsto dall'art. 5, D.Lgs. n. 231/2001, l'art. 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'art. 5 tra soggetti "apicali" e "sottoposti", viene limitata a figure particolari, quali amministratori, direttori generali e liquidatori (apicali), ed a tutti coloro che siano soggetti alla loro vigilanza (sottoposti).

Dopo l'inserimento dei reati societari, l'intervento del legislatore è continuato con la L. 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'art. **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'art. **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. 262) e la Legge sul risparmio (Legge 28 dicembre 2005, n. 262) hanno modificato alcuni reati societari già previsti dal D.Lgs. n. 231/2001 e inserito i c.d. reati di abuso di mercato per le società quotate (**art. 25-sexies**, D.Lgs. n. 231/2001).

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 **art. 25-quater 1** ha introdotto la responsabilità amministrativa degli enti per l'ipotesi di reato prevista e punita dall'art. 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'art. 25-quinquies, D.Lgs. n. 231/2001 e l'ampliamento dei reati ivi previsti.

Ed 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 amministrativa 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, si è preferito disciplinare direttamente le nuove fattispecie e rinviare al D.Lgs. 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 reati 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 (**art. 25-septies**, D.Lgs. 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 (TU 81/2008 e non solo) possono oggi rappresentare per gli enti un'area di rischio ai sensi dell'art. 25-septies, D.Lgs. n. 231/2001.

Invece, l'**art. 25-octies**, D.Lgs. n. 231/2001 (relativo ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita) viene inserito con la L. 21 novembre 2007, n. 231 di attuazione delle Direttive 2005/60/CE e 2006/70/CE.

Nel 2008 l'art. 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'**art. 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'art. 2 della Legge 15 Luglio 2009 n. 94 (Pacchetto sicurezza) ha introdotto l'**art. 24-ter** relativo ai delitti di criminalità organizzata (Associazione per delinquere, Associazioni di tipo mafioso anche straniere, Scambio elettorale 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 ex D.Lgs. n. 231/2001 dall'art.10 della legge n. 146/2006 "Ratifica della Convenzione ONU 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'art 15 della Legge 23 luglio 2009 n. 99, tra le altre disposizioni contenute, modifica l'**art 25-bis** (estendendo la sua applicazione anche alla tutela di strumenti o segni di riconoscimento), ed inserisce l'**art 25-bis 1** (delitti contro l'industria e il commercio) e l'**art 25-nonies** (delitti in materia di violazioni del diritto d'autore).

3) L'art. 4 della Legge 3 agosto 2009, n. 116 introduce 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 art. 25 nonies (delitti in materia di violazione del diritto d'autore).

Va, infine, precisato che la Legge delega n. 300 del 2000 (art. 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 ad un secondo intervento normativo l'inserimento degli illeciti penali ambientali nel catalogo dei reati ex D.Lgs. n. 231/2001. Tale inserimento dovrà in ogni caso avvenire entro la 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, deve tassativamente essere recepita entro il 26 dicembre 2010. L'art. 6 della suddetta 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...».

1.2 Soggetti destinatari.

L'art. 1 del D.Lgs. n. 231 definisce l'ambito di applicazione soggettivo; 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. Con 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.

1.3 Presupposti per l'imputazione della responsabilità all'ente.

L'art. 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 (c.d. soggetti apicali); ovvero da soggetti sottoposti alla direzione o alla vigilanza di chi gestisce o controlla l'ente (c.d. 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'art. 6 del D.Lgs. n. 231/2001 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 offrendo 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'art. 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 ad 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'art. 25-ter, D.Lgs. n. 231/2001 (che fa esclusivo riferimento al criterio dell'interesse).

Un ultimo filone interpretativo, ad oggi prevalente anche in giurisprudenza, parte dall'opposto assunto per cui i termini "interessi e vantaggio" sarebbero assolutamente distinti ed alternativi, in ossequio ad una lettura sistematica del D.Lgs. n. 231/2001 ed al generale principio interpretativo di conservazione delle norme. In conformità alla stessa Relazione governativa di accompagnamento al D.Lgs. n. 231/2001, il concetto di "interesse dell'ente" andrebbe interpretato in senso soggettivo, con riferimento cioè alla volontà dell'autore materiale del reato da valutare *ex ante*; al contrario, il vantaggio andrebbe letto 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"* (art. 5, comma 2, D.Lgs. 231/2001).

1.4 I Modelli di organizzazione, gestione e controllo.

L'art. 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, preme ricordare che i suddetti modelli devono rispondere a 5 specifiche esigenze:

- individuare le c.d. 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.

1.5 Le Linee Guida di Confcooperative ex art. 6, comma 3, D.Lgs. n. 231/2001.

Ai sensi dell'art. 6, comma 3, D.Lgs 8 giugno 2001, n. 231, 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".

In base a tale previsione, Confcooperative, in qualità di principale organizzazione di rappresentanza, assistenza e tutela del mondo cooperativo italiano, ha costruito le presenti Linee Guida tenendo conto della variegata realtà aziendale degli enti aderenti.

Tale disomogeneità di base non ha tuttavia impedito di formulare principi, indicazioni e misure utili per l'adozione di adeguati modelli organizzativi e per la corretta individuazione di un organo di controllo.

Le presenti Linee Guida si rivolgono quindi, a tutti gli associati a Confcooperative fatta eccezione per le Banche di Credito Cooperativo.

La definizione di quali sono gli enti associabili è contenuta nei primi tre commi dell'articolo 3 dello Statuto della Confederazione ai sensi dell'articolo 3 del vigente Statuto secondo cui:

“

1. *La Confederazione è costituita da enti cooperativi e mutualistici e loro consorzi e da imprese sociali, la cui adesione sia stata deliberata ed accolta secondo il disposto del comma 4° e seguenti del presente articolo.*
2. *Può essere consentita, in base a procedure definite in sede regolamentare, l'adesione di società ordinarie cui partecipino in maggioranza enti cooperativi già aderenti o loro controllate, nonché di società semplici o di fatto, regolate secondo i principi della cooperazione e della mutualità.*
3. *Può essere altresì consentita, in base a procedure definite in sede regolamentare, l'adesione di enti ed organismi con finalità solidaristiche o che esplicano attività affini a quelle della cooperazione e delle imprese sociali, o che comunque ne favoriscano l'incremento.*

“

Pertanto il riferimento alle "cooperative" o il più generico agli "enti" contenuto nelle pagine che seguono deve essere sempre inteso nei confronti della totalità dei soggetti aderenti come sopra individuati.

Si evidenzia inoltre un concetto fondamentale che sarà ripreso più volte nel corso del presente lavoro: la base sociale di Confcooperative è in larga parte costituita da enti che rientrano nella definizione comunitaria (si veda la Raccomandazione della Commissione europea n. 2003/361/Ce del 6 maggio 2003) di micro imprese (meno di 10 addetti e un fatturato non superiore a 2 milioni di euro) e piccole imprese (tra 10 e 49 addetti e un fatturato non superiore a 10 milioni di euro), ma vede anche la presenza di enti che rientrano nella definizione di media impresa nonché di enti che superano tali parametri qualificandosi come grandi imprese.

Il ventaglio di ipotesi che deve essere coperto dalle presenti Linee Guida è molto ampio e variegato anche sotto il profilo dimensionale e organizzativo (basti pensare, ad esempio, che una buona parte degli enti aderenti a Confcooperative non hanno il Collegio Sindacale ai sensi dell'articolo 2543 del codice civile).

Si sottolinea da subito che l'applicazione delle presenti linee alla micro e piccole imprese aderenti deve evitare appesantimenti burocratici in situazioni ove le ridotte dimensioni dell'impresa non li giustificano, soprattutto in considerazione del fatto che queste realtà sono caratterizzate da una struttura meno articolata rispetto ad altre realtà e quindi da minori risorse da poter dedicare alla realizzazione e attuazione di modelli organizzativi.

In particolare, le presenti Linee Guida dovranno essere applicate agli enti di piccole dimensioni avendo presente che nella costruzione di un idoneo modello organizzativo le piccole dimensioni dell'impresa nella stragrande parte dei casi possono comportare:

- una minore complessità dell'analisi dei rischi, in termini di numerosità ed articolazione delle funzioni aziendali interessate e di casistiche di illecito aventi potenziale rilevanza per l'ambito di attività;
- la possibilità che le modalità operative di conduzione dell'attività di gestione dei rischi, possa essere svolta, direttamente dall'Organo Amministrativo, eventualmente con apporti professionali esterni;
- la possibilità che l'articolazione dei controlli preventivi sia posta in essere utilizzando procedure, eventualmente, anche in forme semplificate.

Ovviamente spetterà, caso per caso, agli estensori del singolo modello organizzativo e all'Organismo di Vigilanza la valutazione di quanto la natura dell'attività svolta, la dimensione dell'ente, intesa anche sotto il profilo dell'articolazione organizzativa, incide sul livello di "alleggerimento" e "semplificazione" del contenuto del modello organizzativo, dovendosi sempre motivare le scelte in questo senso compiute e avendo riguardo al fatto 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.

Capitolo II: Modello Organizzativo – Analisi dei rischi – Protocolli.

2.1 Il Modello di organizzazione, gestione e controllo.

L'art. 6, c.1 del D.Lgs. 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, poi, 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 ed 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.

Scopo del modello organizzativo (di seguito il Modello) è, in altri termini, la costruzione di un sistema strutturato ed 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 ed 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 D.Lgs. n. 231/2001 può comportare il sorgere di responsabilità e sanzioni per l'ente stesso;
- sottolineare che tutti i comportamenti difforni 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, ed ogni altro accordo intercorso con l'ente stesso;

- consentire all'ente, grazie ad 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 ed applicazione del modello (Organismo di Vigilanza o O.d.V.).

2.2 Il concetto di rischio accettabile.

La costruzione di un Modello, in base all'art. 6, c.2, D.Lgs. 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 di cui al D.Lgs. n. 231/2001.

A tal 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, ad 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 ad 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'art. 40, c.2 c.p., ci si può concretamente e ragionevolmente attendere nella situazione concreta al fine di evitare il verificarsi dell'evento lesivo.

Lo stesso D.Lgs. n. 231/2001 sembra orientarsi in questa direzione quando all'art. 6, c.1 lett. 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 artifici 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 stesso, in base alla sua attività, struttura, estensione geografica, dimensione ecc.

In sintesi, dunque, il "rischio accettabile" si ridurrà a quel rischio che "residua" a seguito della corretta definizione ed applicazione delle procedure, regole e principi previsti dal sistema di controllo aziendale ed a seguito di un controllo diligente ed efficace da parte dell'ente (per mezzo dell'Organismo di Vigilanza e del management aziendale).

Questo concetto di rischio accettabile va, però, adattato alle ipotesi di reati colposi (art. 25-septies, D.Lgs. n. 231/2001), 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/area aziendale di una reale ed oggettiva quantificazione del rischio accettabile e del rischio residuo. Per compiere tale percorso possono venire in ausilio tecniche di *risk assessment* 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, ecc...), di mercato, di credito, ecc.

La metodologia consente di utilizzare il medesimo approccio anche qualora i principi del D.Lgs. n. 231/2001 vengano estesi ad altri ambiti. Se poi tali ambiti sono regolati da specifica normativa (es. adeguamento a standard internazionali previsti dalle norme UNI EN ISO per i sistemi di gestione qualità, ambiente sicurezza, etica ecc.), il modello dovrà integrarsi (non sovrapporsi e sostituirsi) con le regole preesistenti.

2.3 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 (As Is analysis); b) analisi delle eventuali carenze rilevate (Gap analysis ed altre metodologie); c) definizione/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. A ciascun quesito corrisponderanno specifici input, attività da svolgere ed output.

Chi siamo.

Input: organigramma aziendale, mansionario, sistema di deleghe interne, procure, certificazioni camera di commercio, analisi di poteri e natura di organi aziendali statuari 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 input mira a definire un quadro chiaro di ruoli e responsabilità, individuando soprattutto i soggetti qualificabili come figure apicali ai sensi dell'art. 5, comma 1, lett.a, D.Lgs. n. 231/2001, in quanto "*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 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.

(Esempio: per conoscere la struttura organizzativa di una cooperativa, come prima attività, è necessario esaminare il soggetto cui è attribuita la legale rappresentanza dell'ente (es. Presidente, Direttore Generale), da quale fonte essa deriva (ex lege, per Statuto, per delibera del CdA, per procura formale ecc.). E' un passaggio estremamente importante, visto che alcuni reati previsti dal Decreto n. 231 sono illeciti propri dei legali rappresentanti).

Output: mappa delle figure apicali, adeguato sistema di deleghe e procure.

A quali norme siamo soggetti.

Input: 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, e 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 ed informazioni vengono inseriti ed integrati nel Modello 231, che da un lato li recepisce come presidi organizzativi preesistenti, dall'altro li utilizza come strumento di controllo e verifica dei processi aziendali.

(Esempio: nell'ipotesi in cui una cooperativa abbia effettivamente attuato, ed eventualmente certificato, un Sistema di gestione della sicurezza sul lavoro conforme alle Linee Guida UNI-INAIL e/o al British Standard OHSAS 18001:2007, essa avrebbe una metodologia organizzativa efficace per gestire e migliorare gli aspetti di salute e sicurezza nell'azienda; inoltre, ai sensi dell'art. 30, comma 5 "*i Modelli di Organizzazione aziendale definiti conformemente alle Linee Guida UNI-INAIL o al*

Brithis Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti”).

Output: elenco dei presidi normativi esistenti per ciascun processo/area.

Cosa facciamo.

Input: Processi, funzioni, attività, aree, istruzioni, regolamenti, procedure, prassi operative aziendali. Esame storico degli 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 D.Lgs. 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 finale¹.

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 D.Lgs. n. 231/2001 e le attività poste in essere in ciascuna area aziendale al fine di definire quali soggetti/processi/attività siano esposti al rischio di potenziale realizzazione dei reati medesimi.

(Esempio: Esaminando il processo di gestione e amministrazione delle risorse umane, e guardando in particolare alla fase di selezione ed assunzione del personale, si può ritenere che l'attività in questione sia esposta, fra gli altri, anche al rischio di commissione del reato di corruzione di pubblico ufficiale ex artt. 318 ss. c.p.: il rischio si

1 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.

concretizza nella possibile assunzione di personale gradito alla P.A. al fine di trarne un indebito vantaggio).

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

Come controlliamo.

Input: sistema dei controlli interni esistenti.

Attività da svolgere: verifica dei sistemi di controllo già applicati. Quantificazione del c.d. “rischio residuo”. Individuazione di protocolli aggiuntivi.

Una volta individuate le c.d. aree “sensibili”, occorre verificare i protocolli esistenti, ossia gli eventuali presidi già applicati in azienda ed in grado di prevenire la realizzazione degli illeciti.

In base a tale analisi sarà possibile procedere alla quantificazione del c.d. “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'art. 6, c.2, lett. b, D.Lgs. 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 reati 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) ed 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 D. Lgs. 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 ed 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 e/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 amministrativo-finanziaria (l'art. 6, c. 2, lett. c, D.Lgs. 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, prevedendo, 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.

TRACCIABILITA' e RINTRACCIABILITA': 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 ed 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.

E' necessario, inoltre, garantire la corretta individuazione dei responsabili ed identificare chiaramente i poteri ad essi attribuiti. Occorre, pertanto, un adeguato sistema di procure, deleghe e nomine conformi a quanto previsto dal TU 81/2008 e ss.mm. 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. Ad 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 ed appalto; a tale proposito è necessario predisporre un adeguato sistema di selezione, e trasmettere a fornitori ed appaltatori tutte le informazioni 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 ed una fase di verifiche ispettive periodiche, rivolte a processi, attività, soggetti specifici, condotte da figure adeguatamente formate e competenti. A seguito di tali verifiche il "sistema sicurezza" nel suo complesso dovrebbe essere sottoposto ad 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 ex D.Lgs. n. 231/2001 ed essere congruente con la gestione complessiva dei processi aziendali.

----- - -----

I principi di controllo fin qui indicati rappresentano una mera esemplificazione, necessitando di uno specifico adeguamento alle realtà aziendali in cui vengono 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.

(Esempio: ritornando all'esempio precedente, relativo al rischio di commissione del reato di corruzione tramite l'assunzione di personale gradito alla P.A. al fine di trarne un indebito vantaggio, si può ipotizzare l'introduzione e diffusione - quale protocollo di prevenzione - di una specifica policy per la corretta selezione, assunzione e gestione del personale).

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

Come verifichiamo.

Input: Audit test.

Attività da svolgere: programmazione ed esecuzione di sessioni di audit test.

La gestione del Modello deve prevedere una fase di verifica del suo mantenimento ed aggiornamento nonché dell'applicazione ed efficacia dei protocolli adottati.

Le verifiche, eventualmente svolte o disposte dall'Organismo di Vigilanza, devono essere innanzitutto pianificate, ed 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 e/o all'Organismo di Vigilanza;

Output della fase: Esito degli audit di controllo.

Come rimediamo.

Input: Audit di controllo.

Attività da svolgere:

Gli esiti degli audit 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/introduzione 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.

Output della fase: Action plan degli interventi da effettuare.

2.4 Adozione e diffusione del Modello di organizzazione, gestione e controllo.

Il processo di analisi dei rischi e di definizione dei protocolli di contenimento trova la sua sintesi finale in un documento complessivo, definito esso stesso "Modello Organizzativo".

Tale 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 aventi un'attinenza più specifica all'attività istituzionale della cooperativa.

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'art. 6, c.1 D.Lgs. 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 apposita delibera del Consiglio di Amministrazione.

In relazione alle modifiche del Modello, queste possono ritenersi necessarie a seguito di aggiornamenti normativi, cambiamenti nell'organizzazione, nei processi e nelle attività aziendali, verificarsi di eventi straordinari (gravi violazioni, contestazioni, sanzioni ecc.).

E' auspicabile che queste modifiche giungano all'approvazione del Consiglio di Amministrazione principalmente su proposta dell'Organismo di Vigilanza. Dopo la delibera del CdA, 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 Cooperativa; in particolare:

- L'Organo Amministrativo (CdA)
 - 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 Collegio 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.

Capitolo III: Codice etico e sistema disciplinare.

3.1 Premessa

Il codice etico può definirsi un 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

Di seguito si richiamano sinteticamente i principi etici cui le Società Cooperative e gli enti diversi dalle cooperative aderenti a Confcooperative ispirano le proprie scelte e le proprie norme di comportamento.

Rispetto delle norme previste dell'ordinamento giuridico

Il movimento cooperativo 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 rapporti con 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 cooperativa. 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 le 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 mansioni 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 perseguire 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 parti.

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 le 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 nei 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, né 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/collaboratori 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 società cooperative.

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 nonché 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'art. 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 (art. 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 cooperative 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, con 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 di un 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 societarie di piccole o medie dimensioni. Con particolare riguardo alle cooperative, si rileva che stante quanto previsto dall'articolo 2543 del codice civile la nomina del collegio è obbligatoria nei soli casi previsti 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 2435bis: 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 preconditione necessaria ad assicurare l'idoneità stessa della composizione dell'O.d.V. . Ovvio che 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.

Preliminare è la definizione di enti di piccole dimensioni.

Confcooperative, in virtù delle particolari caratteristiche dimensionali di una larga parte della propria base associativa, non può esimersi dall'offrire una definizione ai fini dell'applicazione delle presenti linee guida. Poiché né il legislatore né la giurisprudenza fino ad ora formatasi soccorrono, è necessario rifarsi alla dottrina.

Secondo la dottrina che qui si recepisce, l'approccio interpretativo alla definizione deve muovere dalla struttura dell'ente, dalla configurazione organizzativa e dall'ambito in cui esso opera. In altri termini, la definizione di piccola dimensione non può essere ricercata solo in parametri quantitativi quale la definizione di piccola e media impresa di origine comunitaria (Raccomandazione della Commissione Europea n. 2003/361/CE del 6-5-2003) pure importante al fine della definizione di tali enti, quanto piuttosto anche nella struttura interna gerarchica e funzionale, tenuto conto delle concrete esigenze organizzative del singolo ente, dell'ambito in cui esso agisce e del relativo livello reddituale. Si può ritenere che si sia in presenza di un'impresa di piccole dimensioni, ai fini previsti dal D.Lgs. n. 231/2001, allorquando la struttura sia di tipo elementare ed in essa le funzioni di governo societario ed economico, nonché quella di direzione aziendale, sostanzialmente siano svolte da un unico soggetto. In buona sostanza, si ritiene che vi sia un ente di piccole dimensioni quando il potere decisionale non è delegato ma si concentra nelle mani di una singola persona fisica.

Ci riferiamo principalmente ad enti che non hanno il Collegio Sindacale ai sensi dell'articolo 2543 del codice civile e il cui Organo Amministrativo è costituito da un Amministratore unico il quale svolge direttamente, in prima persona, tutte le funzioni proprie della direzione d'impresa. Ma anche ad enti che, sempre in assenza dell'obbligo di Collegio Sindacale, hanno un Organo Amministrativo che presenta al vertice un soggetto il quale, oltre a svolgere direttamente, in prima persona, tutte le funzioni proprie della direzione dell'impresa, somma altresì in sé la figura di Presidente, e quindi normalmente di legale rappresentante, e di unico Amministratore delegato, con estensione di poteri delegati tali da lasciare al resto dell'Organo i soli poteri non delegabili ai sensi degli articoli 2381 e 2544 del codice civile.

In tali casi appare evidente la difficoltà di individuare una dissociazione tra la volontà dell'agente persona fisica e la volontà dell'ente, vista la compenetrazione esistente tra tali soggetti: di conseguenza, il legislatore consente all'Organo dirigente di svolgere anche le funzioni di Organismo di Vigilanza.

E' necessario sottolineare come l'adozione di una struttura estremamente elementare, in enti a base societaria aperta come le cooperative, 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 del 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'art. 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 questa 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 le procedure 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 della conoscenza 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;

- raccogliere, 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 migliorare il monitoraggio delle attività nelle aree di rischio nonché 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.

Tale 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 la successiva 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 dell'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 la 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 rilievo, come ex art. 6, comma 2, lett.d) del D.Lgs. n. 231/01, i Modelli Organizzativi debbano prevedere specifici obblighi di informazione nei 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 relazionare all'Organismo di controllo, con cadenza periodica che deve essere fissata nel Modello, è rivolto alle funzioni aziendali a rischio-reato e riguarda:

- i risultati dei controlli effettuati periodicamente dalle funzioni sul modello tramite prospetti riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi ecc.
- 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 dai responsabili delle funzioni aziendali nell'ambito della attività di controllo svolte, dai 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, evidenziando i procedimenti disciplinari avviati e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nei confronti dei dipendenti), ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari;
- richiesta di assistenza legale avanzata 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, e comunque 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 o necessarie.

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 art. 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'art. 7, c.2; b)... senza ritardo al titolare dell'attività o al legale rappresentante o a un suo delegato, le infrazioni all'art. 41 di cui abbiano notizia; c)... entro trenta giorni, al Ministero dell'Economia e delle Finanze le infrazioni alle disposizioni di cui all'art. 49.e 50 di cui abbiano notizia; d)... entro trenta giorni, all'Autorità di Vigilanza di settore le infrazioni alle disposizioni contenute nell'art.36 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'art. 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 le condizioni affinché 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 art. 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. 8 GIUGNO 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 cooperativa 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. Sotto questo profilo si deve nuovamente sottolineare che una parte significativa delle aderenti a Confcooperative rientra nella definizione comunitaria di micro imprese ed una larga parte in quella di piccole imprese. 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:

Art. 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.

Art. 24bis. Delitti informatici e trattamento illecito di dati.

Art. 24ter. Delitti di criminalità organizzata.

Art. 25. Concussione e corruzione.

Art.25bis. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

Art.25bis-1. Delitti contro l'industria e il commercio.

Art.25ter. Reati societari.

Art.25quater. Delitti con finalità di terrorismo o di eversione dell'ordine democratico.

Art.25quater-1. Pratiche di mutilazione degli organi genitali femminili.

Art.25quinquies. Delitti contro la personalità individuale.

Art.25sexies. Abusi di mercato.

Art.25septies. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

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

Art.25novies. Delitti in materia di violazione del diritto d'autore.

Art.25novies. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

L. 146, 16 marzo 2006. Reati transnazionali.

ART. 24 D.LGS 231/2001: INDEBITA PERCEZIONE 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).

Art. 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, è 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 artifici 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 sostanzia 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.

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

Soggetti attivi	Chiunque; trattasi di reato comune
Elemento oggettivo:	Il reato si consuma con la condotta.
Presupposto	Erogazione ed ottenimento di contributi, sovvenzioni o finanziamenti pubblici
Condotta	Mancata destinazione dei fondi o delle agevolazioni pubbliche allo scopo tipico previsto ed entro i termini previsti
Elemento soggettivo	Dolo generico: coscienza e volontà di dare alla prestazione pubblica ricevuta una destinazione diversa da quella stabilita o concordata.
Pena	Reclusione da sei mesi a quattro anni. Sanzione pecuniaria 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.

Relativamente a questa fattispecie per le cooperative 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 (es. formazione del personale, finanziamenti europei all'agricoltura, finanziamenti per lo sviluppo tecnologico ecc.).

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.

Art. 316ter 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 (art. 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 (art. 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 artifici e raggiri finalizzati all'induzione in errore, ricorrerà la fattispecie di cui all'art. 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 (art. 640, c.2, n.1 c.p.), rispetto al quale l'elemento specializzante –oltre che dalla mancanza di artifici 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	Chiunque estraneo alla pubblica amministrazione; trattasi di reato comune.
Elemento oggettivo: Condotta	Il reato è di danno. La condotta può essere tanto commissiva (impiego o presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere) quanto omissiva (omissione di
Evento	Conseguimento indebito del di erogazioni pubbliche a fondo perduto o agevolate,
Elemento soggettivo	Dolo specifico (fine di conseguire l'erogazione indebita).
Cause di esclusione del reato	Il reato in esame non sussiste qualora l'erogazione indebitamente ottenuta sia inferiore ad euro 3.999,96: tale ipotesi configura illecito amministrativo. Il reato è parimenti non sussistente qualora l'erogazione pubblica, anche senza la condotta incriminata, sarebbe comunque avvenuta senza pertanto potersi considerare come percepita indebitamente.
Pena	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.

Anche relativamente a questa fattispecie le cooperative risultano esposte ad una considerevole rischiosità; le **aree maggiormente esposte a rischio** risultano essere le seguenti:

- 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 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.

Art. 640, c. 2 n.1 c.p. Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea.

Chiunque, con artifici 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 artifici 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 artifici 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 (Tr. Cosenza n. 1342 del 03/12/08, dep. 2/03/09).

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

Il reato di truffa aggravata ai danni dello Stato è quello che espone le imprese cooperative 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 TU 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 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 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.

Art. 640bis 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 (art. 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; presentazioni 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'art. 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 art. 640 bis c.p. (Cass. 3055/2007).

Soggetti attivi	Chiunque; trattasi di reato comune.
Elemento oggettivo: Condotta	Reato di danno. La condotta è identica a quella del reato previsto dall'art.640: impiego di artifizi e raggiri ed induzione in

Evento	L'evento consiste nell'ottenimento (indebito) non di un generico profitto, bensì di provvidenze pubbliche non dovute
Elemento soggettivo	Dolo specifico (intento ingannatorio inteso all'indebita percezione delle erogazioni pubbliche).
Pena	Reclusione da uno a sei anni.

Anche relativamente a questa fattispecie le cooperative risultano esposte ad una considerevole rischiosità; si pensi alla rendicontazione fittizia di docenze per formazione del personale in relazione a corsi mai svolti, o alla presentazione di attestazioni fasulle per l'ottenimento di agevolazioni o finanziamenti dalla Comunità europea (es. settore agricoltura), o alle dichiarazioni indirizzate ad enti previdenziali al fine di ottenere contributi economici di vario tipo.

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;
- Ricerca e sviluppo tecnologico;
- Selezione e gestione del personale, formazione finanziata;
- Acquisizione e 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 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 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.

Art. 640ter 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 (art. 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 cooperative 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	Chiunque.
Elemento oggettivo: Condotta	Reato di danno. Alterazione o danneggiamento di un sistema informatico; manipolazione di dati o informazioni; intrusione illegittima in programmi <i>software</i> .
Evento	Conseguimento di un profitto ingiusto (momento di consumazione del reato) in corrispondenza di un danno patrimoniale patito dallo Stato o da altro ente pubblico.
Elemento soggettivo	Dolo specifico
Pena	Reclusione da uno a cinque anni e multa da 309 a 1.549 euro.

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 gare, appalti e finanziamenti pubblici;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione investimenti ambientali;
- Ricerca e sviluppo tecnologico;
- 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 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 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 degli atti 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 (art. 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 cooperative che gestiscono, sviluppano e realizzano i suddetti sistemi in base a contratti o accordi con enti pubblici.

ART. 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, 617-quinquies, 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 615-quinquies 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).

Art. 491bis c.p. Falsità in un documento informatico pubblico o avente efficacia probatoria.

Se alcuna delle falsità previste dal presente 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.

[Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici.

Art. 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative.

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

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

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

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

Art. 482. Falsità materiale commessa dal privato.

Art. 483. Falsità ideologica commessa dal privato in atto pubblico.

Art. 484. Falsità in registri e notificazioni.

Art. 485. Falsità in scrittura privata.

Art. 486. Falsità in foglio firmato in bianco. Atto privato.

Art. 487. Falsità in foglio firmato in bianco. Atto pubblico.

Art. 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali.

Art. 489. Uso di atto falso.

Art. 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.

Soggetti attivi	Chiunque /Pubblico ufficiale
Elemento oggettivo	Falsità in atti, su documento informatico pubblico o privato avente efficacia probatoria.
Elemento soggettivo	Dolo

Le realtà cooperative 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 cooperativa, 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 gare, appalti e finanziamenti pubblici;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione investimenti ambientali;
- Ricerca e sviluppo tecnologico;
- 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:

- Individuazione della funzione deputata a 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 procure 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.

Art. 615ter 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) .

Si tratta di una fattispecie perseguibile a querela della persona offesa, salvo che non si verificano 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).

Soggetti attivi	Chiunque
Elemento oggettivo: Condotta	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 o titolare del sistema stesso.
Aggravanti	<ul style="list-style-type: none"> - Fatto commesso, con abuso dei poteri o in violazione dei doveri, da pubblico ufficiale o incaricato di pubblico servizio, da investigatore privato o da operatore del sistema; - fatto commesso con uso di violenza su cose o persone ovvero con impiego di armi; - fatto cui consegue la distruzione o il danneggiamento del sistema, l'interruzione del suo funzionamento, ovvero la distruzione o il danneggiamento di dati, informazioni o programmi in esso contenuti; - fatto commesso su sistemi di interesse militare, ovvero relativi all'ordine o alla sicurezza pubbliche, alla sanità, alla protezione civile o comunque di interesse pubblico.
Elemento soggettivo	Dolo generico (volontarietà della condotta con consapevolezza del carattere abusivo e illegittimo di questa).
Pena	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).

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 *password* e *username* di terzi per visualizzare e riprodurre documenti senza autorizzazione;
- ottengano, riproducano, diffondano, comunichino o divulgino codici di accesso a sistemi 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, bloccino o interrompano comunicazioni per via informatica/telematica: ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui;
- 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'accesso 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;
- Ricerca e sviluppo tecnologico.

Tenuto conto della diffusione delle tecnologie informatiche si porta, a titolo esemplificativo, l'attenzione sulla esecuzione delle seguenti attività/funzioni aziendali:

- 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 *e-procurement*;
- 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.

Art. 615^{quater} c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

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

Osservazioni

Il reato in questione punisce le condotte di procacciamento, riproduzione, diffusione, comunicazione o consegna di codici, parole-chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto, con il fine di procurarsi un profitto o di arrecare un danno. Rispetto alla disposizione prevista dall'art. 615 ter c.p. vi è anticipazione della soglia di tutela poiché il reato sanziona condotte che riguardano i codici d'accesso e non direttamente i sistemi informatici che con tali codici possono essere aggrediti. Di qui la natura di reato di pericolo che va attribuita alla fattispecie in esame, che si consuma nel momento in cui l'agente, alternativamente, si procura o diffonde i codici di accesso ovvero fornisce indicazioni utili a tal fine, indipendentemente dall'effettivo danno o turbamento del sistema (ad esempio, a prescindere dall'effettivo utilizzo dei codici per accedere abusivamente nel sistema).

Il reato è perseguibile d'ufficio e la condotta criminosa può limitarsi alla mera detenzione di mezzi o dispositivi idonei all'accesso abusivo (*virus, spyware*) e comunque è sanzionata la condotta di chi illegittimamente operi su codici di accesso, parole chiave o

altri mezzi di accesso a sistemi informatici protetti da misure di sicurezza. Vista la formulazione ampia della norma, vi rientrano sia gli strumenti "virtuali" di accesso (*password* e codici) che quelli fisici (chiavi meccaniche e tessere elettroniche). Tra gli "altri mezzi idonei" a consentire l'accesso vanno compresi anche gli strumenti biometrici fondati sul riconoscimento da parte del sistema della voce o delle impronte.

Può configurare il reato anche la detenzione o diffusione abusiva di *pics-card* ossia di schede informatiche che consentono di vedere programmi televisivi criptati, oppure il procacciamento abusivo di numeri seriali di apparecchi telefonici cellulari altrui al fine di clonarlo ed effettuare una illecita connessione ad una rete telefonica protetta.

Ricorre il "procurarsi" nel caso di ottenimento del codice /*password* da persona o cosa (elaboratore elettronico) che ne sia a conoscenza; il "riprodurre" è ravvisabile nel caso in cui il soggetto agente riesca a creare autonomamente (di solito con programmi informatici "pirata") il codice, una parola chiave o altri mezzi idonei all'accesso al sistema; il "diffondere" ricorre nel caso di illecita comunicazione ad una pluralità indeterminata di soggetti, il "comunicare" sussiste nell'ipotesi in cui, invece, il soggetto agente porti a conoscenza del codice di accesso uno o più soggetti determinati; il "consegnare" si configura nel caso in cui l'accesso sia consentito da mezzi fisici (scheda o chiave) che venga, in originale o in copia, portata nella disponibilità di soggetti non autorizzati dal titolare del sistema.

La norma prevede, poi, per estendere al massimo l'ambito di operatività della disposizione sanzionatoria, la penale rilevanza anche del comportamento di chi "fornisce indicazioni o istruzioni idonee al predetto scopo", in modo tale da coprire ogni sorta di comportamento che consenta a chiunque di acquisire la possibilità di accedere abusivamente a sistemi informatici.

Soggetti attivi	Chiunque
Elemento oggettivo Condotta	Reato di pericolo. Ottenimento, riproduzione, diffusione, comunicazione o divulgazione di codici di accesso a sistemi informatici protetti o crittati; fornitura di indicazioni o istruzioni dirette all'ottenimento di tali codici.
Elemento soggettivo	Dolo specifico (fine di ottenere un profitto o di arrecare danno)
Pena	Reclusione fino ad un anno e multa fino a 5.164 euro; reclusione da uno a due anni e multa da 5.164 a 10.329 euro se i codici di accesso riguardano sistemi informatici utilizzati dallo Stato, da altro ente pubblico, o da impresa esercente servizi pubblici o di pubblica necessità.

A titolo esemplificativo, le condotte criminose configurabili si ricollegano ad ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci o consulenti:

- ottengano, riproducano, diffondano, comunichino o divulgino 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, bloccino o interrompano comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo stato o altro ente pubblico o di pubblica utilità;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui.
- distruggano, danneggino sistemi informatici/telematici altrui tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi;
- distruggano, 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'accesso 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. E' altresì ipotizzabile la condotta di un operatore che comunica ad un collega le credenziali per accedere alla casella mail di un altro dipendente al fine di controllarne l'operato, anche nell'interesse dell'azienda stessa.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica;
- Gestione sistema privacy;
- Gestione gare, appalti e finanziamenti pubblici;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;

- Ricerca e sviluppo tecnologico.

Tenuto conto della diffusione delle tecnologie informatiche si porta l'attenzione, a titolo esemplificativo, sulle esecuzioni delle seguenti attività/funzioni aziendali:

- 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 *e-procurement*;
- 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 relativi alla sicurezza dei dati;
- Formazione periodica sui reati informatici e sulle procedure aziendali in essere.

Art. 615quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Osservazioni

Il reato punisce il procacciamento, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione, la consegna o la messa a disposizione in qualsiasi modo di programmi o dispositivi volti a danneggiare sistemi informatici o telematici, o dati e programmi ivi contenuti, o comunque volti ad alterare il loro funzionamento.

Le condotte tipiche si realizzano mediante l'introduzione di *virus*, *worms*, programmi contenenti le c.d. bombe logiche ecc. Potrebbe, pertanto, ipotizzarsi una responsabilità della società nel caso in cui tali condotte siano poste in essere ad esempio con la

finalità di distruggere dati, documenti o evidenze di attività ipoteticamente illecite in vista di un controllo/ispezione delle autorità competenti.

Rispetto alla fattispecie precedente, questo reato richiede già la realizzazione di una condotta attiva idonea a realizzare il danneggiamento.

Il reato è perseguibile d'ufficio.

Soggetti attivi	Chiunque
Elemento oggettivo Condotta	Reato di pericolo. Ottenimento, produzione, riproduzione, importazione, diffusione, comunicazione, consegna o messa a disposizione di apparecchiature, dispositivi o programmi lesivi dell'integrità dei dati e dei sistemi informatici. Non è richiesta la produzione dell'evento (lesione effettiva).
Elemento soggettivo	Dolo specifico (intento di danneggiare illecitamente un sistema informatico o i dati in esso contenuti ovvero di interromperne o alterarne il funzionamento).
Pena	Reclusione fino a due anni.

Le condotte criminose configurabili si ricollegano ad ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci o consulenti:

- accedano abusivamente ad un sistema informatico, (ad esempio utilizzo *password* e *username* di terzi per visualizzare e riprodurre documenti senza autorizzazione);
- ottengano, riproducano, diffondano, comunichino o divulgino 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 "bombe logiche" etc);
- installino mezzi volti ad intercettare, bloccino o interrompano comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui.
- distruggano, danneggino sistemi informatici/telematici altrui tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi;

- distruggano, danneggino sistemi informatici/telematici di pubblica utilità;
- violino gli obblighi previsti dalla legge per il rilascio di un certificato qualificato di firma elettronica.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

Tenuto conto della diffusione delle tecnologie informatiche si porta l'attenzione sulle esecuzioni delle seguenti attività/funzioni aziendali:

- 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 e-procurement;
- 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 del Regolamento informatico/policy aziendale per uso del computer sui luoghi di lavoro (in conformità alle Linee Guida Garante privacy);
- 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.

Art. 617^{quater} c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

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

Osservazioni

Il reato in esame è inserito nella sezione V (delitti contro l'inviolabilità dei segreti), del capo III (delitti contro la libertà individuale), del titolo XII (delitti contro la persona) del libro secondo del codice penale.

L'articolo prevede tre ipotesi criminose:

1. il fatto di chiunque fraudolentemente intercetta una comunicazione proveniente da un sistema informatico o telematico o da più sistemi fra loro collegati;
2. il fatto di chiunque fraudolentemente interrompe o impedisce tali comunicazioni;
3. il fatto di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni informatiche o telematiche di cui fraudolentemente abbia preso conoscenza. Tale ipotesi è sussidiaria, infatti è prevista autonomamente solo se non costituisce un più grave reato.

Per "comunicazioni informatiche o telematiche" s'intendono le trasmissioni di dati, immagini, simboli, programmi e ogni altra informazione attraverso sistemi informatici e telematici.

Per "intercettazione" si intende ogni operazione compiuta col fine di prendere conoscenza, direttamente o di nascosto, di corrispondenza, nella sua più ampia accezione.

Per "impedire" si intende il frapporre ostacoli *hardware* e *software* alla normale utilizzazione di un sistema informatico e telematico.

Per "interrompere" si intende sospendere il flusso di informazioni.

Per "rivelare" si intende portare a conoscenza, o rendere noto, senza averne facoltà o diritto, e quindi abusivamente, a terzi il contenuto di documenti informatici destinati a rimanere segreti.

Per "qualsiasi mezzo di informazione al pubblico", si intende quello dotato di specifica idoneità tecnica a divulgare la notizia nei confronti della generalità di terzi o di una parte di essi.

Per “fraudolentemente” si intende l’uso di mezzi ingannevoli o raggirevoli, cioè l’intercettazione deve consistere in attività volta a rappresentare al sistema stesso in via automatica o al gestore del sistema una situazione non corrispondente al vero.

Il tentativo di reato nei casi previsti dall’articolo in esame è ipotizzabile. Si tratta di un reato comune perchè può essere commesso da chiunque.

La norma considera l’ipotesi dell’illecita riproduzione mediante strumenti di comunicazione di massa di notizie riservate, di atti o messaggi inseriti in un sistema informativo complesso e chiuso al pubblico, o di agenzie di informazione destinate a un numero chiuso di abbonati collegati telematicamente.

La responsabilità è esclusivamente dolosa. Il dolo richiesto è quello generico, consistente nella coscienza e volontà di commettere una delle fattispecie previste.

Le condotte consistono nell’intercettazione, impedimento o interruzione fraudolenta di comunicazioni relative ad un sistema informatico, nonché nella rivelazione all’esterno delle comunicazioni in tal modo raccolte.

Si tratta di una fattispecie perseguibile a querela della persona offesa, salvo che non si verificano le circostanze aggravanti di cui al comma 4 (danneggiamento di un sistema pubblico; abuso o violazione dei doveri della funzione di pubblico ufficiale, o della qualità di operatore del sistema).

I mezzi tipici utilizzati per la commissione di tale reato sono normalmente *software spyware*, introduzione di *virus*, ma anche ad esempio l’installazione di *software* non autorizzati dall’azienda o non strumentali allo svolgimento delle proprie mansioni e aventi l’effetto di rallentare la comunicazione telematica. La condotta materiale è configurabile anche nell’utilizzo di una carta di credito contraffatta attraverso un proprio terminale POS, o nell’intrusione non autorizzata nella casella di posta elettronica altrui protetta da apposita *password*.

Soggetti attivi	Chiunque (reato comune).
Elemento oggettivo Condotta	Reato di pericolo. Intercettazione, impedimento o interruzione di comunicazioni relative ad un sistema informatico/telematico o intercorrenti tra più sistemi.
Elemento soggettivo	Dolo generico (volontarietà della condotta).
Pena	Reclusione da sei mesi a quattro anni (a querela). Reclusione da uno a cinque anni se il fatto è commesso in danno di un sistema informatico utilizzato dallo Stato, da altro ente pubblico ovvero da impresa esercente servizi pubblici o di pubblica necessità (d’ufficio).

Ad esempio, il rischio potrebbe verificarsi nelle ipotesi in cui i dipendenti/soci/consulenti della cooperativa:

- accedano abusivamente ad un sistema informatico protetto nonostante i tentativi di estromissione del proprietario, gestore o titolare del sistema, (ad esempio utilizzo *password* e *username* di terzi per visualizzare e riprodurre documenti senza autorizzazione);

- ottengano, riproducano, diffondano, comunichino o divulgino 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 "bombe logiche" etc);
- installino mezzi volti ad intercettare, bloccino o interrompano comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui.
- distruggano o danneggino sistemi informatici/telematici altrui tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi;
- distruggano, danneggino sistemi informatici/telematici di pubblica utilità;
- violino gli obblighi previsti dalla legge per il rilascio di un certificato qualificato di firma elettronica.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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 relativi alla sicurezza dei dati;
- Formazione periodica sui reati informatici e sulle procedure aziendali in essere.

Art. 617quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Osservazioni

Il reato, perseguibile d'ufficio, punisce la mera installazione di strumenti volti a rendere possibile l'intercettazione, l'impedimento o l'interruzione di comunicazioni telematiche o informatiche. Si prescinde dunque dalla realizzazione dell'intercettazione in concreto.

Si tratta di una norma a tutela anticipata che mira a tutelare la riservatezza e la libertà delle comunicazioni con l'incriminazione di fatti prodromici rispetto all'effettiva lesione del bene giuridico.

Pertanto, ai fini della configurabilità del reato, occorrerà verificare la sola attività di installazione e non anche l'eventuale successiva intercettazione o impedimento di comunicazioni.

Il reato è configurabile anche se gli apparecchi installati di fatto poi non abbiano funzionato correttamente, purchè non ricorra un'inidoneità tecnica assoluta.

Il dolo è generico e consiste nella coscienza e volontà di installare apparecchiature in grado di intercettare comunicazioni informatiche o telematiche.

Costituisce condotta di reato ex art. 617 *quinquies* c.p. l'installazione abusiva di un telecamera per captare codici di accesso di utenti di un sistema telematico o informatico, nonché l'utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico.

Soggetti attivi	Chiunque
Elemento oggettivo Condotta	Reato di pericolo. Installazione di mezzi volti ad intercettare, bloccare o interrompere comunicazioni per via informatica/telematica.
Elemento soggettivo	Dolo generico.
Pena	Reclusione da uno a quattro anni (d'ufficio). Reclusione da uno a cinque anni se il fatto è commesso in danno di un sistema informatico/telematico utilizzato dallo Stato, da altro ente pubblico ovvero da impresa esercente servizi pubblici o di pubblica necessità (d'ufficio).

Ad esempio, il rischio potrebbe verificarsi nelle ipotesi in cui i dipendenti/soci/consulenti della cooperativa:

- accedano abusivamente ad un sistema informatico protetto nonostante i tentativi di estromissione del proprietario, gestore o titolare del sistema, (ad esempio utilizzo di *password* e *username* di terzi per visualizzare e riprodurre documenti senza autorizzazione);
- ottengano, riproducano, diffondano, comunichino o divulgino 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 "bombe logiche" etc);
- installino mezzi volti ad intercettare, bloccino o interrompano comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo stato o altro ente pubblico o di pubblica utilità;
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui;
- distruggano o 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.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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);
- 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.

Art. 635bis c.p. Danneggiamento di informazioni, dati e programmi informatici.

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

Osservazioni

La condotta punita si concretizza nelle attività di distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui.

In realtà, la formulazione normativa, nella sua ampiezza, rende effettivamente problematico distinguere tra loro talune delle condotte incriminate. Ciò che però conta è l'integrale copertura rispetto a qualsivoglia condotta, sia fisica che più probabilmente informatica, che si risolva in un pregiudizio, anche solo qualitativo, delle informazioni, dei dati o dei programmi informatici. Ciò che quindi rileva non è tanto la "modalità" dell'aggressione produttiva di danno, quanto piuttosto l'oggetto materiale di questa: costituito appunto dalle informazioni, dai dati o dai programmi informatici, anziché dal

sistema informatico o telematico in sé (preso in considerazione nel successivo art. 635 quater c.p.).

Alla fattispecie in esame possono ricondursi, esemplificando, i fenomeni dello *spamming*, quando consiste nella saturazione intenzionale delle risorse informatiche a seguito di un elevato numero di comunicazioni, così da provocare l'interruzione del servizio di comunicazione e altre eventuali disfunzioni.

Il reato è punibile a querela della persona offesa, a meno che non ricorra una delle circostanze aggravanti previste dalla norma (violenza o minaccia contro persone o abuso della qualità di operatore del sistema).

Soggetti attivi	Chiunque.
Elemento oggettivo Condotta-Evento	Reato di danno. Distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui.
Elemento soggettivo	Dolo generico (volontarietà della condotta e consapevolezza dell'altruità del bene compromesso; irrilevanza delle finalità perseguite dal reo).
Pena	Reclusione da sei mesi a tre anni (a querela). Reclusione da uno o quattro anni se il fatto è commesso con violenza o minaccia alle persone ovvero con abuso della qualità di operatore del sistema (d'ufficio).

Le condotte criminose configurabili si ricollegano ad ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci, consulenti:

- accedano abusivamente ad un sistema informatico protetto (ad esempio utilizzo *password* e *username* di terzi per distruggere o alterare documenti senza autorizzazione);
- ottengano, riproducano, diffondano, comunichino o divulgino codici di accesso a sistema informatici protetti;
- 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 "bombe logiche" etc);
- installino mezzi volti a bloccare o interrompere comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o di pubblica utilità;

- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici altrui;
- distruggano, danneggino sistemi informatici/telematici tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi, ovvero tramite la distruzione o il danneggiamento dello stesso *hardware*;
- distruggano, danneggino sistemi informatici/telematici di pubblica utilità.

Le condotte di cui sopra, sia che l'accesso 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 distruggere i file relativi alla partecipazione alla gara di appalto di un concorrente o bloccarne i sistemi informatici durante le fasi di una procedura d'asta elettronica ovvero alterare o danneggiare il sito di e-commerce di un concorrente ovvero eliminare informazioni che diano evidenza del credito vantato da eventuali fornitori ovvero cancellare la memoria.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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 e ad 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);
- Regolamentazione degli accessi alle aree fisiche in cui sono contenuti gli *hardware*;
- Tracciabilità e archiviazione delle attività effettuate sui sistemi informatici e patrimonio informativo (sia a sistema che documentale);
- 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.

Art. 635ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Osservazioni

La fattispecie punisce i fatti di danneggiamento previsti nel precedente art. 635bis c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. Si introduce una tutela rafforzata rispetto ad aggressioni particolarmente insidiose per la qualità delle informazioni colpite. Ciò che rileva è l'utilità sociale dell'oggetto dell'aggressione, per le gravi conseguenze lesive che possono derivarne in termine di interesse pubblico.

Analogamente al precedente articolo 635bis il legislatore si pone come obiettivo l'integrale copertura rispetto a qualsivoglia condotta che si risolva in un pregiudizio, anche solo qualitativo, delle informazioni, dei dati o dei programmi informatici. Ciò che

quindi rileva non è tanto la "modalità" dell'aggressione produttiva di danno, quanto piuttosto l'oggetto materiale di questa: costituito appunto dalle informazioni, dai dati o dai programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

Nel primo comma, il reato è costruito come reato di pericolo, attraverso la previsione della diretta punibilità delle condotte "dirette a" distruggere, deteriorare, ecc. le informazioni i dati o i programmi informatici.

La concreta realizzazione dello scopo integra un'autonoma ipotesi di reato di danno, prevista e sanzionata più pesantemente nel secondo comma.

Alla fattispecie in esame possono ricondursi, esemplificando, i fenomeni dello *spamming*, quando consiste nella saturazione intenzionale delle risorse informatiche a seguito di un elevato numero di comunicazioni, così da provocare l'interruzione del servizio di comunicazione e altre eventuali disfunzioni.

Il reato è sempre perseguibile d'ufficio e per la sua realizzazione è sufficiente porre in essere "atti diretti" a realizzare gli eventi dannosi previsti, a prescindere dal loro concreto verificarsi.

Soggetti attivi	Chiunque.
Elemento oggettivo ipotesi base (c.1) - Condotta	Reato di pericolo. Atti diretti a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato, o da altro ente pubblico o comunque di pubblica utilità.
Elemento oggettivo ipotesi aggravata (c.2) - Evento	Reato di danno. Distruzione, deterioramento, cancellazione, alterazione o soppressione delle informazioni, dei dati o dei programmi informatici.
Elemento soggettivo	Dolo generico (volontarietà della condotta e consapevolezza della pertinenza del bene compromesso allo Stato o soggetti pubblici equiparati; irrilevanza delle finalità perseguite dal reo).
Pena	Reclusione da uno a quattro anni per l'ipotesi base di pericolo (d'ufficio). Reclusione da tre a otto anni per l'ipotesi aggravata di evento-danno (d'ufficio).

Ad esempio, le condotte criminose configurabili si ricollegano a ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci, consulenti:

- accedano abusivamente ad un sistema informatico dello Stato o di altro ente pubblico per distruggere o alterare documenti senza autorizzazione;

- ottengano, riproducano, diffondano, comunichino o divulgino codici di accesso a sistema informatici protetti per i fini punti dal reato in esame ;
- 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 "bombe logiche" etc);
- installino mezzi volti a bloccare o interrompere comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI):
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi.

Le condotte di cui sopra dirette contro un sistema informatico pubblico e che si traducano in un interesse o vantaggio per la società stessa (ad esempio distruggere dati relativi a controlli o ispezioni, ovvero impedire in qualunque modo lo svolgimento di un asta con procedura elettronica), pur essendo tutte astrattamente possibili non sembrano alla portata della maggior parte delle cooperative aderenti a Confcooperative tenuto conto della complessità e rischiosità delle operazioni richieste per "attaccare" un soggetto pubblico, in quanto poco proporzionate alla limitate dimensioni e conseguenti disponibilità di *know how* ma anche degli interessi in gioco che caratterizzano le stesse.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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);
- 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.

Art. 635quater c.p. Danneggiamento di sistemi informatici o telematici.

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Osservazioni

Il sistema sanzionatorio dei reati informatici è completato con l'introduzione di due fattispecie incriminatrici dirette a punire le condotte di danneggiamento che abbiano ad

oggetto non singoli documenti o dati informatici, bensì il funzionamento di un sistema informatico.

I due reati sono costruiti in modo non difforme dalle corrispondenti ipotesi rispettivamente previste negli artt. 635**bis** e 635**ter** c.p.

La previsione autonoma, invero, si giustifica per il significativo aggravamento di pena che in tal modo si è introdotto, in ragione della maggiore insidiosità della condotta.

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.

Alla fattispecie in esame può ricondursi, esemplificando, il fenomeno dello *spamming*, quando consiste nella saturazione intenzionale delle risorse informatiche a seguito di un elevato numero di comunicazioni, così da provocare l'interruzione del servizio di comunicazione e altre eventuali disfunzioni.

Il reato *de quo* punisce l'introduzione o la trasmissione di dati, informazioni o programmi che causino la distruzione, il danneggiamento, l'inservibilità o il grave malfunzionamento di sistemi informatici o telematici. E' necessario che l'evento dannoso si verifichi in concreto.

Soggetti attivi	Chiunque.
Elemento oggettivo Condotta-Evento	Reato di danno. Distruzione, danneggiamento, inservibilità o grave malfunzionamento di sistemi informatici/telematici causati tramite la distruzione, cancellazione o alterazione di dati o programmi esistenti, ovvero tramite l'immissione nel sistema di nuovi dati o programmi.
Elemento soggettivo	Dolo generico (volontarietà della condotta e consapevolezza dell'altruità del sistema compromesso; irrilevanza delle finalità perseguite dal reo).
Pena	Reclusione da uno a cinque anni, aumentata fino a un terzo se il fatto è commesso con violenza o minaccia alle persone ovvero con abuso della qualità di operatore del sistema (d'ufficio).

Ad esempio, le condotte criminose configurabili si ricollegano ad ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci, consulenti:

- accedano abusivamente ad un sistema informatico protetto (ad esempio utilizzo *password* e *username* di terzi per distruggere o alterare il sistema operativo o altri *software*);
- ottengano, riproducano, diffondano, comunichino o divulgino codici di accesso a sistema informatici protetti;

- 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 rendere impossibile o comune eccessivamente difficoltosa la comunicazione telematica);
- ottengano, producano, riproducano, mettano a disposizione apparecchiature dispositivi o programmi lesivi dell'integrità dei sistemi informativi (ad esempio introduzione di *virus*, programmi contenenti le "bombe logiche" etc).
- distruggano, danneggino sistemi informatici/telematici altrui sia fisicamente(il c.d.*hardware*) che tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi.
- distruggano o danneggino sistemi informatici/telematici di pubblica utilità.

Le condotte di cui sopra possono tradursi in operazioni che portino un interesse o un vantaggio per la società stessa, ad esempio bloccare i sistemi informatici di un concorrente durante le fasi di una procedura d'asta elettronica ovvero alterare o bloccare il sito di *e-commerce* concorrente ovvero cancellarne la memoria informatica.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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);
- 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.

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

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Osservazioni

L'articolo in questione punisce le stesse condotte criminose di cui all'art. 635quater c.p., al cui commento si rinvia, anche se gli eventi dannosi, aventi come oggetto materiale sistemi informatici o telematici di pubblica utilità, non si realizzino concretamente.

Soggetti attivi	Chiunque.
Elemento oggettivo ipotesi	Reato di pericolo.

base (c.1) - Condotta	Atti diretti a distruggere, danneggiare, rendere in tutto o in parte inservibili ovvero ad ostacolare gravemente il funzionamento di sistemi informatici/telematici di pubblica utilità.
Elemento oggettivo ipotesi aggravata (c.2) - Evento	Reato di danno. Conseguimento dell'obiettivo lesivo.
Elemento soggettivo	Dolo generico.
Pena	Reclusione da uno a quattro anni per l'ipotesi base di pericolo (d'ufficio). Reclusione da tre a otto anni per l'ipotesi aggravata di danno (d'ufficio).

Ad esempio, le condotte criminose configurabili si ricollegano a ipotesi in cui persone fisiche che appartengono all'organigramma societario e/o aziendale della cooperativa, soci, consulenti:

- accedano abusivamente ad un sistema informatico dello Stato o di altro ente pubblico per distruggere o alterare il sistema;
- ottengano, riproducano, diffondano, comunichino o divulgino codici di accesso a sistema informatici protetti per i fini punti dal reato in esame;
- 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 "bombe logiche" etc);
- installino mezzi volti a bloccare o interrompere comunicazioni per via informatica/telematica (ad esempio utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti al SI);
- distruggano, deteriorino, cancellino informazioni e dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o di pubblica utilità tramite la distruzione, cancellazione di dati o l'immissione di nuovi dati o programmi.

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

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);
- 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.

Art. 640^{quinq}ies c.p. Frode informatica del certificatore di firma elettronica.

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

Osservazioni

Si tratta di un reato proprio che può essere commesso dal soggetto che presta servizi di certificazione di firma elettronica. Le condotte di reato si concretizzano nella generica violazione degli obblighi di legge per il rilascio di un certificato qualificato, con il dolo specifico di procurare a sé un vantaggio o un danno ad altri.

Soggetti attivi	Chiunque.
Elemento oggettivo Condotta	Reato di pericolo. Violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato di firma elettronica (v. D.lgs. 7 marzo 2005, n.82, cd. codice dell'amministrazione digitale).
Elemento soggettivo	Dolo specifico (volontarietà della condotta accompagnata dall'intento di procurare un ingiusto profitto per sé o per altri ovvero di arrecare ad altri danno).
Pena	Reclusione fino a tre anni e multa da 51 a 1.032 euro (d'ufficio).

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 trasmissione comunicazioni ed informazioni con la PA per via elettronica.

Poiché non risulta allo stato che nessuna aderente a Confcooperative sia un soggetto che presta servizi di certificazione di firma elettronica si ritiene di non prevedere alcun protocollo per il contenimento o l'eliminazione del rischio.

ART. 24 TER D.LGS 231/2001 - DELITTI DI CRIMINALITA' ORGANIZZATA.

In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416-bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché ai delitti previsti dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.

In relazione alla commissione di taluno dei delitti di cui all'articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applica la sanzione pecuniaria da trecento a ottocento quote.

Nei casi di condanna per uno dei delitti indicati nei commi 1 e 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno.

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nei commi 1 e 2, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3.

Art. 416 c.p. Associazione per delinquere.

Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni.

Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.

I capi soggiacciono alla stessa pena stabilita per i promotori.

Se gli associati scendono in armi le campagne o le pubbliche vie si applica la reclusione da cinque a quindici anni.

La pena è aumentata se il numero degli associati è di dieci o più.

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.

Osservazioni

Si realizza la fattispecie quando tre o più persone si associano allo scopo di commettere più delitti; è punita anche la mera promozione, costituzione, organizzazione dell'associazione o la partecipazione ad essa.

I delitti contro la criminalità organizzata erano già previsti come potenziali illeciti amministrativi ex D.Lgs 231/2001 dall'art.10 della legge n. 146/2006 ("Ratifica della Convenzione ONU sulla lotta alla criminalità organizzata transnazionale"). In tale disposizione erano già previsti alcuni delitti associativi tra i reati presupposto, purchè tali reati avessero carattere transnazionale.

L'estensione di tali illeciti anche all'ambito nazionale si inquadra in un più articolato programma di lotta alla criminalità di impresa (si pensi alle frodi fiscali, ai reati in danno delle finanze pubbliche commessi in associazione da più imprese, ai reati ambientali ecc.).

L'associazione a delinquere si caratterizza per tre elementi fondamentali, costituiti: a) da un vincolo associativo tendenzialmente permanente, o comunque stabile (formato a almeno tre persone); b) dall'indeterminatezza del programma criminoso (diversamente da quanto avviene ad esempio nel concorso di persone nel reato); c) dall'esistenza di una struttura organizzativa criminosa.

Le pene sono differenziate a seconda del ruolo rivestito dall'associato: promotori, organizzatori e capi sono puniti più gravemente rispetto ai semplici associati.

Per quanto riguarda l'elemento soggettivo esso consiste nella manifestazione dell'*affectio societatis scelerum*, ossia nella coscienza e volontà di far parte di un'associazione e di contribuire alla sua vita.

Per quanto riguarda l'iscrizione alle persone giuridiche del reato di associazione a delinquere, e degli altri delitti associativi di cui all'art. 24 ter D.Lgs 231/2001, occorre operare una distinzione fra la tipologia di enti destinatari di tali fattispecie incriminatrici.

Potrebbero essere chiamati a rispondere dei reati in questione sicuramente enti di per sé non criminali, ma che occasionalmente con la loro condotta appoggino, favoriscano, promuovano, o concorrano ad un'associazione criminosa; d'altro canto, potrebbero essere incriminati anche enti intrinsecamente illeciti, creati con l'unica finalità di consentire o agevolare la commissione di un reato, come ad esempio un'associazione a delinquere in sé.

La prima ipotesi (l'impresa intrinsecamente lecita) è senz'altro quella più aderente alle finalità originarie del D.Lgs 231/2001; potrebbero, pertanto, incorrere nel reato di associazione a delinquere enti in cui figure apicali o soggetti subordinati, pur operando all'interno di un ente lecito inserito in un circuito lecito, si associno con altre persone per commettere reati, anche con l'intento di apportare un interesse o vantaggio al medesimo ente cui appartengono.

Al contrario l'impresa di per sé illecita è considerata un'ipotesi residuale come si evince dai lavori preparatori, dalla Relazione governativa e dall'art. 16 comma 3 dello stesso d.Lgs 231/2001 (che applica l'interdizione definitiva dall'esercizio dell'attività agli enti costituiti "... *allo scopo unico o prevalente di consentire o agevolare la commissione di reati...*").

Per quanto riguarda le realtà cooperative, il rischio maggiore è rappresentato dalla scelta di *partners*, fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare ecc; pertanto, andrà sempre verificato e assicurato che la persona fisica o giuridica con la quale la società intrattiene rapporti sia in possesso di adeguati requisiti di professionalità e di onorabilità.

Esempi di condotte a rischio per la realtà cooperativa: alcuni responsabili di un istituto di credito cooperativo truffano dei clienti al fine di collocare titoli "tossici"; qualora agli stessi venisse contestato l'art. 416 c.p., tale addebito potrebbe trasferirsi per i

meccanismi del D.lgs 231 sullo stesso istituto; alcune figure apicali, in accordo (ed in concorso) con alcuni fornitori, creano un articolato sistema di finte fatturazioni al fine di creare fondi neri a disposizione dell'ente, ad esempio per ulteriori attività corruttive; tre o più società si legano tramite un accordo commerciale (*joint ventures*, ATI ecc.) al fine di aggiudicarsi illegittimamente appalti pubblici.

Soggetti attivi	Chiunque (purchè vi siano almeno tre persone)
Elemento oggettivo	Struttura organizzativa/associativa permanente anche se non stabile, finalizzata alla commissione di più delitti . Condotte soggettive: partecipazione, promozione, costituzione, organizzazione dell'associazione.
Elemento soggettivo	Dolo (<i>affectio societatis</i>)

Principali aree aziendali esposte a rischio:

- Ricerca, gestione e selezione del personale;
- Identificazione e contrattazione con fornitori, collaboratori, consulenti e partners;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Ufficio Legale;
- Gestione omaggi, regalie e sponsorizzazioni;
- Gestione rapporti con organi amministrativi aziendali e gestione di eventuali conflitti di interesse;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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, ed in particolare da parte di *partners* in ATI e non, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- Previsione di clausole con controparti contrattuali che regolamentino la cessione del contratto o il subappalto, prevedendo una esplicita autorizzazione in tal senso;

- 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);
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a *partners* in ATI, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti;
- 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 soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti da e verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- Diffusione di prassi e procedure interne finalizzate alla corretta selezione e gestione di fornitori, controparti contrattuali, *partners* in ATI, collaboratori, enti da sostenere e finanziare, in base a specifici requisiti di professionalità e onorabilità (es. richiesta preventiva certificato antimafia, DURC, iscrizione CCIA, legale rappresentanza, ecc.);
- Inoltro all'O.d.V del riepilogo operazioni a rischio (ad esempio avanzamento delle commesse aperte);

Art. 416bis c.p. Associazioni di tipo mafioso anche straniere.

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

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

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

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

L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplosive, anche se occultate o tenute in luogo di deposito. Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

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

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

Osservazioni

L'associazione è di tipo mafioso quando coloro che ne fanno parte secondo una delle modalità di cui all'art. 416 c.p. si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti e servizi pubblici, o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire, ostacolare o influenzare il libero esercizio del voto.

Il legislatore punisce il solo fatto dell'appartenenza all'associazione mafiosa, che deve presentare i requisiti di cui al terzo comma della norma in esame: avvalimento della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per finalità illecite specifiche.

Gli elementi costitutivi dell'associazione mafiosa sono:

- a) la forza di intimidazione, quale capacità intrinseca dell'organizzazione criminale in grado di esprimersi all'esterno di essa;
- b) la condizione di assoggettamento e di omertà, quale effetto diretto della forza intimidatrice dell'associazione;
- c) le finalità del sodalizio criminale, il cui raggiungimento è indifferente ai fini della configurabilità del delitto.

Si tratta di un reato permanente, che si consuma con l'ingresso nell'associazione e sussiste fino all'abbandono o allo scioglimento.

L'elemento soggettivo è il dolo specifico che consiste nella coscienza delle caratteristiche dell'organizzazione e nella volontà dell'ingresso in essa.

La condotta di partecipazione all'associazione si realizza con l'ingresso e la permanenza stabile all'interno di un'organizzazione criminale di tipo mafioso ex art. 416bis, comma 3 c.p.; la partecipazione può esplicarsi in forme diverse (messa a disposizione del sodalizio criminale, avere rapporti d'affari, fornire mezzi materiali, supportare economicamente l'associazione ecc.), purchè la prestazione sia in grado di

dare un contributo effettivo al mantenimento in attività dell'associazione e dei suoi scopi illeciti.

La promozione, la dirigenza e l'organizzazione dell'associazione rappresentano, invece, forme di partecipazione più attive e rilevanti, e perciò punite più gravemente.

I commi 4 e 5 dell'art. 416*bis* c.p. prevedono, poi, alcune aggravanti specifiche.

Si sottolinea, infine, il fatto che l'art. 24*ter* del D.Lgs 231/2001 prevede la responsabilità dell'ente nelle ipotesi di commissione di reati "avvalendosi delle condizioni previste dall'art. 416*bis*" o "al fine di agevolare l'associazione mafiosa"; tale inserimento amplia di fatto in modo considerevole il numero di reati punibili ai sensi del D.Lgs 231/2001.

Il rischio è chiaramente configurabile per le grandi imprese, eventualmente costituite in ATI, appaltatrici di opere o servizi, anche a favore di enti pubblici (imprese costruttrici impegnate in grandi opere, società *multi utility*, ecc.). Ma anche le piccole realtà imprenditoriali cooperative sono quotidianamente esposte a tali rischi, soprattutto qualora si trovino ad operare in settori e luoghi dove notoriamente l'influenza di organizzazioni criminali di stampo mafioso è diffusa. Particolarmente esposte sono le imprese che operano nel settore dei subappalti e delle forniture, sia nell'ambito di opere pubbliche, sia nell'ambito di *outsourcing* privati.

Le attività delittuose poste in essere dall'associazione, o da suoi componenti, possono essere le più varie: pressioni sulle predisposizioni dei bandi di gara, offerte anomale, accordi fra imprese concorrenti, cartelli sui prezzi, subappalti nascosti o comunque posti in essere fuori dalle ipotesi regolamentate, attività finalizzate al controllo o alla fuoriuscita di imprese concorrenti da determinati mercati ecc.

Soggetti attivi	Chiunque (purchè vi siano almeno tre persone)
Elemento oggettivo	Struttura organizzativa/associativa permanente, anche se non stabile, finalizzata alla commissione di più delitti e caratterizzata dall'uso del metodo mafioso. Condotte soggettive: partecipazione, promozione, direzione, organizzazione dell'associazione mafiosa.
Elemento soggettivo	Dolo (<i>affectio societatis</i>)

Aree aziendali esposte a rischio:

- Ricerca, gestione e selezione del personale;
- Identificazione e contrattazione con fornitori, collaboratori, consulenti e *partners*;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;

- Ufficio Legale;
- Gestione omaggi, regalie e sponsorizzazioni;
- Gestione rapporti con organi amministrativi aziendali e gestione di eventuali conflitti di interesse;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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, ed in particolare da parte di *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- Previsione di clausole con controparti contrattuali che regolamentino la cessione del contratto o il subappalto, prevedendo una esplicita autorizzazione in tal senso;
- 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);
- Previsione di procedura per la verifica preventiva di attività economiche da attivare o attivate in settori e territori geografici notoriamente esposti al rischio di influenza di organizzazioni criminali di stampo mafioso;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti;
- 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 soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti da e verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- Diffusione di prassi e procedure interne finalizzate alla corretta selezione e gestione di fornitori, controparti contrattuali, *partners* in ATI, collaboratori, dirigenti, enti da sostenere e finanziare, in base a specifici requisiti di

professionalità e onorabilità (es. richiesta preventiva certificato antimafia, DURC, iscrizione CCA, legale rappresentanza, ecc.);

- Procedure di trasparenza nella selezione delle SOA (Società Organismi di Certificazione);
- Inoltro all'O.d.V del riepilogo operazioni a rischio (ad esempio avanzamento delle commesse aperte);
- Segnalazione all'O.d.V di operazioni anomale o ad alto indice di rischio.

Ancorché non ne sia prevista l'applicazione obbligatoria con riferimento al reato associativo mafioso, potrebbe inoltre rivelarsi opportuno l'impiego di alcune delle procedure stabilite dalla normativa specifica antiriciclaggio di cui al D.Lgs. n. 231/2007 (al cui riguardo si veda, ampiamente, la disamina riportata in commento ai delitti di cui agli articoli 648, 648bis e 648ter c.p., *infra* nelle presenti Linee Guida).

A titolo di esempio, potrebbero essere mutate da tale disciplina specifica le modalità e le procedure ivi stabilite per l'adeguata verifica della clientela, come anche l'impiego degli indici di rischio ivi previsti ai fini della segnalazione di operazioni sospette. Con riferimento a questi ultimi, trattasi infatti di veri e propri campanelli d'allarme idonei a porre in risalto eventuali situazioni critiche al fine di consentire agli organi gestori e di controllo di effettuare le opportune valutazioni e di adottare le conseguenti decisioni, quali, *in primis*, la non instaurazione o l'interruzione di rapporti contrattuali a rischio.

Art. 416ter c.p. Scambio elettorale politico-mafioso.

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

Osservazioni.

La condotta di reato consiste nell'ottenere la promessa di voti dietro erogazione di denaro, avvalendosi dell'intimidazione o della prevaricazione mafiosa, con le modalità di cui al terzo comma dell'art. 416bis c.p., per impedire o ostacolare il libero esercizio del voto e per falsare il risultato elettorale.

Soggetti attivi	Soggetti politici.
Elemento oggettivo	Ottenimento di appoggio elettorale dietro erogazione di somme di denaro, attraverso il ricorso all'intimidazione o alla prevaricazione mafiosa ex art. 416 bis c.p. .
Elemento soggettivo	Dolo

Aree aziendali esposte a rischio:

Il reato in questione può essere realizzato in diverse aree aziendali ed in modo trasversale a tutti i livelli dell'organizzazione cooperativa, prevalentemente a livello

direzionale, essendo quest'ultimo normalmente investito della gestione dei rapporti con soggetti politici ed enti pubblici; in particolare si segnalano i seguenti processi a rischio:

- Ricerca, gestione e selezione del personale;
- Identificazione e contrattazione con fornitori, collaboratori, consulenti e *partners*;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Ufficio Legale;
- Gestione omaggi, regalie e sponsorizzazioni;
- Gestione rapporti con organi amministrativi aziendali e gestione di eventuali conflitti di interesse;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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, ed in particolare da parte di *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- 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);
- Previsione di procedura per la verifica preventiva di attività economiche da attivare o attivate in settori e territori geografici notoriamente esposti al rischio di influenza di organizzazioni criminali di stampo mafioso;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito ad eventuali candidature o sostegno candidature politiche offerte dalla cooperativa;
- 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 soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Comunicazione immediata all'O.d.V. in caso di svolgimento di incarichi o funzioni pubbliche, o in caso di candidature politiche da parte di figure apicali societarie;

- Comunicazione immediata all'O.d.V. dell'instaurazione di rapporti economici con soggetti candidati ad elezioni politiche o con loro familiari;
- Segnalazione all'O.d.V di operazioni anomale o ad alto indice di rischio.

Anche per il reato in questione potrebbe, inoltre, rivelarsi opportuno l'impiego di alcune delle procedure stabilite dalla normativa specifica antiriciclaggio di cui al D.Lgs. n. 231/2007 (al cui riguardo si veda, ampiamente, la disamina riportata in commento ai delitti di cui agli articoli 648, 648**bis** e 648**ter** c.p., *infra* nelle presenti Linee Guida).

A titolo di esempio, potrebbero essere mutate da tale disciplina specifica le modalità e le procedure ivi stabilite per l'adeguata verifica della clientela, come anche l'impiego degli indici di rischio ivi previsti ai fini della segnalazione di operazioni sospette. Con riferimento a questi ultimi, trattasi infatti di veri e propri campanelli d'allarme idonei a porre in risalto eventuali situazioni critiche al fine di consentire agli organi gestori e di controllo di effettuare le opportune valutazioni e di adottare le conseguenti decisioni, quali, *in primis*, la non instaurazione o l'interruzione di rapporti contrattuali a rischio.

Art. 630 c.p. Sequestro di persona a scopo di estorsione.

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

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

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

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

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

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

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

Osservazioni

Il sequestro di persona ex art. 630 c.p. si realizza in caso di limitazione della libertà personale di un soggetto, in qualsiasi forma e durata, al fine di ottenere un ingiusto profitto.

Si tratta di un reato complesso caratterizzato dal dolo specifico della mercificazione della persona.

Si può ritenere che la realizzazione di tale fattispecie appare di difficile previsione, vista la necessità di accertare in ogni caso l'interesse o vantaggio ricavato dall'ente dalla realizzazione dell'illecito stesso.

Soggetti attivi	Chiunque
Elemento oggettivo	Privazione della libertà personale altrui allo scopo di ottenere un profitto ingiusto quale prezzo della liberazione.
Elemento soggettivo	Dolo specifico

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

Il reato in questione è una forma di associazione a delinquere speciale, caratterizzata dalla finalità specifica dell'organizzazione criminale.

In ogni caso per l'imputazione del reato in questione ad una società è necessario accertare l'interesse o vantaggio della stessa.

Particolare attenzione dovrà essere posta nella scelta di partner, fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare; pertanto, andrà sempre verificato e assicurato che la persona fisica o giuridica con la quale la Società intrattiene rapporti sia in possesso di adeguati requisiti di professionalità e di onorabilità.

Aree aziendali esposte a rischio:

- Ricerca, gestione e selezione del personale;
- Identificazione e gestione contrattazione con fornitori, collaboratori, consulenti e *partners*;
- Gestione *import/export* e logistica aziendale;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti da e verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad

eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;

- Gestione omaggi, regalie e sponsorizzazioni;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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, ed in particolare da parte di *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- 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);
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti;
- *Audit* e/o 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 soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Diffusione di prassi e procedure interne finalizzate alla corretta selezione e gestione di fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare, in base a specifici requisiti di professionalità e onorabilità (es. richiesta preventiva certificato antimafia, DURC, iscrizione CCIA, legale rappresentanza, ecc.);

Art. 407, co. 2, lett. a), numero 5), c.p.p. 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.

Particolare attenzione dovrà essere posta anche in questo caso nella scelta di *partners*, fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare; pertanto, andrà sempre verificato e assicurato che la persona fisica o giuridica con la quale la Società intrattiene rapporti sia in possesso di adeguati requisiti di professionalità e di onorabilità.

Aree aziendali esposte a rischio:

- Ricerca, gestione e selezione del personale;

- Identificazione e contrattazione con fornitori, collaboratori, consulenti e *partners*;
- Gestione *import/export* e logistica aziendale;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Gestione omaggi, regali e sponsorizzazioni;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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, ed in particolare da parte di *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- 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);
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di una relazione periodica in merito a *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti;
- *Audit* e/o 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 soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti da e verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- Diffusione di prassi e procedure interne finalizzate alla corretta selezione e gestione di fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare, in base a specifici requisiti di professionalità e onorabilità (es. richiesta preventiva certificato antimafia, DURC, iscrizione CCIA, legale rappresentanza, ecc.);

ART. 25 D.LGS 231/2001 - CONCUSSIONE E CORRUZIONE.

In relazione alla commissione dei delitti di cui agli articoli 318, 321 e 322, commi 1 e 3, del codice penale, si applica la sanzione pecuniaria fino a duecento quote.

In relazione alla commissione dei delitti di cui agli articoli 319, 319 ter, comma 1, 321, 322, commi 2 e 4, del codice penale, si applica all'ente la sanzione pecuniaria da duecento a seicento quote.

In relazione alla commissione dei delitti di cui agli articoli 317, 319, aggravato ai sensi dell'articolo 319 bis quando dal fatto l'ente ha conseguito un profitto di rilevante entità, 319 ter, comma 2, e 321 del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

Le sanzioni pecuniarie previste per i delitti di cui ai commi da 1 a 3, si applicano all'ente anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322 bis.

Nei casi di condanna per uno dei delitti indicati nei commi 2 e 3, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno.

Art. 317 c.p. Concussione.

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

Osservazioni

Vi è concussione quando un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovute.

Soggetto attivo del reato può dunque essere tanto un pubblico ufficiale quanto un incaricato di pubblico servizio.

L'abuso può estrinsecarsi in due forme: come uso antidoveroso dei poteri pubblici (utilizzo di poteri attinenti alle funzioni esercitate per scopi diversi da quelli previsti per legge, in violazione dei principi di buon andamento e imparzialità) oppure come abuso di qualità (strumentalizzazione della posizione di preminenza pubblica ricoperta dal soggetto, a prescindere dalle sue competenze specifiche).

L'abuso così definito deve essere finalizzato al costringimento o all'induzione alla illegittima dazione. Nel primo caso vi è una chiara prospettazione alla vittima di un male ingiusto, nel secondo caso vi è una implicita suggestione o persuasione psicologica.

In ogni caso, per la sussistenza del delitto non è necessaria l'iniziativa del pubblico ufficiale o dell'incaricato di pubblico servizio, il quale può limitarsi a tenere un mero

comportamento passivo alla richiesta della vittima, inducendo con tale comportamento la vittima alla dazione o promessa.

Effetto del costringimento deve essere la dazione o la promessa indebita, cioè non dovuta, per legge o per consuetudine, di denaro o altra utilità; per dazione si intende l'effettiva consegna del bene in modo definitivo, la promessa invece è l'impegno ad eseguire la futura prestazione.

Colui che subisce la costrizione non è correo ma persona offesa; pertanto tale fattispecie potrà configurarsi in capo alle cooperative in via residuale, o nella forma del concorso dell'*extraneus* tra una figura apicale o subordinata della società e il pubblico ufficiale o incaricato di pubblico servizio (sempre che via sia un interesse/vantaggio per la società), oppure in quei casi in cui la cooperativa gestisca attività a rilevanza pubblicistica (es. la Corte di Cass. Pen. Sez. VI, 22/01/2003 ha ritenuto responsabile per concussione un ente fieristico per aver indotto un privato ad accogliere la pretesa di versamento di una tangente al fine di aggiudicargli una fornitura, in quanto –pur rientrando la stipula del contratto nell'attività di gestione privatistica- la procedura per la corretta individuazione del fornitore attiene ad aspetto pubblicistico)

Infatti, sia il legislatore sia la giurisprudenza prevalente, ritengono che gli esponenti di fattispecie societarie a carattere privato ma depositarie dello svolgimento di un pubblico servizio, sono assolutamente equiparati a pubblici ufficiali o un incaricati di un pubblico servizio (es. soggetti che possono rappresentare all'esterno la volontà della PA o suoi poteri autoritativi, deliberativi o certificativi a prescindere da formali investimenti; componenti di vertice di enti ospedalieri o società esercenti prestazioni sanitarie convenzionate con il Servizio Sanitario Nazionale; operatori di Istituti di credito; soggetti appartenenti a società a partecipazione pubblica o concessionarie di pubblici servizi; operatori di società per la gestione di guardie giurate; operatori di società deputate alla gestione, organizzazione ed erogazione di formazione e addestramento professionale regolato dalla legge, ecc.).

Soggetto attivo	Pubblico ufficiale o incaricato di pubblico servizio
Elemento oggettivo	1) Abuso della qualità e dei poteri 2) Costrizione ed induzione 3) Dazione o promessa indebita per sé o terzi di denaro o altra utilità
Elemento soggettivo	Dolo generico
Pena	Sanzione pecuniaria da 300 ad 800 quote; Sanzioni interdittive non inferiori ad un anno.

Il reato in questione, come tutti i reati con la pubblica Amministrazione, può essere realizzato in diverse aree aziendali ed in modo trasversale a tutti i livelli dell'organizzazione cooperativa; in particolare, si segnalano i seguenti **processi a rischio**:

- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);

- Richiesta e gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie da parte di enti pubblici;
- Gestione sistemi informativi aziendali pubblici;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Erogazione di servizi aggiudicati con procedura ad evidenza pubblica;
- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione contenziosi;
- Gestione verifiche di pubbliche autorità;
- Gestione omaggi, regalie e sponsorizzazioni;
- Assegnazione e gestione incarichi di consulenza e collaborazione.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di report periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;
- *Audit* e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita (pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);
- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari;

- Diffusione di prassi e procedure finalizzate a garantire processi di selezione ed assunzione del personale improntati alla massima imparzialità ed oggettività.

Art. 318 c.p. Corruzione per un atto d'ufficio.

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni.

Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino a un anno.

Osservazioni

E' l'ipotesi di un accordo fra un pubblico ufficiale o incaricato di pubblico servizio e un privato, in forza del quale il primo riceve, per sé o per altri, denaro o altri vantaggi per compiere, omettere, o ritardare atti del suo ufficio con vantaggio in favore del corruttore privato (c.d. corruzione impropria).

Diversamente dalla concussione, le parti sono in posizione paritaria, pertanto entrambe punibili. Si tratta, infatti, di un reato plurisoggettivo a concorso necessario.

Il reato può realizzarsi in due forme: corruzione attiva (condotta del privato corruttore) e corruzione passiva (condotta del pubblico ufficiale/incaricato di pubblico servizio che accetta la retribuzione non dovuta per compiere un atto del suo ufficio).

Tale fattispecie potrà configurarsi in capo alle cooperative, o nella forma attiva, quando una figura apicale o subordinata della società metta in atto materialmente l'attività di corruzione del pubblico ufficiale o incaricato di pubblico servizio, oppure in quei casi in cui la cooperativa gestisca attività a rilevanza pubblicistica e l'operatore della cooperativa sia pertanto considerato pubblico ufficiale/incaricato di pubblico servizio (si veda quanto riportato nell'analisi del reato di concussione in relazione alla definizione di pubblico ufficiale/incaricato di pubblico servizio).

Oggetto materiale della condotta è "il denaro o altra utilità". Col termine utilità va inteso tutto ciò che rappresenta un vantaggio per la persona, materiale e morale, patrimoniale e non, consistente in un *facere* o in un *dare*. Vi rientra pertanto anche la realizzazione o promessa di assunzione di persona gradita al pubblico ufficiale, o la dazione diretta o indiretta di omaggi, sponsorizzazioni, regali che travalichino l'ordinaria cortesia.

Soggetto attivo	Pubblico ufficiale – Soggetto corruttore
Elemento oggettivo	<ol style="list-style-type: none"> 1) <i>Pactum sceleris</i> fra pubblico ufficiale e privato 2) Ricezione/accettazione promessa per sé o per un terzo di retribuzione in denaro o altra utilità indebita 3) Finalità del compimento di un atto d'ufficio (corruzione impropria)
Elemento soggettivo	Dolo generico

Il reato in questione, come tutti i reati con la pubblica Amministrazione, può essere realizzato in diverse aree aziendali ed in modo trasversale a tutti i livelli dell'organizzazione cooperativa; in particolare si segnalano i seguenti **processi a rischio**:

- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Richiesta e gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie da parte di enti pubblici;
- Gestione sistemi informativi aziendali pubblici;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione finanziaria-contabile, controllo di gestione, internal auditing, rendicontazione;
- Gestione investimenti ambientali;
- Ricerca e sviluppo tecnologico;
- Gestione rapporti con le Autorità di Vigilanza;
- Gestione contenziosi;
- Gestione omaggi, regalie e sponsorizzazioni;
- Selezione e gestione del personale, formazione finanziata;
- Assegnazione e gestione incarichi di consulenza e collaborazione.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di *reports* periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;
- *Audit e/o* incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;

- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita (pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);
- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari;
- Diffusione di prassi e procedure finalizzate a garantire processi di selezione ed assunzione del personale improntati alla massima imparzialità ed oggettività.

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

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

Art. 319 bis c.p. Circostanze aggravanti.

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

Osservazioni

E' l'ipotesi di un pubblico ufficiale o incaricato di pubblico servizio che riceve, per sé o per altri, denaro o altri vantaggi per compiere, omettere, o ritardare atti contrari ai suoi doveri con vantaggio in favore del corruttore (c.d. corruzione propria).

Tale fattispecie si configura ogni qualvolta l'attività svolta dal pubblico ufficiale/incaricato di pubblico servizio sia contraria ai doveri di quest'ultimo (es. accettazione di denaro per garantire l'aggiudicazione di una gara).

In una delle prime sentenze di merito in tema di responsabilità delle persone giuridiche per corruzione propria, si è affermato che l'ente può essere ritenuto responsabile, senza violare il principio di irretroattività, se all'accordo corruttivo, perfezionato prima dell'entrata in vigore del D.lgs 231/01, seguano una o più dazioni di denaro realizzate in un periodo ad essa successivo. Infatti, sebbene il reato di corruzione si perfezioni con la semplice accettazione del *pactum sceleris*, ove segua l'effettiva dazione del denaro, il momento consumativo si sposta in avanti fino all'ultima dazione.

Soggetto attivo	Pubblico ufficiale – Soggetto corruttore
-----------------	--

Elemento oggettivo	1) Pactum sceleris fra pubblico ufficiale e privato 2) Ricezione/accettazione promessa per sé o per un terzo di retribuzione in denaro o altra utilità indebita 3) Finalità del compimento di un atto contrario ai doveri d'ufficio (corruzione propria)
Elemento soggettivo	Dolo generico

Il reato in questione, come tutti i reati con la pubblica Amministrazione, può essere realizzato in diverse aree aziendali ed in modo trasversale a tutti i livelli dell'organizzazione cooperativa; in particolare si segnalano i seguenti **processi a rischio**:

- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Richiesta e gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie da parte di enti pubblici;
- Gestione sistemi informativi aziendali pubblici;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione finanziaria-contabile, controllo di gestione, internal auditing, rendicontazione;
- Gestione investimenti ambientali;
- Ricerca e sviluppo tecnologico;
- Gestione rapporti con le Autorità di Vigilanza;
- Gestione contenziosi;
- Gestione omaggi, regalie e sponsorizzazioni;
- Selezione e gestione del personale, formazione finanziata;
- Assegnazione e gestione incarichi di consulenza e collaborazione.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa;

- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di *reports* periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;
- *Audit e/o* incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita (pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);
- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari;
- Diffusione di prassi e procedure finalizzate a garantire processi di selezione ed assunzione del personale improntati alla massima imparzialità ed oggettività.

Art. 319ter. Corruzione in atti giudiziari.

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da tre a otto anni.

Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni.

Osservazioni

E' l'ipotesi in cui il reato di corruzione sia posto in essere da una parte di un procedimento giudiziario, nei confronti di un magistrato, cancelliere o altro funzionario pubblico.

Tale fattispecie si caratterizza, infatti, dal fine specifico di favorire una parte in un processo civile, penale o amministrativo.

Soggetto attivo	Pubblico Ufficiale . Soggetto corruttore
-----------------	--

Elemento oggettivo	Atti corruttivi (propri e impropri) rivolti ad un magistrato, cancelliere o altro pubblico funzionario coinvolto in atti/procedimenti giudiziari.
Elemento soggettivo	Dolo specifico: coscienza e volontà di favorire o danneggiare una parte in un processo civile, penale o amministrativo.
Pena	Cfr. artt. 318-319 c.p.

Il reato in questione, come tutti i reati con la pubblica Amministrazione, può essere realizzato in diverse aree aziendali ed in modo trasversale a tutti i livelli dell'organizzazione cooperativa; in particolare si segnalano i seguenti **processi a rischio**:

- Gestione finanziaria-contabile, controllo di gestione, rendicontazione;
- Gestione ispezioni e rapporti con le autorità pubbliche di controllo;
- Gestione contenziosi e conciliazioni;
- Gestione omaggi, regalie e sponsorizzazioni;
- Selezione e gestione del personale, formazione finanziata;
- Assegnazione e gestione incarichi di consulenza e collaborazione.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa, specialmente in caso di contenziosi giudiziari;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione, specialmente in caso di contenziosi giudiziari;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di *reports* periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;
- *Audit e/o* incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita (pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);

- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari.

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

Le disposizioni dell'art. 319 si applicano anche all'incaricato di un pubblico servizio; quelle dell'art. 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualifica di pubblico impiegato.

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

Osservazioni

Cfr. artt. 318 e 319 c.p.

Art. 321 c.p. pene per il corruttore.

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

Osservazioni

La norma in questione estende al corruttore le pene stabilite per il corrotto. Si tratta, pertanto, della disposizione principale attraverso cui gli enti possono essere chiamati a rispondere – insieme al pubblico ufficiale/incaricato di pubblico servizio – dei reati di cui agli artt. 318, 319, 319-bis, 319-ter, 320 c.p.

Aree esposte a rischio e protocolli per il contenimento o l'eliminazione del rischio:

Cfr. artt. 318 e 319 c.p.

Art. 322 c.p. Istigazione alla corruzione.

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.

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

La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 318.

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

Osservazioni

La condotta di reato è quella di cui agli artt. 318-319 c.p., tuttavia in tale fattispecie il pubblico ufficiale rifiuta l'offerta illecitamente avanzatagli.

L'istigazione alla corruzione si realizza mediante le stesse condotte previste nei reati di corruzione propria o impropria, con la specifica circostanza della non accettazione della promessa/offerta del privato.

Aree aziendali esposte a rischio:

Cfr. artt. 318 e 319 c.p.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa;
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di *reports* periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;
- *Audit* e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita

(pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);

- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari;
- Diffusione di prassi e procedure finalizzate a garantire processi di selezione ed assunzione del personale improntati alla massima imparzialità ed oggettività.

Art. 322bis c.p. Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri.

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

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

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

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

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

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

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

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

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

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

Osservazioni

L'articolo in questione è stato introdotto dall'art. 3, c.1 l. 29 settembre 2000, n. 300.

Tale norma estende le disposizioni degli artt. 314,316,317, 317bis, 318, 319, 319bis, 319ter, 320 e 322, c. 3 e 4 c.p. a membri ed esponenti di organi della Comunità europea.

Aree aziendali esposte a rischio (il riferimento è sempre ad attività aziendali di rilevanza europea):

- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione rapporti correnti con la Pubblica Amministrazione (autorizzazioni, licenze ed altri adempimenti);
- Richiesta e gestione contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie da parte di enti pubblici;
- Gestione sistemi informativi aziendali pubblici;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Gestione investimenti ambientali;
- Ricerca e sviluppo tecnologico;
- Gestione rapporti con le Autorità di Vigilanza;
- Gestione contenziosi;
- Gestione omaggi, regalie e sponsorizzazioni;
- Selezione e gestione del personale, formazione finanziata;
- Assegnazione e gestione incarichi di consulenza e collaborazione.

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 a gestire e intrattenere rapporti con funzionari pubblici in nome e per conto della cooperativa
- Dichiarazione di assunzione di responsabilità o attribuzione di responsabilità tramite ordine di servizio alle funzioni aziendali competenti a trasmettere dichiarazioni ufficiali di impegno della società di fronte alla Pubblica Amministrazione;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di *reports* periodici contenenti le seguenti informazioni: dati della persona fisica che ha intrattenuto rapporti anche informali con pubblici funzionari, oggetto dell'incontro/rapporto, eventuali problematiche emerse;

- *Audit e/o* incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni inerenti rapporti con enti pubblici, nonché dei flussi finanziari in entrata ed uscita (pagamenti a e da enti pubblici, riconoscimento di provvigioni e premi a collaboratori e dipendenti);
- Segregazione e separazione delle funzioni fra chi svolge funzioni di rappresentanza legale dell'ente e chi gestisce il sistema di comunicazioni ordinarie con la Pubblica Amministrazione (inoltre richieste, documentazioni, certificazioni, istanze, rapporti ecc.);
- Diffusione di prassi e procedure interne finalizzate alla corretta gestione dei rapporti con la Pubblica Amministrazione e al rifiuto di qualsiasi comportamento anche astrattamente finalizzato ad attività di corruzione o influenza di pubblici funzionari;
- Diffusione di prassi e procedure finalizzate a garantire processi di selezione ed assunzione del personale improntati alla massima imparzialità ed oggettività.

ART. 25 BIS D.LGS 231/2001 - FALSITA' IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO.

In relazione alla commissione dei delitti previsti dal codice penale in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di cui all'articolo 453 la sanzione pecuniaria da trecento a ottocento quote;

b) per i delitti di cui agli articoli 454, 460 e 461 la sanzione pecuniaria fino a cinquecento quote;

c) per il delitto di cui all'articolo 455 le sanzioni pecuniarie stabilite dalla lettera a), in relazione all'articolo 453, e dalla lettera b), in relazione all'articolo 454, ridotte da un terzo alla metà;

d) per i delitti di cui agli articoli 457 e 464, secondo comma, le sanzioni pecuniarie fino a duecento quote;

e) per il delitto di cui all'articolo 459 le sanzioni pecuniarie previste dalle lettere a), c) e d) ridotte di un terzo;

f) per il delitto di cui all'articolo 464, primo comma, la sanzione pecuniaria fino a trecento quote;

f-bis) per i delitti di cui agli articoli 473 e 474, la sanzione pecuniaria fino a cinquecento quote.

Nei casi di condanna per uno dei delitti di cui agli articoli 453, 454, 455, 459, 460, 461, 473 e 474 del codice penale, si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno.

Art. 453 c.p. Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate.

E' punito con la reclusione da tre a dodici anni e con la multa da euro 516 a euro 3.098:

1. chiunque contraffà monete nazionali o straniere, aventi corso legale nello Stato o fuori;

2. chiunque altera in qualsiasi modo monete genuine, col dare ad esse l'apparenza di un valore superiore;

3. chiunque, non essendo concorso nella contraffazione o nell'alterazione, ma di concerto con chi l'ha eseguita ovvero con un intermediario, introduce nel territorio dello Stato o detiene o spende o mette altrimenti in circolazione monete contraffatte o alterate;

4. chiunque, al fine di metterle in circolazione, acquista o comunque riceve, da chi le ha falsificate, ovvero da un intermediario, monete contraffatte o alterate.

Art. 454. c.p. Alterazione di monete.

Chiunque altera monete della qualità indicata nell'articolo precedente, scemandone in qualsiasi modo il valore, ovvero, rispetto alle monete in tal modo alterate, commette alcuno dei fatti indicati nei n. 3 e 4 del detto articolo, è punito con la reclusione da uno a cinque anni e con la multa da euro 103 a euro 516 .

Art. 455 c.p. Spendita e introduzione nello Stato, senza concerto, di monete falsificate.

Chiunque, fuori dei casi preveduti dai due articoli precedenti, introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione, soggiace alle pene stabilite nei detti articoli, ridotte da un terzo alla metà.

Art. 457 c.p. Spendita di monete falsificate ricevute in buona fede.

Chiunque spende, o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede, è punito con la reclusione fino a sei mesi o con la multa fino a euro 1.032.

Art. 459 c.p. Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati.

Le disposizioni degli articoli 453, 455 e 457 si applicano anche alla contraffazione o alterazione di valori di bollo e alla introduzione nel territorio dello Stato, o all'acquisto, detenzione e messa in circolazione di valori di bollo contraffatti; ma le pene sono ridotte di un terzo.

Agli effetti della legge penale, si intendono per valori di bollo la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali.

460 c.p. Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo.

Chiunque contraffà la carta filigranata che si adopera per la fabbricazione delle carte di pubblico credito o dei valori di bollo, ovvero acquista, detiene o aliena tale carta contraffatta, è punito, se il fatto non costituisce un più grave reato, con la reclusione da due a sei anni e con la multa da euro 309 a euro 1.032.

Art. 461 c.p. Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata.

Chiunque fabbrica, acquista, detiene o aliena filigrane, programmi informatici o strumenti destinati esclusivamente alla contraffazione o alterazione di monete, di valori di bollo o di carta filigranata è punito, se il fatto non costituisce un più grave reato, con la reclusione da uno a cinque anni e con la multa da euro 103 a euro 516.

La stessa pena si applica se le condotte previste dal primo comma hanno ad oggetto ologrammi o altri componenti della moneta destinati ad assicurare la protezione contro la contraffazione o l'alterazione.

Art. 464 c.p. Uso di valori di bollo contraffatti o alterati.

Chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo contraffatti o alterati è punito con la reclusione fino a tre anni e con la multa fino a euro 516.

Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo.

Osservazioni

L'elemento oggettivo dei reati nummari è costituito dalle seguenti condotte:

- contraffazione (creazione di monete o banconote false);
- alterazione del valore (manipolazione di monete e banconote genuine creando l'apparenza di un valore diverso);
- introduzione nel territorio dello Stato, detenzione, spendita o messa in circolazione di monete o banconote contraffatte o alterate;
- acquisto o ricevimento dal falsario o da un suo intermediario di monete o banconote contraffatte o alterate.

Oggetto materiale delle condotte criminose possono essere, oltre alle monete e banconote (nazionali o straniere, aventi corso legale in Italia come all'estero), anche i valori di bollo, la carta filigranata impiegata per la creazione delle banconote e più in generale le filigrane e gli altri strumenti destinati esclusivamente alla contraffazione o all'alterazione di monete, banconote e valori di bollo.

A parte l'ipotesi base della falsificazione vera e propria (e del concorso in essa), le condotte descritte dalle norme in commento sono punite con sanzioni diverse a seconda dell'elemento soggettivo, andandosi dal fatto commesso di concerto col falsario, vale a dire d'intesa con questi, alla spendita di valori falsi ricevuti tuttavia in buona fede.

Alla base di tutti i reati *de quo* v'è lo stato soggettivo di dolo generico, consistente nella consapevolezza della falsità; non rientrano ovviamente nelle fattispecie penali in esame l'impiego e la spendita di valori falsi posti in essere in buona fede e nell'ignoranza della falsità.

Oltre al dolo generico (necessario e sufficiente nell'ipotesi di cui all'articolo 457), è poi richiesto il dolo specifico, consistente nel fine di mettere in circolazione le monete, banconote o altri valori falsi o alterati.

Rileva, chiaramente, anche lo stato soggettivo di dolo eventuale, rappresentato dal semplice dubbio circa la genuinità dei mezzi di pagamento ciononostante spesi o messi in circolazione.

E' esclusa la punibilità nelle ipotesi di falso grossolano: la giurisprudenza è tuttavia alquanto rigorosa nel tracciare i contorni di tale esimente, richiedendo l'inidoneità assoluta della falsificazione ad ingannare chicchessia o, più di frequente, precisando che la grossolanità sussiste qualora la falsità sia *ictu oculi* riconoscibile dalla generalità dei cittadini, come espressa dall'uomo di comune esperienza.

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

Chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.500 a euro 25.000. Soggiace alla pena della reclusione da uno a quattro anni e della multa da euro 3.500 a euro 35.000 chiunque contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati.

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

Osservazioni

L'art. 473 c.p., così come modificato dalla L. n.99/2009, mira a tutelare lo specifico bene giuridico rappresentato dalla pubblica fede in senso oggettivo, ossia dalla fiducia dei consumatori nei marchi, segni distintivi, brevetti, modelli o disegni, a prescindere dal fatto che il singolo consumatore venga o meno tratto in inganno sulla genuinità del prodotto. Pertanto il reato può configurarsi anche se l'acquirente viene anticipatamente edotto della non autenticità del marchio.

Si tratta di un reato di pericolo concreto, per la cui configurazione è però richiesto l'oggettivo rischio di inganno del consumatore medio. Ad esempio, per la giurisprudenza il reato de quo non sarebbe configurabile nel caso in cui la condotta sia assolutamente inidonea a creare confusione (es. contraffazione palesemente grossolana o con l'uso dell'espressione "tipo").

La condotta di reato è descritta come contraffazione o alterazione, oppure come uso di prodotti con marchi e segni contraffatti o alterati.

La contraffazione consiste nella riproduzione integrale ed abusiva del marchio genuino.

L'alterazione è la modificazione del marchio ottenuta mediante l'eliminazione o l'aggiunta di elementi costitutivi; dunque, la condotta consiste in un'imitazione fraudolenta o falsificazione parziale.

L'uso punibile ai sensi dell'art. 473 c.p. presuppone che l'autore non abbia commesso o concorso a commettere la falsificazione; è punito anche l'uso del marchio nella corrispondenza commerciale o nella pubblicità.

Oggetto materiale del reato sono marchi o segni distintivi, nazionali o esteri, di prodotti industriali, e brevetti, disegni o modelli industriali, nazionali o esteri.

Il marchio viene definito un segno emblematico o nominativo usato dall'imprenditore per contraddistinguere un prodotto di una determinata specie merceologica. L'art. 7 del Codice della Proprietà Industriale elenca come possibile oggetto di tutela in qualità di marchio anche i nomi di persone, disegni, lettere e cifre, figure, forma del prodotto o confezione, aspetti cromatici ecc, purchè rappresentabili dal punto di vista grafico e dotati di capacità distintiva.

La riforma della disciplina civilistica del marchio (D.Lgs. 10 febbraio 2005, n.10) ha introdotto il concetto di cedibilità del marchio indipendentemente dalla cessione dell'azienda produttrice; in altri termini, il marchio non è più indice di provenienza e origine di un prodotto, ma continua a mantenere una disciplina di tutela penalistica in quanto depositario di un valore in sé per l'insieme dei consumatori.

Oltre al marchio, il primo comma dell'art. 473 c.p. tutela i "segni distintivi, nazionali o esteri, di prodotti industriali"; secondo parte della dottrina la locuzione farebbe riferimento a tutti i contrassegni dei prodotti industriali diversi dai marchi (denominazioni d'origine, segni commerciali ecc.). In realtà, per giurisprudenza prevalente, la locuzione sarebbe pleonastica, in quanto unico oggetto materiale di tutela dell'art. 473, c.1 c.p. è il marchio registrato (cfr. comma 3, art. 473 c.p.); pertanto, non vi rientrano: marchi collettivi, denominazioni d'origine e provenienza, numeri di matricola, bollini, ditta, ragione, denominazione sociale, insegna, emblema.

Il secondo comma dell'art. 473 c.p. estende la medesima tutela a brevetti per invenzioni industriali, e per modelli di utilità, ed alle registrazioni per disegni e modelli ornamentali (nuove forme, grafica, colore del prodotto). Il brevetto è un formale atto della Pubblica Autorità (Ufficio centrale brevetti) che fa sorgere il diritto esclusivo a trarre profitto da un'invenzione industriale e dal suo commercio. A tale atto e alla relativa procedura fa riferimento il comma 3.

Il terzo comma contiene un vero e proprio presupposto del reato consistente nell'osservanza delle norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale o intellettuale; in altri termini, per la configurabilità del reato in questione occorre che il marchio o il segno distintivo di cui si assume la falsità sia stato depositato, registrato o brevettato nelle forme di legge.

L'elemento soggettivo è il dolo generico, quale coscienza e volontà di contraffare, alterare e usare cose con la consapevolezza della falsificazione.

Esempi di condotte: presentazione di un prodotto industriale in una confezione diversa da quella originariamente indicata dal marchio depositato; commercializzazione delle effigi di marchi contraffatti indipendentemente dal fatto che le stesse siano impresse sul prodotto finale; vendita di prodotti con una forma ed un colore specifico tali da indurre falsamente il consumatore ad identificarlo come proveniente da una data impresa.

Il reato in questione va letto in rapporto all'art. 517 c.p.; infatti, quest'ultima norma tutela la generica onestà degli scambi commerciali, pertanto per la sua configurabilità è

sufficiente l'uso di nomi, marchi o segni distintivi che, senza essere contraffatti, risultano idonei ad indurre in errore i consumatori circa l'origine, la provenienza o la qualità del prodotto.

Soggetto attivo	Chiunque
Elemento oggettivo	<p>Contraffazione o alterazione di marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero uso di tali marchi o segni contraffatti o alterati.</p> <p>Contraffazione o alterazione di brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, uso di tali brevetti, disegni o modelli contraffatti o alterati.</p>
Elemento soggettivo	Dolo generico

Aree aziendali a rischio:

- *Import/export,*
- Produzione, *Packaging,* distribuzione;
- Ricerca e sviluppo;
- Qualità di prodotto;
- Commerciale.

Art. 474 c.p. Introduzione nello Stato e commercio di prodotti con segni falsi.

Fuori dei casi di concorso nei reati previsti dall'articolo 473, chiunque introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati è punito con la reclusione da uno a quattro anni e con la multa da euro 3.500 a euro 35.000.

Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello Stato, chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti di cui al primo comma è punito con la reclusione fino a due anni e con la multa fino a euro 20.000.

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

Osservazioni

Le osservazioni svolte per il reato di cui all'art. 473 c.p. sono estendibili anche alla presente fattispecie, con la precisazione che l'art. 474 c.p. prevede la punibilità di due specifiche condotte:

- l'introduzione nello Stato italiano dei prodotti con segni falsi;

- il commercio dei prodotti con segni falsi (inteso nel triplice concetto di detenzione finalizzata alla vendita, compravendita vera e propria e generica messa in circolazione).

Presupposto necessario è che la condotta non venga posta in essere da chi ha commesso la contraffazione.

La commercializzazione di prodotti a contraffazione grossolana non sarebbe punibile in quanto la condotta mancherebbe dell' idoneità ad ingannare un consumatore mediamente avveduto.

Soggetto attivo	Chiunque
Elemento oggettivo	Introduzione nello Stato italiano dei prodotti con segni falsi; commercio di prodotti con segni falsi.
Elemento soggettivo	Dolo generico

Aree aziendali a rischio:

- *Import/export*;
- Produzione, *Packaging*, distribuzione;
- Ricerca e sviluppo;
- Qualità di prodotto;
- Commerciale.

ART. 25 BIS-1 D.LGS 231/2001 - DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO.

In relazione alla commissione dei delitti contro l'industria e il commercio previsti dal codice penale, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per i delitti di cui agli articoli 513, 515, 516, 517, 517-ter e 517-quater la sanzione pecuniaria fino a cinquecento quote;
- b) per i delitti di cui agli articoli 513-bis e 514 la sanzione pecuniaria fino a ottocento quote.

Nel caso di condanna per i delitti di cui alla lettera b) del comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

Art. 513 c.p. Turbata libertà dell'industria o del commercio.

Chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio è punito, a querela della persona offesa, se il fatto non costituisce più grave reato, con la reclusione fino a due anni e con la multa da 103 euro a 1.032 euro.

Osservazioni

Il reato *de quo*, modificato dalla legge n.99/09, mira a tutelare non più l'interesse pubblico dell' economia, ma l'interesse privato dell'esercizio di un'industria o commercio. Ciò è dimostrato innanzitutto dalla procedibilità a querela.

Elemento essenziale per la configurazione dell'illecito è l'uso della violenza sulle cose (danneggiamento, trasformazione o mutamento di destinazione) o di mezzi fraudolenti (artifici e raggiri di ogni tipo, comprese le condotte di concorrenza sleale ex art. 2598 c.c.) in connessione teleologica con la turbativa.

Pertanto, l'uso di mezzi ingannevoli finalizzato esclusivamente ad assicurare all'agente un utile economico può concretizzare solo una concorrenza sleale e non la fattispecie di cui all'art. 513 c.p.

E' importante tener distinto il reato *de quo* dalla fattispecie civilistica della concorrenza sleale (art. 2598 c.c.).

Es. di condotte: atti idonei a generare una situazione di inganno che vizia la scelta del consumatore, sviando così la clientela di un'azienda; duplicazione e commercializzazione di programmi software; trasferimento fraudolento di cognizioni tecniche ad altra azienda; inserimento nel proprio sito internet, attraverso il quale viene pubblicizzato il proprio prodotto commerciale, di parole chiave direttamente riferibili alla persona, all'impresa e al prodotto di un concorrente, in modo da rendere maggiormente "visibile" sui motori di ricerca operanti in rete il proprio sito, sfruttando la notorietà commerciale e la diffusione del prodotto concorrente.

Soggetto attivo	Chiunque
Elemento oggettivo	Impedimento o turbamento dell'esercizio di un'industria o di un commercio, tramite violenza o uso di mezzi fraudolenti.
Elemento soggettivo	Dolo specifico

Aree aziendali esposte a rischio:

- Commerciale;
- Gestione rapporti con *competitors*;
- Produzione;
- Ricerca e Sviluppo;
- *Customer*;
- Direzione.

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 a rischio;
- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di 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 aziendali;
- Segregazione e separazione delle funzioni fra chi gestisce i rapporti con i clienti ed i *competitors* e chi delibera le strategie commerciali aziendali;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione dei rapporti commerciali con clienti, *competitors*, istituzioni.

Art. 513 bis c.p. Illecita concorrenza con minaccia o violenza.

Chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia è punito con la reclusione da due a sei anni.

La pena è aumentata se gli atti di concorrenza riguardano un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.

Osservazioni

La norma mira a sanzionare quelle forme tipiche di intimidazione che tendono a controllare le attività commerciali, industriali o produttive (anche agricole), o comunque a condizionarle, incidendo sulla fondamentale legge di mercato che vuole la concorrenza libera e lecita. Tuttavia, non occorre che il reato si realizzi in ambienti di criminalità organizzata o che l'autore appartenga a tali ambienti; inoltre, gli atti di concorrenza non vanno intesi in senso tecnico giuridico ex art. 2595 c.c.

Il bene giuridico tutelato è il libero svolgimento dell'iniziativa economica ex art. 41 Cost.

Nessun tipo di attività imprenditoriale sembra essere escluso dalla tutela che vuole assicurare la norma; pertanto sarà sufficiente una qualsiasi attività d'impresa ex art. 2082 c.c.

Invece, i soggetti attivi possono essere solo coloro che esercitano, anche di fatto, una qualsiasi attività, commerciale, industriale, produttiva.

La condotta può realizzarsi con atti di concorrenza o di violenza o minaccia. Per giurisprudenza l'espressione rinvierebbe alle condotte riconducibili ad un generale metodo di intimidazione mafiosa, pur non essendo necessaria l'appartenenza dei soggetti attivi ad un sodalizio mafioso in senso tecnico.

Un esempio di illecita concorrenza punibile ex art. 513 bis c.p. è l'accordo collusivo fra due o più imprese finalizzato alla predisposizione di offerte attraverso cui influenzare la scelta della ditta aggiudicatrice di un appalto.

Soggetto attivo	Chiunque.
Elemento oggettivo	Compimento di atti di concorrenza con violenza o minaccia.
Elemento soggettivo	Dolo specifico diretto a scoraggiare la concorrenza

Aree aziendali esposte a rischio:

- gestione rapporti con i *competitors*;
- predisposizione ed applicazione di clausole contrattuali per la regolamentazione dei comportamenti anticoncorrenziali, in conformità alla normativa vigente (codice civile, codice di proprietà industriale, normativa Antitrust ecc.);
- partecipazione a gare, appalti e procedure di evidenza pubblica.

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 a rischio, dei soggetti deputati a gestire rapporti con la P.A., delle figure responsabili della corretta individuazione ed applicazione della normativa cogente in materia di concorrenza;

- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di 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 aziendali;
- Segregazione e separazione delle funzioni fra chi gestisce i rapporti con i clienti ed i *competitors* e chi delibera le strategie commerciali aziendali;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione dei rapporti commerciali con clienti, *competitors*, istituzioni.

Art. 514 c.p. Frodi contro le industrie nazionali.

Chiunque, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, o marchi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a 516 euro. Se per i marchi o segni distintivi sono state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale, la pena è aumentata e non si applicano le disposizioni degli art. 473 e 474.

Osservazioni

La norma mira a tutelare genericamente l'industria nazionale, apparendo in tal modo chiaramente statalista ed anacronistica.

La condotta si esplica nella vendita o messa in circolazione di beni con marchi o segni distintivi contraffatti.

Il dolo è generico.

Soggetto attivo	Chiunque
Elemento oggettivo	Porre in vendita o mettere altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, o marchi o segni distintivi contraffatti o alterati,
Elemento soggettivo	Dolo specifico; volontà di cagionare un nocumento all'industria nazionale.

Art. 515 c.p. Frode nell'esercizio del commercio.

Chiunque, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità diversa da quella dichiarata o pattuita, è punito, qualora il fatto non costituisca un più grave delitto, con la reclusione fino a due anni o con la multa fino a 2.065 euro.

Se si tratta di oggetti preziosi, la pena è della reclusione fino a tre anni o della multa non inferiore a 103 euro.

Osservazioni

L'oggettività giuridica della fattispecie in questione è riconducibile alla c.d. buona fede commerciale, a tutela sia del pubblico dei consumatori, sia dell'insieme di produttori e commercianti.

Il reato de quo può essere commesso da chiunque agisca nell'esercizio di un'attività commerciale, non essendo essenziale la qualità di commerciante.

La responsabilità ricade sul titolare dell'attività e sull'impresa stessa anche nel caso in cui la consegna venga effettuata da un dipendente, socio, commesso, familiare ecc...; tuttavia, occorre accertare che, tenendo conto delle dimensioni dell'organizzazione, la consegna dell'*aliud pro alio* si sia verificata sulla base di direttive univoche del preponente e/o dell'impresa stessa, e non per iniziativa o negligenza del dipendente.

Per giurisprudenza diffusa, si ritiene che soggetto attivo del reato possa essere anche colui che, fuori da un esercizio commerciale o spaccio, ponga in essere un singolo ed occasionale scambio (es. agricoltore ed artigiano che vendono direttamente al consumatore).

La condotta materiale consiste nella consegna di una cosa mobile non conforme a quella convenuta per:

-essenza: occorre una diversità materiale (es. consegna di acqua invece di olio, di farina invece di zucchero; ma anche pratica di massaggi presso centri estetici senza l'uso di specifiche creme dotate di caratteristiche e marchi particolari e preventivamente pubblicizzati nell'offerta del servizio);

-origine: si fa riferimento in questo caso ad un mendacio relativo all'origine geografica del prodotto (es. consegna di un formaggio di provenienza diversa da quella indicata dal cliente con la richiesta di un prodotto dotato di una denominazione che richiama un emblematico luogo di fabbricazione);

-provenienza: marchio genuino apposto su un prodotto diverso da quello originario oppure marchio genuino che contrassegna un prodotto proveniente solo in parte dall'azienda indicata;

-qualità: falsa indicazione della composizione del prodotto e dei requisiti specifici della tipologia merceologica di appartenenza (es. consegna di televisore di un certo tipo non nuovo ma riparato, diversamente da quanto pattuito con l'acquirente; consegna di ciclomotore riparato e dotato di caratteristiche diverse da quella pattuite, poiché dotato di una diversa velocità e potenza o poiché necessitante di una particolare abilitazione per la guida; vendita di bevande edulcorate con saccarina; vendita di cibi congelati come freschi; consegna di merce con termine di scadenza superato, purché ciò alteri i requisiti di qualità essenziali richiesti dal cliente; vendita di scarto da decanter di pomodoro, proveniente dalla centrifugazione degli scarti dei pelati, come concentrato di pomodoro, consistente, invece, nel frutto della prima trasformazione del pomodoro fresco).

-quantità: diversità di peso e misura (es. vendita di prodotti confezionati meccanicamente e con contenuto netto risultante inferiore al peso dichiarato, per percentuali eccedenti le previste tolleranze).

In ogni caso, la condotta prescinde dalla causazione o meno di un danno economico alla vittima, essendo sufficiente la consegna di un bene diverso, per uno dei parametri sopra indicati.

Per giurisprudenza è, invece, “tentativo di frode in commercio” la condotta dell’esercente che esponga sui banchi o comunque offra al pubblico prodotti alimentari scaduti sulle cui confezioni sia stata alterata o sostituita l’originale indicazione del termine minimo di conservazione.

L’elemento psicologico del reato è il dolo generico; la giurisprudenza ritiene che la popolarità del prodotto, e la conseguente abitudine ad utilizzare il nome specifico di un prodotto come denominazione generica per tutta la categoria di prodotti ad esso simili, non comporta la volgarizzazione del marchio; infatti quest’ultima richiede la rinuncia anche tacita del titolare all’utilizzo del marchio.

Per quanto riguarda la configurabilità di tale reato in capo a realtà cooperative, la rischiosità è pressoché generale, in particolare, se alcuni processi o impianti produttivi sono gestiti in autonomia da soggetti apicali; questi ultimi, al fine di assicurare all’azienda una maggiore concorrenzialità e garantire al tempo stesso un utile superiore, potrebbero essere indotti a tenere condotte qualificabili come frode in commercio.

Va precisato tuttavia, che la locuzione “qualora il fatto non costituisca un più grave delitto” rende la norma inapplicabile in caso di truffa, dunque in caso di trasmissione all’acquirente di un bene diverso tramite artifici e raggiri con contestuale nocimento patrimoniale per la vittima.

Al contrario, il reato di frode in commercio può concorrere con quelli previsti e puniti dagli artt. 516 e 517 c.p.

Soggetto attivo	Chiunque
Elemento oggettivo	Consegna all’acquirente una cosa mobile per un’altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità diversa da quella dichiarata o pattuita.
Elemento soggettivo	Dolo generico

Aree aziendali esposte a rischio:

- Produzione (selezione materie prime, tecnologia della produzione, rapporti con terzisti, controllo qualità di prodotto, adozione disciplinari e regolamenti d’uso marchi e segni distintivi, ingresso e uscita merci, *packaging*, distribuzione ecc.);
- Distribuzione;
- Gestione singoli impianti o processi produttivi in autonomia;
- *Import/export*;
- Gestione contratti c/terzisti;
- Ricerca e sviluppo (investimenti per *know-how*, marchi e brevetti);
- *Marketing*;
- Gestione sistemi informativi *hardware* e *software*;

- Area Commerciale (approvvigionamenti, tecniche e politiche commerciali, controlli su terzi e magazzini esterni).

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 a rischio, dei soggetti deputati a gestire rapporti con la P.A., delle figure responsabili della corretta individuazione ed applicazione della normativa cogente, dei soggetti responsabili della liberalizzazione del prodotto e della qualità del prodotto finale;
- Costruzione di un sistema di tracciabilità del prodotto;
- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di 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 aziendali;
- Segregazione e separazione delle funzioni fra chi gestisce i rapporti con i clienti ed i *competitors* e chi delibera le strategie commerciali aziendali;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione dei rapporti commerciali con i clienti.

Art. 516 c.p. Vendita di sostanze alimentari non genuine come genuine.

Chiunque pone in vendita o mette altrimenti in commercio come genuine sostanze alimentari non genuine è punito con la reclusione fino a sei mesi o con la multa fino a 1.032 euro.

Osservazioni

La condotta punita è concretizzabile con qualsiasi operazione comunque diretta allo scambio ed allo smercio di cibi e bevande non genuini; pertanto, è sufficiente porre in essere atti chiaramente rivelatori della finalità di vendere o porre in commercio (esposizione al pubblico, indicazione in offerte al pubblico, presenza del prodotto non genuino nel magazzino o deposito del venditore ecc.).

Tuttavia, occorre precisare che il reato di cui all'art. 516 c.p. è finalizzato a tutelare il commercio e non la salute pubblica; pertanto, nel caso in cui quest'ultima venga posta in pericolo, saranno configurabili altre fattispecie di reato più gravi, come quella di cui all'art. 442 c.p., commercio di sostanze alimentari adulterate o contraffatte (non richiamata ad oggi dal D.Lgs 231/2001).

Per sostanze alimentari si intendono non solo le sostanze alimentari provenienti dalla terra, ma anche quelle ottenute da processi di manipolazione, lavorazione e trasformazione industriale.

Per giurisprudenza prevalente la genuinità è sia quella naturale (alterazione della sostanza alimentare), sia quella formale (determinazione legislativa di caratteristiche e requisiti essenziali per qualificare un determinato tipo di prodotto alimentare); pertanto, sono considerati non genuini sia i prodotti che hanno subito un'artificiosa alterazione nella loro essenza e nella composizione mediante commistione di sostanze estranee e sottrazione dei principi nutritivi caratteristici, sia i prodotti che contengano sostanze diverse da quelle che la legge prescrive per la loro composizione:

es. Vendita di pane qualificato all'olio ma contenente strutto; vendita di acque gassate non conformi alla normativa vigente in tema di igiene e sanità di alimenti e bevande; vendita di latte vaccino con residuo magro inferiore a quello fissato ex lege; vendita di carne trattata con anidride solforosa.

Soggetto attivo	Chiunque
Elemento oggettivo	Vendita o messa in commercio di alimentari non genuine come genuine.
Elemento soggettivo	Dolo generico

Aree aziendali esposte a rischio:

- Produzione (selezione materie prime, tecnologia della produzione, rapporti con terzisti, controllo qualità di prodotto, adozione disciplinari e regolamenti d'uso marchi e segni distintivi, ingresso e uscita merci, *packaging*, distribuzione ecc.);
- Distribuzione;
- Gestione singoli impianti o processi produttivi in autonomia;
- *Import/export*;
- Gestione contratti c/terzisti;
- Ricerca e sviluppo (investimenti per *know-how*, marchi e brevetti);
- *Marketing*;
- Gestione sistemi informativi *hardware* e *software*;
- Area Commerciale (approvvigionamenti, tecniche e politiche commerciali, controlli su terzisti e magazzini esterni).

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 a rischio;

- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di incontri periodici e/o *audit* fra O.d.V. e funzioni aziendali esposte al rischio *de quo* (Responsabile di produzione, Responsabile Assicurazione qualità ecc.); comunicazione immediata all'O.d.V. di eventuali anomalie che ineriscano la genuinità del prodotto commercializzato dall'azienda;
- Documentazione, archiviazione e tracciabilità degli atti e delle operazioni aziendali;
- Segregazione e separazione delle funzioni fra chi coordina l'attività produttiva e chi autorizza la liberalizzazione del prodotto (ad es. a seguito di adeguato periodo di quarantena);
- Corretta adozione ed applicazione di adeguate procedure in materia di produzione di prodotti alimentari e corretta registrazione ed archiviazione dei controlli effettuati; diffusione di tali procedure anche ad eventuali terzisti;
- Adozione ed applicazione di specifiche procedure a garanzia della rintracciabilità dei prodotti, nonché del corretto richiamo degli stessi al verificarsi di eventuali problematiche;
- Corretta applicazione Piano HACCP nella aziende alimentari che gestiscano processi di preparazione, trasformazione, fabbricazione, confezionamento, deposito, trasporto, distribuzione, manipolazione, vendita o fornitura, compresa la somministrazione di prodotti alimentari;
- Adozione di buone prassi, certificate e non, ad esempio con riferimento alle norme tecniche UNI EN ISO 22000:2005;
- Adozione eventuale di Sistemi di Gestione Certificati necessari per l'accesso alla Grande distribuzione Organizzata ad esempio BRC, IFS, GOST ecc.

Art. 517 c.p. Vendita di prodotti industriali con segni mendaci

Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a due anni o con la multa fino a ventimila euro.

Osservazioni

Il reato in questione ha ad oggetto l'interesse pubblico concernente l'ordine economico in relazione alla lealtà e alla moralità del commercio e tende ad assicurare l'onestà degli scambi commerciali contro il pericolo di frodi nella circolazione dei prodotti.

La condotta di reato si realizza tramite la generica messa in circolazione di beni con nomi, marchi o segni distintivi che, pur non imitando marchi o segni registrati, sono idonei ad ingannare i consumatori.

I prodotti/beni riportanti tali segni/marchi devono essere posti in vendita o altrimenti messi in circolazione; la prima locuzione fa riferimento alla materiale esposizione del prodotto per la vendita; la messa in circolazione, invece, comprende qualunque atto di

commercio (es. alienazione, spedizione, uscita del prodotto dal magazzino per essere destinato alla vendita).

In riferimento al contenuto del mendacio si fa rinvio alle osservazioni riportate in commento all'art. 515 c.p.

Soggetto attivo	Chiunque
Elemento oggettivo	Vendita o messa in circolazione di opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.
Elemento soggettivo	Dolo generico

Aree aziendali esposte a rischio:

- Produzione (selezione materie prime, tecnologia della produzione, rapporti con terzisti, controllo qualità di prodotto, adozione disciplinari e regolamenti d'uso marchi e segni distintivi, ingresso e uscita merci, *packaging*, distribuzione ecc.);
- Distribuzione;
- Gestione singoli impianti o processi produttivi in autonomia;
- *Import/export*;
- Gestione contratti c/terzisti;
- Ricerca e sviluppo (investimenti per *know-how*, marchi e brevetti);
- *Marketing*;
- Gestione sistemi informativi *hardware* e *software*;
- Area Commerciale (approvvigionamenti, tecniche e politiche commerciali, controlli su terzisti e magazzini esterni).

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 a rischio;
- Individuazione di specifiche figure dotate di adeguata competenza e professionalità con la funzione di individuare aggiornare e diffondere la normativa cogente in materia di tutela di nomi, marchi o segni distintivi nazionali o esteri di opere dell'ingegno o di prodotti industriali;
- Segregazione e separazione delle funzioni fra chi gestisce attività commerciale e di ricerca e sviluppo e chi si occupa della verifica della conformità legale del prodotto finale;

- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di incontri periodici e/o *audit* fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione e tracciabilità delle operazioni inerenti marchi o altri segni distintivi, dei documenti accertanti la loro proprietà o il diritto d'uso legittimo;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione di nomi, marchi o segni distintivi nazionali o esteri.

Art. 517ter c.p. Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale.

Salva l'applicazione degli articoli 473 e 474 chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a euro 20.000.

Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al primo comma.

Si applicano le disposizioni di cui agli articoli 474-bis, 474-ter, secondo comma, e 517-bis, secondo comma.

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

Osservazioni

La condotta di reato consiste nel fabbricare o utilizzare beni realizzati tramite usurpazione di un altrui titolo di proprietà industriale, purchè l'agente sia a conoscenza dell'esistenza e del contenuto di tale titolo.

E' altresì punita la condotta di introduzione nello Stato, detenzione per la vendita, messa in vendita, o messa in circolazione di tali beni.

Condizione di punibilità è che siano state osservate le norme interne, comunitarie ed internazionali sulla tutela della proprietà industriale o intellettuale.

Soggetto attivo	Chiunque
Elemento oggettivo	Fabbricazione, utilizzazione, introduzione nello Stato, detenzione per la vendita, messa in vendita, messa in circolazione di beni realizzati tramite l'usurpazione di un titolo di proprietà industriale
Elemento soggettivo	Dolo generico

Aree aziendali esposte a rischio:

- Produzione (selezione materie prime, tecnologia della produzione, rapporti con terzisti, controllo qualità di prodotto, adozione disciplinari e regolamenti d'uso marchi e segni distintivi, ingresso e uscita merci, *packaging*, distribuzione ecc.);
- Distribuzione;
- Gestione singoli impianti o processi produttivi in autonomia;
- *Import/export*;
- Gestione contratti c/terzisti;
- Ricerca e sviluppo (investimenti per *know-how*, marchi e brevetti);
- *Marketing*;
- Gestione sistemi informativi *hardware* e *software*;
- Gestione rapporti commerciali (approvvigionamenti, tecniche e politiche commerciali, controlli su terzisti e magazzini esterni), specialmente con controparti localizzate in zone geografiche a rischio.

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 a rischio;
- Individuazione di specifiche figure dotate di adeguata competenza, professionalità ed eventuali deleghe con la funzione di individuare aggiornare e diffondere la normativa cogente in materia di tutela di nomi, marchi o segni distintivi nazionali o esteri di opere dell'ingegno o di prodotti industriali;
- Segregazione e separazione delle funzioni fra chi gestisce attività commerciale e di ricerca e sviluppo e chi si occupa della verifica della conformità legale del prodotto finale;
- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di incontri periodici e/o *audit* fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Documentazione, archiviazione e tracciabilità delle operazioni inerenti marchi o altri segni distintivi, dei documenti accertanti la loro proprietà o il diritto d'uso legittimo;
- Diffusione di prassi e procedure, anche integrate nel Modello 231, finalizzate alla corretta gestione di nomi, marchi o segni distintivi nazionali o esteri.

Art. 517^{quater} c.p. Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari.

Chiunque contraffà o comunque altera indicazioni geografiche o denominazioni di origine di prodotti agroalimentari è punito con la reclusione fino a due anni e con la multa fino a euro 20.000.

Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte.

Si applicano le disposizioni di cui agli articoli 474-bis, 474-ter, secondo comma, e 517-bis, secondo comma.

I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali in materia di tutela delle indicazioni geografiche e delle denominazioni di origine dei prodotti agroalimentari.

Osservazioni

L'art. 517 quater c.p. per la prima volta introduce una tutela penale dei prodotti relativi ad indicazioni geografiche o denominazioni di origine, che costituiscono il c.d. *made in Italy* agroalimentare (DOP, IGP, DOC, DOCG, IGT ecc.).

Il bene tutelato appare molteplice, in quanto si riferisce sia alla buona fede dei consumatori, sia al diritto di proprietà dei soggetti depositari della denominazione contraffatta, sia alla generica produzione nazionale.

Le condotte punite sono la contraffazione, l'alterazione, l'introduzione nello Stato, detenzione per la vendita, la messa in vendita, messa in circolazione di indicazioni o denominazioni contraffatte.

Soggetto attivo	Chiunque
Elemento oggettivo	Contraffazione o alterazione di indicazioni geografiche o di denominazioni di origine di prodotti agroalimentari; Commercializzazione in senso lato dei suddetti prodotti contraffatti o alterati.
Elemento soggettivo	Dolo generico

Aree aziendali esposte a rischio:

- Produzione (selezione materie prime, tecnologia della produzione, rapporti con terzi, controllo qualità di prodotto, adozione disciplinari e regolamenti d'uso marchi e segni distintivi, ingresso e uscita merci, packaging, distribuzione ecc.);
- Distribuzione;
- Gestione singoli impianti o processi produttivi in autonomia;
- *Import/export*;
- Gestione contratti c/terzisti;
- Ricerca e sviluppo (investimenti per *know-how*, marchi e brevetti);

- *Marketing*;
- Area Commerciale (approvvigionamenti, tecniche e politiche commerciali, controlli su terzisti e magazzini esterni).

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 a rischio;
- Identificazione di una figura responsabile della corretta gestione di marchi, indicazioni geografiche, denominazioni di origine, e dei relativi regolamenti di utilizzo;
- Previsione di un canale comunicativo specifico con l'O.d.V. e previsione di incontri periodici *e/o audit* fra O.d.V. e funzioni aziendali esposte al rischio *de quo* (Responsabile di produzione, Responsabile Assicurazione qualità ecc.); comunicazione immediata all'O.d.V. di eventuali anomalie che ineriscano la genuinità del prodotto commercializzato dall'azienda;
- Documentazione, archiviazione e tracciabilità degli atti e delle operazioni aziendali;
- Segregazione e separazione delle funzioni fra chi coordina l'attività produttiva e chi autorizza la liberalizzazione del prodotto (ad es. a seguito di adeguato periodo di quarantena);
- Corretta adozione ed applicazione di adeguate procedure in materia di produzione di prodotti alimentari e corretta registrazione ed archiviazione dei controlli effettuati; diffusione di tali procedure anche ad eventuali terzisti;
- Adozione ed applicazione di specifiche procedure a garanzia della rintracciabilità dei prodotti, nonché del corretto richiamo degli stessi al verificarsi di eventuali problematiche;
- Corretta applicazione Piano HACCP nella aziende alimentari che gestiscano processi di preparazione, trasformazione, fabbricazione, confezionamento, deposito, trasporto, distribuzione, manipolazione, vendita o fornitura, compresa la somministrazione di prodotti alimentari;
- Adozione di buone prassi certificate e non, ad esempio con riferimento alle norme tecniche UNI EN ISO 22000:2005;
- Adozione eventuale di Sistemi di Gestione Certificati necessari per l'accesso alla Grande distribuzione Organizzata ad esempio BRC, IFS, GOST ecc.

ART. 25 TER D.LGS 231/2001 - REATI SOCIETARI.

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, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica, si applicano le seguenti sanzioni pecuniarie:

a) per la contravvenzione di false comunicazioni sociali, prevista dall'articolo 2621 del codice civile, la sanzione pecuniaria da duecento a trecento quote;

b) per il delitto di false comunicazioni sociali in danno dei soci o dei creditori, previsto dall'articolo 2622, primo comma, del codice civile, la sanzione pecuniaria da trecento a seicentosessanta quote;

c) per il delitto di false comunicazioni sociali in danno dei soci o dei creditori, previsto dall'articolo 2622, terzo comma, del codice civile, la sanzione pecuniaria da quattrocento a ottocento quote;

d) per la contravvenzione di falso in prospetto, prevista dall'articolo 2623, primo comma, del codice civile, la sanzione pecuniaria da duecento a duecentosessanta quote;

e) per il delitto di falso in prospetto, previsto dall'articolo 2623, secondo comma, del codice civile, la sanzione pecuniaria da quattrocento a seicentosessanta quote;

f) per la contravvenzione di falsità nelle relazioni o nelle comunicazioni delle società di revisione, prevista dall'articolo 2624, primo comma, del codice civile, la sanzione pecuniaria da duecento a duecentosessanta quote;

g) per il delitto di falsità nelle relazioni o nelle comunicazioni delle società di revisione, previsto dall'articolo 2624, secondo comma, del codice civile, la sanzione pecuniaria da quattrocento a ottocento quote;

h) per il delitto di impedito controllo, previsto dall'articolo 2625, secondo comma, del codice civile, la sanzione pecuniaria da duecento a trecentosessanta quote;

i) per il delitto di formazione fittizia del capitale, previsto dall'articolo 2632 del codice civile, la sanzione pecuniaria da duecento a trecentosessanta quote;

l) per il delitto di indebita restituzione dei conferimenti, previsto dall'articolo 2626 del codice civile, la sanzione pecuniaria da duecento a trecentosessanta quote;

m) per la contravvenzione di illegale ripartizione degli utili e delle riserve, prevista dall'articolo 2627 del codice civile, la sanzione pecuniaria da duecento a duecentosessanta quote;

n) per il delitto di illecite operazioni sulle azioni o quote sociali o della società controllante, previsto dall'articolo 2628 del codice civile, la sanzione pecuniaria da duecento a trecentosessanta quote;

o) per il delitto di operazioni in pregiudizio dei creditori, previsto dall'articolo 2629 del codice civile, la sanzione pecuniaria da trecento a seicentosessanta quote;

p) per il delitto di indebita ripartizione dei beni sociali da parte dei liquidatori, previsto dall'articolo 2633 del codice civile, la sanzione pecuniaria da trecento a seicentosessanta quote;

q) per il delitto di illecita influenza sull'assemblea, previsto dall'articolo 2636 del codice civile, la sanzione pecuniaria da trecento a seicentosessanta quote;

r) per il delitto di aggio, previsto dall'articolo 2637 del codice civile e per il delitto di omessa comunicazione del conflitto d'interessi previsto dall'articolo 2629-bis del codice civile, la sanzione pecuniaria da quattrocento a mille quote;

s) per i delitti di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, previsti dall'articolo 2638, primo e secondo comma, del codice civile, la sanzione pecuniaria da quattrocento a ottocento quote;

Se, in seguito alla commissione dei reati di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Art. 2621 cod.civ. False comunicazioni sociali.

Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

Art.2622 cod.civ. False comunicazioni sociali in danno della società, dei soci o dei creditori.

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato, a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici o delle Comunità europee.

Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio.

La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori.

Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT ovvero se sia consistito nella distruzione o riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo.

La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore

generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

Osservazioni

Tra le due fattispecie criminose sussiste un rapporto non di alternatività, ma di sussidiarietà, in virtù del quale l'articolo 2621 è applicabile anche nelle ipotesi in cui, pur in presenza di un danno patrimoniale, non sia possibile procedere per il delitto di cui all'art.2622 cod. civ.

Le due norme contemplano, rispettivamente, la contravvenzione di falso in bilancio² semplice (reato di pericolo), ed il delitto di falso in bilancio cui consegua un danno patrimoniale in capo alla società, ai soci o ai creditori (reato di evento).

In entrambe le fattispecie, la punibilità (con sanzione penale) resta esclusa in caso di mancato superamento delle "soglie di divergenza" stabilite dai commi 3 e 4 dell'art.2621 e dai commi 7 e 8 dell'art. 2622. In tali casi sono previste, comunque, sanzioni amministrative pecuniarie nonché la pena accessoria dell'interdizione dalle cariche societarie.

Rilevante è l'introduzione (ad opera della legge n.262/2005, cd. legge sul risparmio) della figura del dirigente preposto alla redazione dei documenti contabili societari e la sua inclusione tra gli eventuali soggetti attivi del reato di falso in bilancio. Pur essendo la nomina e la previsione statutaria di tale soggetto obbligatoria solo per le società quotate, si segnala che la sua "istituzionalizzazione" è contenuta anche in norme del codice civile riferibili a tutte le società per azioni, ed alle cooperative che di quelle mutuino la disciplina (v. art. 2434 cod. civ. sulla responsabilità civile delle cariche sociali in materia di bilanci). Ciò potrebbe comportare, ancorché il punto sia dubbio in dottrina, l'applicazione della responsabilità penale ex artt.2621 e 2622 anche al dirigente contabile di società non quotate.

Entrambi i reati in epigrafe sono reati propri, la cui commissione è ascrivibile non a chiunque ma esclusivamente a determinati soggetti qualificati, in particolare ai soggetti c.d. apicali espressamente indicati.

Si rappresentano nelle seguenti tabelle gli elementi costitutivi delle fattispecie penali in esame:

Art.2621 False comunicazioni sociali (contravvenzione)

Soggetti attivi	Reato proprio. Amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori
Condotta	Esposizione di fatti falsi o omissione di informazioni obbligatorie(nei bilanci, nelle relazioni o nelle altre comunicazioni sociali obbligatorie dirette ai soci o al pubblico) sulla situazione economica, patrimoniale o finanziaria della società o del gruppo cui essa appartiene, in modo idoneo ad indurre in errore i destinatari
Evento	Il reato si consuma con la condotta, senza necessità di eventi

² Ed altre comunicazioni sociali equiparate.

	pregiudizievoli ulteriori.
Pena	Arresto fino a due anni
Sanzioni amministrative e pene accessorie per i casi di illecito sottosoglia	<p>Sanzione pecuniaria da dieci a cento quote.</p> <p>Interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, direttore generale, liquidatore, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.</p>

Art.2622 False comunicazioni sociali in danno della società, dei soci o dei creditori (delitto)

Soggetti attivi	<p>Reato proprio.</p> <p>Amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori</p>
Condotta	Esposizione di fatti falsi o omissione di informazioni obbligatorie (nei bilanci, nelle relazioni o nelle altre comunicazioni sociali obbligatorie dirette ai soci o al pubblico) sulla situazione economica, patrimoniale o finanziaria della società o del gruppo cui essa appartiene, in modo idoneo ad indurre in errore i destinatari
Evento	Danno patrimoniale alla società, ai soci o ai creditori
Pena	<p>3. Reclusione da sei mesi a tre anni (società non quotate)</p> <p>4. Reclusione da uno a quattro anni (società quotate)</p> <p>5. Reclusione da due a sei anni (società quotate e grave danno ai risparmiatori)</p>
Procedibilità	<p>6. A querela della persona offesa (società non quotate)</p> <p>7. D'ufficio (società quotate)</p>
Sanzioni amministrative e pene accessorie per i casi di illecito sottosoglia	<p>Sanzione pecuniaria da dieci a cento quote.</p> <p>Interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, direttore generale, liquidatore, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.</p>

Oltre ai soggetti qualificati individuati dal legislatore (amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori), vanno considerati come soggetti potenzialmente idonei a porre in essere condotte penalmente rilevanti in relazione alle fattispecie di cui sopra, anche eventuali soggetti subordinati al responsabile di funzione, ma dotati di un sufficiente potere discrezionale. Si pensi all'ipotesi in cui il collaboratore amministrativo deputato alla gestione contabile, in accordo anche tacito con il responsabile, inserisca nei documenti aziendali valutazioni fittizie di crediti; nel momento in cui il soggetto apicale recepisce tale falsità

inserendolo nelle comunicazioni sociali ufficiali, possono dirsi integrati tutti gli estremi della fattispecie.

Pertanto, pur ribadendo la natura propria di tali reati, **i processi/attività** in grado di esporre le cooperative ad una discreta rischiosità risultano le seguenti:

- Processi/attività aziendali di gestione di dati che contribuiscono alla formazione del bilancio (fatturazione -ciclo attivo-passivo, acquisti, budget, gestione di cassa ecc.);
- Redazione bilancio e situazioni contabili infrannuali, redazione relazione sulla gestione, redazione bilancio consolidato e altre comunicazioni sociali;
- Attività di controllo interno, compresa registrazione contabile e/o di gestione contabile in generale.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e Collegio Sindacale prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2623 cod.civ. Falso in prospetto.

L'articolo in epigrafe è stato abrogato dalla legge sul risparmio (l. n.262/2005) e sostituito, ma con esclusivo riferimento alle società quotate, dall'art.173**bis** del T.u.f.:

Chiunque, allo scopo di conseguire per sé o per altri un ingiusto profitto, nei prospetti richiesti per la offerta al pubblico di prodotti finanziari o l'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con l'intenzione di ingannare i destinatari del prospetto, espone false informazioni od occulta dati o notizie in modo idoneo a indurre in errore i suddetti destinatari, è punito con la reclusione da uno a cinque anni.

E' rimasto tuttavia invariato il riferimento all'art.2623 contenuto nel D.Lgs. n.231/2001 (art.25**ter**, comma 1, lett.d ed e)): l'abrogazione della norma del codice ed il mancato richiamo al nuovo art.173**bis** del T.u.f. inducono a ritenere il falso in prospetto quale reato non rilevante ai fini della responsabilità amministrativa degli enti e persone giuridiche, quanto meno con riferimento alle società non quotate. Sussiste qualche dubbio, invece, con riferimento agli emittenti quotati.

Art. 2624 cod.civ. Falsità nelle relazioni o nelle comunicazioni delle società di revisione.

Osservazioni

L'articolo in epigrafe è stato abrogato dall'art. 37 del D.Lgs. 27 gennaio 2010, n. 39 ed ivi riprodotto, senza sostanziali modifiche, all'art. 27.

Al pari dell'articolo 2623 cod.civ., è rimasto tuttavia anche qui invariato il riferimento testuale contenuto nel D.Lgs. n. 231/2001 (art.25**ter**, comma 1, lett. f e g)).

L'abrogazione della norma del codice ed il mancato richiamo al nuovo art. 27 del D.Lgs. n. 39/2010 inducono a ritenere il reato in esame non più rilevante ai fini della responsabilità amministrativa degli enti e persone giuridiche; ciò, quantomeno, alla stregua del canone ermeneutico d'interpretazione giuridica letterale.

Non possono tuttavia nascondersi le perplessità derivanti da tale risultato, probabilmente dovuto, semplicemente, a mancato coordinamento legislativo: stante la possibile futura correzione, si ritiene opportuno fornire comunque un commento del reato *de quo* corredato dall'indicazione dei protocolli specifici.

D.Lgs. n. 39/2010, articolo 27, commi 1 e 2. Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale.

I responsabili della revisione legale i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno.

Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari delle comunicazioni, la pena è della reclusione da uno a quattro anni.

La norma, come per il passato, individua due fattispecie criminose, a formazione progressiva: la prima, di natura contravvenzionale, costituisce un reato di pericolo che si perfeziona col semplice porsi in essere della condotta descritta, senza necessità di ulteriori eventi pregiudizievoli; la seconda, di natura delittuosa, costituisce invece un reato d'evento, caratterizzato dall'esistenza di un danno patrimoniale conseguente alla condotta illecita.

Trattasi anche qui di reato proprio, esclusivamente ascrivibile ai "responsabili della revisione legale", vale a dire ai soggetti – dipendenti o collaboratori – in concreto incaricati del controllo contabile e conseguente certificazione dei bilanci societari.

Gli amministratori della società cooperativa, tuttavia, potranno essere chiamati a rispondere a titolo di concorso, tanto commissivo quanto omissivo.

A differenza del reato di false comunicazioni sociali, la punibilità delle condotte descritte nella norma in commento non è condizionata al superamento di alcuna soglia di divergenza tra la situazione reale e quella rappresentata.

L'elemento soggettivo del reato è plurimo, essendo richiesto sia il dolo specifico volto al conseguimento di un ingiusto profitto (per sé o per altri) sia il dolo generico rappresentato dall'intento ingannatorio.

Pene: arresto fino a un anno in caso di reato di pericolo; reclusione da uno a quattro anni in caso del verificarsi dell'evento (danno patrimoniale in capo ai destinatari delle comunicazioni).

Soggetti attivi	Reato proprio. Soggetti attivi sono i "responsabili della revisione legale", per tali dovendosi intendere i revisori legali o i responsabili delle società di revisione incaricati del controllo contabile sui bilanci societari.
Condotta	Reato di pericolo nell'ipotesi prevista dal primo comma; reato di danno nell'ipotesi di cui al comma secondo. Attestazione di fatti falsi ovvero occultamento di informazioni concernenti la situazione economica, patrimoniale o finanziaria della società o ente sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni.
Evento	L'evento, nell'ipotesi aggravata, è rappresentato dal danno patrimoniale eventualmente derivato ai destinatari delle comunicazioni effettuate dai revisori (o società di revisione).
Elemento soggettivo	Dolo specifico (consapevolezza delle falsità attestate, od omissioni + intento ingannatorio + perseguimento di un ingiusto profitto per sé o per altri).
Pena (procedibilità d'ufficio)	Arresto fino a un anno nella fattispecie di pericolo. Reclusione da uno a quattro anni nella fattispecie di danno.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art. 2625 cod.civ. Impedito controllo.

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

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

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Osservazioni

Trattasi anche qui di due fattispecie a formazione progressiva, la prima di mero pericolo e avente natura di illecito amministrativo (comma 1), la seconda, invece, avente natura di reato d'evento, vale a dire rappresentata dalla concreta produzione di un danno concreto derivante dalla condotta.

Ai sensi dell'art.25^{ter}, comma 1, lett.h del d.lgs. n.231/2001, ai fini della responsabilità amministrativa dell'ente o persona giuridica, rileva esclusivamente la seconda fattispecie, restando pertanto non rilevanti condotte d'impedito controllo non seguite da evento di danno.

Soggetti attivi del reato sono gli amministratori. La condotta è costituita da qualsiasi comportamento, commissivo come omissivo, volto ad impedire od ostacolare il controllo spettante per legge ai soci o agli altri organi sociali, *in primis* al collegio sindacale. Rilevano, pertanto, anche le condotte volte semplicemente ad ostacolare, ossia ad intralciare o rallentare, l'attività di controllo, indipendentemente dal fatto che tali comportamenti abbiano o meno l'effetto finale di impedire concretamente lo svolgimento di dette attività.

L'espressione impiegata nella norma ("*controllo...legalmente attribuito... ad altri organi sociali*") induce ad includere tra i soggetti titolari del potere di controllo, altresì, l'organismo di vigilanza ex d.lgs. n.231/2001.

Resta esclusa, nell'ambito delle ipotesi di controllo esterno contemplate dalla norma, la revisione cooperativa, per la quale invece rileva l'articolo 2638 (ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza)

Pena: reclusione fino a un anno. Procedibilità: a querela della persona offesa (socio).

Soggetti attivi	Reato proprio. Gli amministratori.
Condotta	Occultamento di documenti od impiego di altri artifici (es: distruzione di documenti, diniego espresso di fornire informazioni sull'attività di gestione, ritardi nell'adempiere alle richieste dei titolari del potere di controllo).
Evento	Impedimento o ostacolo allo svolgimento delle attività di controllo o di revisione attribuite dalla legge ai soci, ad altri organi sociali o alle società di revisione. Danno ai soci. I poteri di controllo devono essere attribuiti direttamente dalla legge: restano escluse dall'ambito di applicazione della norma le fattispecie concernenti attività di controllo attribuite statutariamente o in forza di patti parasociali.

Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).
Pena (procedibilità a querela)	Reclusione fino ad un anno.

Aree aziendali esposte a rischio:

- Convocazione e gestione riunioni e deliberazioni Cda;
- Gestione comunicazioni CDA-Collegio sindacale;
- Gestione funzione amministrativa;
- Redazione bilancio consuntivo.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;

- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art. 2632 cod.civ. Formazione fittizia del capitale.

Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in matura o di crediti ovvero del patrimonio della società in caso di trasformazione, sono puniti con la reclusione fino a un anno.

Osservazioni

La norma intende tutelare l'affidamento dei terzi in ordine alla reale consistenza del capitale sociale, sanzionando condotte tra loro eterogenee ma tutte caratterizzate dalla medesima finalità: la rappresentazione di un capitale apparente cui non corrispondono risorse patrimoniali effettive.

Le modalità di commissione del reato (che è a condotta vincolata) possono essere tre:

- attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale.

Ai sensi dell'art.2346, commi 4 e 5, salvo diversa previsione statutaria, a ciascun socio è assegnato un numero di azioni proporzionale alla parte del capitale sociale sottoscritta e per un valore non superiore a quello del suo conferimento, mentre in nessun caso il valore dei conferimenti può essere complessivamente inferiore all'ammontare del capitale sociale (prescrizioni analoghe sono previste, per le s.r.l., dagli artt. 2464, c.1 e 2468, c.2).

La riforma del 2003 ha eliminato il precedente principio per cui le azioni non potevano essere emesse per una somma inferiore al loro valore nominale, consentendo oggi che gli statuti possano prevedere l'emissione di *alcuni* titoli di valore nominale non corrispondente ai rispettivi conferimenti (emissioni sopra o sotto la pari), purchè l'ammontare *complessivo* delle azioni (o quote) corrisponda al capitale sociale effettivo, ossia ai conferimenti realmente effettuati.

Una volta rispettata la corrispondenza complessiva tra titoli emessi e capitale sociale, l'attribuzione ai singoli soci potrà anche avvenire in misura non proporzionale ai conferimenti (se tale possibilità è prevista in statuto).

- sottoscrizione reciproca di azioni o quote.

Ai sensi dell'art.2360, è vietato alle società di costituire o di aumentare il capitale mediante sottoscrizione reciproca di azioni, anche per tramite di società fiduciaria o per interposta persona.

La norma è espressione di un principio generale volto ad impedire che uno stesso patrimonio possa essere fittiziamente impiegato due volte per la costituzione o per l'aumento di capitale di più società, le quali apparirebbero così possedere due distinti capitali sociali in realtà corrispondenti ad un'unica somma. E' il caso della società A che partecipa alla costituzione della società B la quale poi sottoscrive un aumento di capitale di pari importo deliberato da A: formalmente sia A che B hanno ciascuna il proprio capitale sociale, in realtà trattasi sempre della stessa ricchezza.

La partecipazione incrociata deve essere frutto di uno specifico accordo e disegno volto alla formazione di capitali fittizi, nel mentre non è necessaria la contestualità delle condotte, potendo le stesse realizzarsi anche ad apprezzabile distanza di tempo.

- sopravvalutazione rilevante dei conferimenti dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

Ai sensi dell'art.2343, i conferimenti di beni in natura e di crediti devono essere assistiti dalla relazione giurata di un esperto designato dal tribunale, contenente la descrizione dei beni o dei crediti conferiti e la stima del loro valore (per le s.r.l. l'art.2465 prescrive la relazione giurata di un esperto o di una società di revisione iscritti nel registro dei revisori contabili).

Gli amministratori devono, poi, entro 180 giorni dalla iscrizione della società, controllare le valutazioni contenute nella relazione. Se risulta che il valore dei beni o dei crediti conferiti era inferiore di oltre un quinto a quello per cui avvenne il conferimento, la società deve proporzionalmente ridurre il capitale sociale, annullando le azioni scoperte. Tuttavia, il socio conferente può versare la differenza in denaro o recedere dalla società con diritto alla restituzione del conferimento, qualora sia possibile in tutto o in parte in natura.

Si ricordano qui le novità introdotte per le società azionarie (e conseguentemente per le cooperative per azioni) dal d.lgs. n.142/2008, il quale ha fatto venir meno la necessità della relazione di stima dell'esperto di nomina giudiziaria in alcune tassative ipotesi: è evidente che la diligenza richiesta in tali casi agli amministratori, al fine di non incorrere in responsabilità, sarà maggiore, non potendo essi invocare la valutazione del perito giudiziario.

Quanto alla "rilevanza" della sopravvalutazione, necessaria ai fini della responsabilità penale, si segnala un contrasto d'opinioni tra gli studiosi: ad avviso di alcuni la rilevanza andrebbe valutata utilizzando il criterio civilistico del quinto; per altri, viceversa, essendo la norma penale autonoma rispetto a quella civile, pur se a questa collegata, si imporrebbe una valutazione parimenti autonoma sostanzialmente fondata sul caso per caso.

Soggetti attivi	Reato proprio, di danno. Gli amministratori ed i soci (questi ultimi nella sola ipotesi di formazione o aumento fittizio del capitale mediante sopravvalutazione rilevante dei conferimenti in natura o di crediti).
Condotta	<ul style="list-style-type: none"> ➤ attribuzione di azioni/quote di valore <i>complessivamente</i> superiore all'entità del capitale sociale; ➤ sottoscrizione reciproca di azioni/quote ➤ sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti; ➤ sopravvalutazione rilevante del patrimonio della società in caso di trasformazione.
Evento	Formazione, aumento e rappresentazione di un capitale sociale fittizio.

Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).
Pena (procedibilità d'ufficio)	Reclusione fino a un anno.

Aree aziendali esposte a rischio:

- operazioni su capitale sociale;
- attività del Consiglio di Amministrazione e dei suoi componenti,
- Comunicazioni e gestione rapporti fra CdA, Collegio Sindacale; Assemblea dei soci.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di una procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art. 2626 cod. civ. Indebita restituzione dei conferimenti.

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

Osservazioni

Trattasi, al pari della precedente, di disposizione penale posta a tutela dell'integrità del capitale sociale, e quindi a protezione dell'affidamento dei creditori e dei terzi.

Assumono rilevanza tutte le condotte di restituzione dei conferimenti o di liberazione dall'obbligo di eseguirli, attuate al di fuori dei casi di *legittima riduzione* del capitale sociale.

Tali casi sono:

- la riduzione facoltativa cd. per esuberanza (art.2445);
- la riduzione per perdite, obbligatoria o meno a seconda dell'entità delle stesse (artt.2446 e 2447).

E' da rilevare che per le società cooperative, stante il regime di variabilità del capitale sociale (connesso al principio della porta aperta in entrata e in uscita), non può parlarsi, tecnicamente, di "aumento" o "riduzione" del capitale, nel senso valevole per le società azionarie.

Non integreranno pertanto la condotta sanzionata dalla norma in esame i casi di liquidazione della partecipazione derivanti dal recesso dei soci, casi ai quali resta inapplicabile la disciplina stabilita dall'art.2437^{quater}, alla cui stregua in caso di mancato collocamento delle azioni del socio recedente ed in caso d'impossibilità d'acquisto da parte della società si dà luogo a riduzione obbligatoria del capitale sociale.

Quanto al rimborso di quote o azioni, vale la disciplina particolare sancita dall'art.2529 ai sensi della quale l'atto costitutivo può autorizzare gli amministratori a rimborsare quote o azioni della società, purchè il rapporto tra patrimonio e indebitamento sia superiore a un quarto ed il rimborso avvenga nei limiti degli utili distribuibili o delle riserve disponibili risultanti dall'ultimo bilancio regolarmente approvato.

Le modalità di commissione del reato potranno essere sia dirette (dazione di somme o rinuncia al credito), sia indirette (compensazione con credito vantato dal socio); sia palesi che simulate, come, ad esempio, nel caso di pagamenti per prestazioni inesistenti o sproporzionati rispetto all'entità delle stesse.

Rilevano sia l'indebita restituzione integrale che quella parziale.

Soggetti attivi	Reato proprio, di danno. Gli amministratori.
Condotta	Restituzione illegittima, palese o simulata, dei conferimenti effettuati dai soci o liberazione di costoro dall'obbligo di

	eseguirli.
Evento	Riduzione illegittima del capitale sociale.
Elemento soggettivo	Dolo generico
Pena (procedibilità d'ufficio)	Reclusione fino a un anno.

Aree aziendali esposte a rischio:

- Gestione economico-finanziaria dei conferimenti;
- Gestione attività di competenza degli amministratori;
- Gestione comunicazioni e rapporti fra CdA. Collegio Sindacale ed Assemblea dei soci.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;

- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art. 2627 cod. civ. Illegale ripartizione degli utili e delle riserve.

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

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

Osservazioni

Stante il particolare regime di indivisibilità delle riserve, la norma è di estrema rilevanza per le società cooperative.

Vengono in rilievo, *esclusivamente*, le riserve non distribuibili per legge (non quindi quelle configurate tali solo a livello statutario): nelle cooperative a mutualità prevalente, tuttavia, tutte le riserve sono indivisibili ed indisponibili, con le sole eccezioni della riserva da sovrapprezzo (che può a determinate condizioni essere rimborsato, salvo previsione statutaria contraria) e della riserva eventualmente costituita a beneficio dei soci finanziatori.

Si tenga altresì presente che la ripartizione di riserve indivisibili è suscettibile di comportare, oltre alla responsabilità penale degli amministratori alla stregua della norma in commento, la revoca dei medesimi e la gestione commissariale ex art.2545*sexiesdecies*.

Utili destinati per legge a riserva sono, in primo luogo, quelli da imputare a riserva legale ex art.2545*quater*.

Nelle cooperative a mutualità prevalente, inoltre, sono altresì indisponibili, e conseguentemente destinati a riserva, gli utili che, dedotte le destinazioni obbligatorie, eccedano i limiti di distribuibilità previsti dall'art.2514, c.1., lett.a).

Un particolare caso di utili destinati per legge a riserva è poi quello degli utili realizzati successivamente all'impiego di riserve indivisibili per la copertura di perdite (l. n.28/1999, art.3, c.1): tali utili non possono essere distribuiti fino alla ricostituzione delle riserve precedentemente impiegate (ancorché sulla perdurante vigenza di tale norma si registrino dubbi in dottrina).

Soggetti attivi	Reato contravvenzionale proprio, di danno. Gli amministratori
Condotta	La fattispecie prevede tre condotte alternative: – distribuzione di utili o acconti su utili non effettivamente conseguiti;

	<ul style="list-style-type: none"> – distribuzione di utili o acconti su utili destinati <i>per legge</i> a riserva; – distribuzione di riserve indisponibili <i>per legge</i>.
Evento	Riduzione illegittima del patrimonio sociale indisponibile.
Elemento soggettivo	Dolo generico.
Pena (procedibilità d'ufficio)	Arresto fino a un anno.

Aree aziendali esposte a rischio:

- gestione societaria utili e riserve, operazioni di ripartizione;
- attività del Consiglio di Amministrazione e dei suoi componenti;
- comunicazioni e gestione rapporti fra CdA, Collegio Sindacale; Assemblea dei soci.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di una procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;

- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2628 cod. civ. Illecite operazioni sulle azioni o quote sociali o della società controllante.

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

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

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

Osservazioni

La norma punisce la violazione del divieto di sottoscrizione o il superamento dei limiti di acquisto di azioni o quote proprie.

Quanto alla sottoscrizione, in sede di costituzione o di aumento di capitale, vale il divieto assoluto sancito dagli articoli 2357^{quater} (quanto alle s.p.a. ed alle cooperative-s.p.a) e 2474 (quanto alle s.r.l. ed alle cooperative-s.r.l.).

Quanto all'acquisto, l'art.2529 detta una disciplina speciale per le cooperative, alla cui stregua l'atto costitutivo può autorizzare gli amministratori ad acquistare quote o azioni proprie della società, purchè sussistano le condizioni previste dal secondo comma dell'art.2545^{quinquies} (rapporto tra patrimonio e indebitamento superiore a un quarto) e l'acquisto sia fatto nei limiti degli utili distribuibili e delle riserve disponibili risultante dall'ultimo bilancio regolarmente approvato.

L'estensione alla sottoscrizione o all'acquisto di partecipazioni della società controllante, contenuto al secondo comma della norma in esame, mira evidentemente ad impedire elusioni realizzabili compiendo l'operazione, anziché direttamente, per il tramite di una controllata.

Soggetti attivi	Reato proprio, di danno.
Condotta	Acquisto o sottoscrizione di azioni o quote proprie fuori dei casi consentiti dalla legge (per le cooperative, art.2529 cod. civ.).

Evento	Lesione all'integrità del capitale sociale o delle riserve non distribuibili.
Elemento soggettivo	Dolo generico.
Pena (procedibilità d'ufficio)	Reclusione fino a un anno.

Aree aziendali esposte a rischio:

- Gestione e vigilanza su società controllate.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2629 cod. civ. Operazioni in pregiudizio dei creditori.

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

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

Osservazioni

La norma sanziona il mancato rispetto delle tutele a beneficio del ceto creditorio imposte agli amministratori nel compimento di determinate operazioni.

Tali tutele sono fondamentalmente rappresentate dai termini dilatori di novanta giorni decorrenti dall'iscrizione nel registro delle imprese delle delibere di riduzione del capitale sociale (ipotesi non direttamente applicabile alle cooperative), di fusione e di scissione: termini imposti onde consentire ai creditori di proporre eventuale opposizione prima del compimento effettivo dell'operazione deliberata.

Trattasi di reato di danno, essendo richiesto un pregiudizio effettivo e non meramente potenziale.

Diversamente rispetto al passato (previgente art.2623, c.1), il reato è procedibile a querela del o dei soggetti danneggiati.

Soggetti attivi	Reato proprio, di danno. Gli amministratori.
Condotta	Effettuazione di operazioni di riduzione capitale, fusione o scissione senza il rispetto delle tutele poste dalla legge a tutela dei creditori (pubblicità e termini dilatori funzionali a eventuali opposizioni).
Evento	Danno in capo ai creditori.
Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).
Pena (procedibilità a querela)	Reclusione da sei mesi a tre anni.

Aree aziendali esposte a rischio:

- Operazioni societarie che possono incidere sull'integrità del capitale sociale.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2633 cod. civ. Indebita ripartizione dei beni sociali da parte dei liquidatori.

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

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

Osservazioni

La disposizione in esame "rinforza" con sanzione penale la responsabilità incombente sui liquidatori ex art.2491 per il caso di ripartizione di somme tra i soci prima del soddisfacimento dei creditori sociali o prima dell'accantonamento degli importi ad essi spettanti.

La norma è verosimilmente da ritenersi applicabile alla liquidazione ordinaria delle società ex artt.2487 ss. e non anche alle ipotesi di liquidazione coatta amministrativa delle cooperative: in tale seconda fattispecie, infatti, i liquidatori non sono organi della società nominati dall'assemblea ma soggetti designati dall'autorità di vigilanza, ed eventuali irregolarità o condotte illecite da costoro poste in essere non paiono suscettibili d'ingenerare la responsabilità amministrativa della cooperativa ex d.lgs. n.231/2001.

Trattasi anche qui di reato di danno (pregiudizio ai creditori) procedibile solo a querela dei soggetti lesi dalla condotta illecita.

Soggetti attivi	Reato proprio, di danno. I liquidatori.
Condotta	Ripartizione dei beni sociali tra i soci prima del soddisfacimento dei creditori sociali o prima dell'accantonamento delle somme destinate a soddisfarli.
Evento	Danno in capo ai creditori.
Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).
Pena (procedibilità a querela)	Reclusione da sei mesi a tre anni.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;

- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa–contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2636 cod. civ. Illecita influenza sull'assemblea.

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

Osservazioni

Diversamente rispetto al passato, dove soggetti attivi dell'illecito potevano essere solo gli amministratori (reato proprio), la norma estende oggi la punibilità a chiunque ponga in essere la condotta incriminata, *in primis* i soci.

La fattispecie in esame è ricalcata su quella della truffa, e configura un reato d'evento (causazione di una delibera assembleare difforme da quella che sarebbe stata adottata in assenza del comportamento delittuoso).

Il dolo è specifico e consiste nel perseguimento di un'utilità indebita per sé o per altri.

L'esempio tradizionale è costituito dalla rappresentazione di fatti falsi o dal silenzio su fatti rilevanti da parte degli amministratori, in guisa tale da condizionare fraudolentemente la formazione della volontà assembleare.

Si ritiene che il reato non sussista qualora la deliberazione *de quo* sarebbe stata comunque adottata anche in assenza della condotta illecita.

Trattasi di reato solitamente commesso nell'interesse di parte e non della società, la quale si configura quale soggetto offeso: tale considerazione induce a ritenerne la rilevanza alquanto marginale ai fini dell'applicazione del d.lgs. n.231/2001.

Soggetti attivi	Reato comune di evento. Chiunque.
Condotta	Impiego di atti simulati o fraudolenti (es: esposizione o produzione di fatti o documenti falsi, reticenza su circostanze

	rilevanti).
Evento	Adozione di decisioni assembleari difformi rispetto a quelle che sarebbero state assunte in assenza della condotta fraudolenta.
Elemento soggettivo	Dolo specifico (fine di conseguire un ingiusto profitto per sé o per altri).
Pena (procedibilità d'ufficio)	Reclusione da sei mesi a tre anni.

Aree aziendali esposte a rischio:

- approvazione bilancio consuntivo;
- gestione convocazione, comunicazioni, verbalizzazione assemblee dei soci.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di una procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;

- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2637 cod. civ. Aggiotaggio.

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

Osservazioni

La norma si applica esclusivamente alle fattispecie concernenti titoli non quotati (o per i quali non è stata richiesta l'autorizzazione alla negoziazione): per questi ultimi rilevano le previsioni del T.U.F. introdotte dalla legge n.62/2005.

Possono pertanto venire in considerazione gli strumenti finanziari emessi dalle società cooperative, sia quelli di nuova generazione introdotti dalla riforma del diritto societario, sia le azioni di sovvenzione e le azioni di partecipazione cooperativa disciplinate dalla legge n.59/1992.

Rilevano, altresì, le obbligazioni e più in generale i titoli di debito contemplati dall'art.2526.

La condotta illecita si sostanzia nella divulgazione di notizie false o nell'adozione di altri artifici comunque idonei a trarre in inganno gli operatori, e più in generale il pubblico, provocando un effetto distorsivo al rialzo o al ribasso sul prezzo di scambio dei titoli.

Il delitto in esame è configurato quale reato di pericolo, non essendo richiesta la causazione di un pregiudizio concreto.

Si ritiene che la comunicazione individuale o comunque ad un numero circoscritto di soggetti non integri il reato di aggioaggio : ricorrerà in tale ipotesi, eventualmente, la fattispecie del reato di truffa.

Soggetti attivi	Reato comune di pericolo. Chiunque.
Condotta	Diffusione di notizie false, realizzazione di operazione simulate (es: finte vendite cospicue dirette a produrre un ribasso dei valori di scambio), impiego di altri artifici ingannatori idonei ad alterare sensibilmente i prezzi di strumenti finanziari non quotati.
Evento	Non è richiesto un danno concreto.
Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).

Pena

(procedibilità d'ufficio)

Reclusione da uno a cinque anni.

Aree aziendali esposte a rischio:

- Emissione comunicati stampa e informative al mercato.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2629bis cod. civ. Omessa comunicazione del conflitto di interessi.

L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico

di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, o del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.

Osservazioni

La norma è applicabile agli amministratori o membri del consiglio di gestione di società quotate (o diffuse), banche, assicurazioni e fondi pensione; conseguentemente, con l'eccezione delle B.c.c. e delle banche popolari, essa riveste importanza alquanto limitata per le cooperative commerciali.

Viene sostanzialmente punito con sanzione penale il comportamento omissivo dell'amministratore che non adempia al dovere di *disclosure* prescritto dall'art.2391 cod.civ.

Il reato è di danno (e non di mero pericolo) essendo richiesta, ai fini della punibilità, la produzione di un pregiudizio in capo alla società o ai terzi (creditori, fornitori, etc..).

Alla luce di quest'ultima considerazione, è da ritenere determinante, quantunque non richiamato dalla norma in commento, il superamento della cd. prova di resistenza, vale a dire l'accertamento della concreta efficacia determinante del voto dell'amministratore in conflitto d'interessi; efficacia determinante che costituisce il presupposto per l'impugnabilità delle deliberazioni adottate (art.2391, c.3).

La responsabilità amministrativa della società, ex d.lgs. n.231/2001, potrà sorgere nelle ipotesi di danno ai terzi, restando esclusa in quei casi che vedano viceversa l'ente quale soggetto offeso e danneggiato dal reato .

Soggetti attivi	Reato proprio di danno. Gli amministratori (o componenti il consiglio di gestione).
Condotta	Mancato rispetto dell'obbligo di <i>disclosure</i> (dovere informativo) da parte dell'amministratore/i in conflitto di interessi.
Evento	Danno alla società o a terzi.
Elemento soggettivo	Dolo generico (consapevolezza e volontarietà della condotta).
Pena (procedibilità d'ufficio)	Reclusione da uno a tre anni.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di un procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato.

Art.2638 cod. civ. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

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

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Osservazioni

La norma è di grande rilevanza per le cooperative, in considerazione del regime di vigilanza particolare cui tali enti sono sottoposti ex d.lgs. n.220/2002 (revisioni ed ispezioni straordinarie).

Trattasi di reato proprio; soggetti attivi possono essere i medesimi soggetti contemplati dagli artt.2621 e 2622 in tema di falso in bilancio: amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori.

Anche la condotta (nel caso di cui al primo comma) è per certi versi simile: essa consiste nell'esposizione di fatti falsi o nel silenzio omissivo su fatti rilevanti concernenti la situazione economica, patrimoniale o finanziaria dell'ente.

L'elemento soggettivo è rappresentato dal fine di ostacolare l'esercizio delle funzioni di vigilanza: si pensi, in particolar modo, alle informazioni richieste in sede di revisione in conformità all'apposito verbale-modello predisposto dal Ministero.

Il reato è di condotta (vincolata) nell'ipotesi contemplata dal primo comma (esso sussiste indipendentemente dall'effettivo impedimento delle funzioni di vigilanza); è di evento (a condotta libera) nel caso previsto dal secondo comma (è richiesto che i comportamenti infedeli, quali che siano, abbiano concretamente ostacolato le funzioni di vigilanza).

La pena è la reclusione da uno a quattro anni.

Soggetti attivi	Reato proprio di pericolo (c.1) o di evento (c.2). Amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società od enti sottoposti per legge a vigilanza pubblica.
Condotta	<ul style="list-style-type: none"> • Ipotesi 1 (c.1): esposizione di fatti falsi od omissione di informazioni obbligatorie (nelle comunicazioni previste dalla legge alle autorità di vigilanza) sulla situazione economica, patrimoniale o finanziaria della società , in modo idoneo ad indurre in errore i destinatari; • Ipotesi 2 (c.2): il reato si configura a condotta libera (“in qualsiasi forma”).

Evento	Solo nella seconda ipotesi: ostacolo (concreto) delle funzioni dell'autorità di vigilanza.
Elemento soggettivo	Dolo specifico (fine di ostacolare i controlli).
Pena (procedibilità d'ufficio)	Reclusione da uno a quattro anni.

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;
- Osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività per la redazione dei bilanci e delle relazioni periodiche;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere e rispettare il piano dei conti di contabilità generale, le regole interne per la gestione e il trattamento delle informazioni, dei dati riservati e per la comunicazione all'esterno di documenti e informazioni, il manuale di contabilità industriale, se presenti;
- Previsione di una procedura formalizzata per la redazione del bilancio di esercizio (livelli autorizzativi, segregazione dei compiti, tracciabilità e archivio documentazione);
- Previsione, da parte della Direzione amministrativa-contabile, di una dichiarazione di veridicità e correttezza dei dati di bilancio trasmessi;
- Previsione di una riunione tra O.d.V. e CS prima dell'approvazione del bilancio con tema la valutazione delle poste di bilancio;
- Segnalazione degli incarichi di revisione attribuiti alla società di revisione (incarichi e audit specifici non rientranti attività ordinaria);
- Previsione di specifiche clausole per terzi/consulenti e promotori per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati societari e sulle procedure aziendali in essere;
- Segnalazione all'O.d.V. di operazioni straordinarie inerenti il capitale sociale;
- Trasmissione all'O.d.V. dei prospetti di bilancio civilistico e consolidato;
- Trasmissione all'O.d.V. della documentazione e delle osservazioni al bilancio da parte del CS e società di revisione.

ART. 25 QUATER D.LGS 231/2001 - DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.

In relazione alla commissione dei delitti aventi finalità di terrorismo o di everzione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore a dieci anni, la sanzione pecuniaria da duecento a settecento quote;

b) se il delitto è punito con la pena della reclusione non inferiore a dieci anni o con l'ergastolo la sanzione pecuniaria da quattrocento a mille quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9 comma 2 per una durata non inferiore ad un anno.

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

Le disposizioni dei commi 1, 2 e 3 si applicano altresì in relazione alla commissione di delitti diversi da quelli indicati nel comma 1 che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999.

Osservazioni

L'art. 25 quater è una norma aperta che punisce i reati aventi finalità di terrorismo o di everzione dell'ordine democratico, previsti nel codice penale italiano, dalle leggi speciali, o in violazione della Convenzione internazionale di New York del 9 dicembre 1999.

La norma richiamata non fa rinvio a specifiche fattispecie di reato, mostrando così qualche carenza sotto il profilo della tassatività. La categoria di reati richiamata fa riferimento ad una molteplicità di fattispecie, la cui condotta criminosa può realizzarsi in diversi modi.

In particolare, il ventaglio di fattispecie ricompreso tra l'art. 270-bis e 270-sezies c.p. prevede una serie di condotte che vanno dalla promozione, costituzione, organizzazione o finanziamento di associazioni deputate a perpetrare azioni violente con finalità terroristiche e/o eversive, all'assistenza agli associati con finalità di terrorismo, all'arruolamento di soggetti per la realizzazione di atti di violenza e/o di sabotaggio connessi a finalità terroristiche, all'addestramento e preparazione di detti soggetti all'uso di armi e strumenti offensivi, fino alle generiche condotte qualificate in una vera norma di chiusura come aventi "finalità di terrorismo" (art. 270 sexies c.p.).

In ogni caso al di là delle singole fattispecie, l'art. 25 quater D.lgs 231/2001 opera un vero rinvio generale "aperto" a tutte le ipotesi attuali e future di reati terroristici ed eversivi.

Nell'ambito cooperativo il rischio non è escludibile a priori soprattutto se si considera che la Convenzione di New York ritiene penalmente rilevante anche l'appoggio economico indiretto (ma pur sempre doloso) ad organizzazioni o gruppi terroristici, nazionali o internazionali.

Infatti la responsabilità penale (e dunque l'eventuale responsabilità della cooperativa), sorge non soltanto a carico di chi realizza la condotta tipica descritta nella singola fattispecie incriminatrice, ma anche a carico di concorra nel reato fornendo un contributo materiale o morale alla realizzazione dello stesso.

Pertanto tutte le società che nell'ambito della propria attività gestiscono somme di denaro destinate a società, gruppi, associazioni, enti, anche a titolo apparentemente benefico, si trovano esposte al rischio concreto di incorrere in tali fattispecie di reato a titolo di concorso, per aver posto in essere condotte di agevolazione, istigazione, finanziamento ecc.

Le aree a maggiore rischiosità sono pertanto:

- Ricerca, gestione e selezione del personale;
- Identificazione e contrattazione con fornitori, collaboratori, consulenti e *partners*;
- Creazione società di scopo, acquisizione partecipazioni, creazione e gestione *partnerships/accordi/joint ventures* ecc.
- Stipula e gestione contratti con la Pubblica Amministrazione;
- Gestione gare, appalti ed altre procedure ad evidenza pubblica;
- Gestione finanziaria-contabile, controllo di gestione, *internal auditing*, rendicontazione;
- Gestione omaggi, regalie e sponsorizzazioni;
- Gestione rapporti con organi amministrativi aziendali e gestione di eventuali conflitti di interesse;
- Gestione contratti ed attività in aree geografiche notoriamente a rischio.

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;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Conoscere liste nominative ed elenco dei paesi a rischio individuati dall'O.d.V. ;

- Previsione di procedura per la verifica preventiva del c.d. “rischio paese” in fase di attuazione iniziative economiche/commerciali in determinate aree geografiche;
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- Valutazione di requisiti di moralità della controparte mediante verifica di idonea documentazione o informazioni volte a valutare affidabilità;
- Previsione di clausole con partner commerciali che vietano la cessione del contratto o il subappalto;
- Tracciabilità delle transazioni finanziarie e loro beneficiari;
- Previsione di specifiche clausole per terzi/agenti per il rispetto del Codice etico e Modello;
- Formazione periodica sui delitti di criminalità organizzata ed eversione ordine democratico e sulle procedure aziendali in essere;
- Inoltro all'O.d.V. del riepilogo operazioni a rischio (ad esempio avanzamento delle commesse aperte);
- Segnalazione all'O.d.V. di operazioni anomale o ad alto indice di rischio.

Si segnala che i centri servizi di assistenza contabile, fiscale e di elaborazione dati di Confcooperative operanti ai sensi del D.lgs. n. 241 del 1997 e quelli convenzionanti con questi ultimi e promossi da articolazioni territoriali di Confcooperative ai sensi dell'articolo 11 del D.M. n. 164 del 1999 e che operano a favore degli enti aderenti alle stesse, sono altresì soggetti agli obblighi specifici stabiliti dal D.Lgs. 21 novembre 2007, n.231, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Per un'ampia disamina di tale disciplina si rinvia alla trattazione specifica del D.Lgs. n. 231/2007, contenuta nel commento agli articoli 648, 648*bis* e 648*ter* c.p. (*infra*, nelle presenti Linee Guida).

ART. 25 QUATER-1 D.LGS 231/2001 - PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI.

In relazione alla commissione dei delitti di cui all'articolo 583-bis del codice penale si applicano all'ente, nella cui struttura è commesso il delitto, la sanzione pecuniaria da 300 a 700 quote e le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno. Nel caso in cui si tratti di un ente privato accreditato è altresì revocato l'accreditamento.

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

Art. 583bis c.p. Pratiche di mutilazione degli organi genitali femminili.

Chiunque, in assenza di esigenze terapeutiche, cagiona una mutilazione degli organi genitali femminili è punito con la reclusione da quattro a dodici anni. Ai fini del presente articolo, si intendono come pratiche di mutilazione degli organi genitali femminili la clitoridectomia, l'escissione e l'infibulazione e qualsiasi altra pratica che cagioni effetti dello stesso tipo.

Chiunque, in assenza di esigenze terapeutiche, provoca, al fine di menomare le funzioni sessuali, lesioni agli organi genitali femminili diverse da quelle indicate al primo comma, da cui derivi una malattia nel corpo o nella mente, è punito con la reclusione da tre a sette anni. La pena è diminuita fino a due terzi se la lesione è di lieve entità.

La pena è aumentata di un terzo quando le pratiche di cui al primo e al secondo comma sono commesse a danno di un minore ovvero se il fatto è commesso per fini di lucro.

Le disposizioni del presente articolo si applicano altresì quando il fatto è commesso all'estero da cittadino italiano o da straniero residente in Italia, ovvero in danno di cittadino italiano o di straniero residente in Italia. In tal caso, il colpevole è punito a richiesta del Ministro della giustizia.

Art. 583ter c.p. Pena accessoria.

La condanna contro l'esercente una professione sanitaria per taluno dei delitti previsti dall'articolo 583bis importa la pena accessoria dell'interdizione dalla professione da tre a dieci anni. Della sentenza di condanna è data comunicazione all'Ordine dei medici chirurghi e degli odontoiatri.

Osservazioni

La fattispecie di reato in questione, difficilmente configurabile nel generico mondo cooperativo, è riferita essenzialmente a quelle società che hanno come oggetto sociale tipico l'erogazione di servizi sanitari, assistenziali, di volontariato ecc. (con particolare attenzione ad enti presso cui si svolgono attività chirurgiche finalizzate ad interventi di ginecologia-ostetricia). Tale enti potrebbero incorrere nel reato di cui all'art. 583 bis c.p., accettando ad esempio di praticare l'infibulazione o altre pratiche di mutilazione nelle proprie strutture o con propri mezzi e personale, al di fuori di una specifica esigenza terapeutica certificata.

L'art. 24quater 1 D.lgs 231/2001 interviene sul criterio oggettivo di imputazione: si prevede infatti la punibilità dell'ente "nella cui struttura" sia commesso il delitto.

In altri termini un'interpretazione rigorosa potrebbe condurre a ritenere non prevalente il criterio dell'interesse/vantaggio: potrebbe essere considerato sufficiente il dato fattuale dell'effettuazione della mutilazione nella sua struttura, configurando così un chiaro caso di responsabilità penale oggettiva.

In ogni caso, occorrerà indagare in modo puntuale quale sia il rapporto giuridico-economico tra la struttura sanitaria, in cui si svolge eventualmente l'intervento chirurgico incriminato, e il sanitario responsabile della materiale esecuzione.

Soggetto attivo	Chiunque
Condotta	<ul style="list-style-type: none"> - Cagionare mutilazioni di organi genitali femminili (clitoridectomia, escissione, infibulazione ecc.). - Provocare, con il fine di menomare le funzioni sessuali, altre lesioni agli organi genitali femminili da cui derivi una malattia nel corpo o nella mente. <p>In ogni caso, quale condizione di punibilità, è previsto che le condotte siano realizzate in assenza di esigenze terapeutiche.</p>
Elemento soggettivo	<p>Dolo generico per ipotesi della mutilazione.</p> <p>Dolo specifico per seconda ipotesi di reato, ossia finalità di menomare le funzioni sessuali.</p>
Pena	<p>Reclusione da 4 a 12 anni (comma 1);</p> <p>Reclusione da tre a sette anni (comma 2).</p>

Aree aziendali esposte a rischio:

- Processi e funzioni coinvolti nell'erogazione di servizi sanitari e assistenziali alla persona.

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;
- Inserimento nello Statuto sociale e nel Codice Etico di principi di massima tutela della dignità e libertà della persona umana, nonché di principi esplicitamente finalizzati a vietare qualsiasi condotta di causazione o agevolazione di

comportamenti che integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25 quater 1 D.Lgs 231/2001;

- 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.;
- Creazione di percorsi formativi specifici, rivolti soprattutto a personale straniero, in merito al rispetto della normativa vigente e dei principi di tutela della libertà e dignità umana appartenenti al nostro ordinamento e allo scopo della stessa cooperativa;
- Adeguato sistema di procure e deleghe (completo, coerente e pubblicizzato) con individuazione delle figure aziendali responsabili dei processi e delle aree aziendali a rischio;
- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta erogazione dei servizi istituzionali (es. compilazione di schede informative, riunioni formali con la Direzione, corsi di formazione professionali);
- *Audit e/o* incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle attività svolte all'interno delle aree sensibili individuate, nel rispetto della riservatezza del paziente (dati degli utenti, servizi erogati, anomalie e criticità riscontrate, dati dei sanitari intervenuti, accertamento dell'esigenza terapeutica).

ART. 25 QUINQUIES D.LGS 231/2001 - DELITTI CONTRO LA PERSONALITA' INDIVIDUALE.

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

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

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

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

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

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

Art. 600 c.p. Riduzione o mantenimento in schiavitù o servitù.

Chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento, è punito con la reclusione da otto a venti anni.

La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Osservazioni

Il reato consiste nell'esercizio su una persona di un potere di proprietà o di soggezione continua, per costringerla a prestazioni lavorative o sessuali o comunque ad uno sfruttamento della stessa.

Pertanto, la condotta non si riconduce necessariamente ad una situazione di diritto, ma a qualunque situazione di fatto avente per effetto la riduzione della persona offesa nella condizione materiale dello schiavo, e cioè nella soggezione esclusiva ad un altrui potere di disposizione.

In particolare, le condotte rilevanti tipizzate sono riconducibili a tre categorie:

1) esercizio su una persona di poteri corrispondenti a quelli del diritto di proprietà.

Tale previsione costituisce la traduzione normativa della nozione pacificamente accolta di schiavitù, di cui all'art. 1 della Convenzione sulla schiavitù di Ginevra del 15 settembre 1926 e all'art. 7 dello Statuto istitutivo della Corte Penale Internazionale.

2) Riduzione di una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento.

Le condotte di soggezione così delineate assumono penale rilievo quando sono attuate mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona (art. 600, c.2 c.p.).

3) Mantenimento di una persona nello stato di soggezione delineato in precedenza.

Attribuendo esplicito rilievo al mantenimento in stato di soggezione, il legislatore supera le obiezioni di quanti ritenevano che la schiavitù potesse riguardare esclusivamente persone in libertà, sanzionando chi mantenga in soggezione soggetti già privati da altri della libertà.

Soggetto attivo	Chiunque; è reato comune.
Condotta	<ul style="list-style-type: none"> - Esercizio su una persona di poteri corrispondenti a quelli del diritto di proprietà; - riduzione di una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento. - mantenimento di una persona nello stato di soggezione così delineato
Elemento soggettivo	Dolo. Coscienza e volontà di ridurre la vittima ad una res.
Pena	Reclusione da 8 a 20 anni.

Il reato potrebbe configurarsi in capo ad una cooperativa soprattutto nel processo di selezione, assunzione e gestione del personale.

Pertanto i **processi/attività aziendali maggiormente a rischio** in relazione a tale fattispecie sono essenzialmente quelle relative a:

- Selezione, assunzione e gestione del personale, soprattutto se stagionale ed addetto ad attività lavorative tipicamente esposte a rischi di sfruttamento illecito (lavori socialmente utili, lavori stagionali ad esempio nel settore agricolo ecc.);
- Gestione contratti di appalto e subappalto;
- Erogazione apparente di servizi di trasporto, organizzazione viaggi, progetti formativi, introduzione al lavoro ecc.

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;
- Inserimento nello Statuto sociale e nel Codice Etico di principi di massima tutela della dignità e libertà della persona umana, nonché di principi esplicitamente finalizzati a vietare qualsiasi condotta di causazione o agevolazione di comportamenti che integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25 quinquies D.Lgs 231/2001;
- 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 e delle aree aziendali a rischio;
- Diffusione di regolamenti, procedure e prassi aziendali sulla corretta gestione delle attività di procacciamento della forza lavoro, gestione del personale, rispetto della normativa sul lavoro vigente, da diffondere eventualmente anche a partners e fornitori;
- Garanzia della corretta gestione dei rapporti sindacali, anche al fine di agevolare eventuali controlli su corretta applicazione normativa e contrattualistica in materia di lavoro all'interno della cooperativa;
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di sospette violazioni del Codice etico o di eventuali anomalie/atipicità (es. assunzione personale minorenni).

Art. 600bis c.p. Prostituzione minorile.

Chiunque induce alla prostituzione una persona di età inferiore agli anni diciotto ovvero ne favorisce o sfrutta la prostituzione è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 a euro 154.937.

Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di denaro o di altra utilità economica, è punito con la reclusione da sei mesi a tre anni e con la multa non inferiore a euro 5.164.

Nel caso in cui il fatto di cui al secondo comma sia commesso nei confronti di persona che non abbia compiuto gli anni sedici, si applica la pena della reclusione da due a cinque anni.

Se l'autore del fatto di cui al secondo comma è persona minore di anni diciotto si applica la pena della reclusione o della multa, ridotta da un terzo a due terzi.

Osservazioni

Il reato consiste nell'induzione alla prostituzione, o nel favoreggiamento/sfruttamento di essa, di un minore di diciotto anni.

In particolare l'art. 600 bis c.p. punisce due distinte tipologie di condotte: quella di chi sfrutta, induce o favorisce la prostituzione minorile, e quella di chi consuma con un minore atti sessuali, punendo al tempo stesso domanda ed offerta della prostituzione minorile.

Le condotte criminose previste da tale norma (e dal successivo art. 600ter c.p.) potrebbero astrattamente ipotizzarsi in quelle realtà cooperative che gestiscono comunità alloggio per minori disagiati, affidati ai servi sociali o semplicemente bisognosi di assistenza sanitaria. La concentrazione di un numero elevato di minori nella medesima struttura, l'alloggio permanente degli stessi, sono elementi che impongono ai vertici della struttura un'attenta attività di vigilanza al fine di scongiurare il verificarsi di condotte di reato finalizzate ad agevolare anche lontanamente la pornografia minorile.

Soggetto attivo	Chiunque
Condotta	1) Induzione, sfruttamento, favoritamento prostituzione minorile; 2) Compimento atti sessuali con minore.
Elemento soggettivo	Dolo generico
Pena	1) Reclusione da 6 a 12 anni e multa da 15.493 a 154.937 euro. 2) Reclusione da 6 mesi a 3 anni e multa non inferiore a 5.164 euro.

Aree aziendali esposte a rischio:

- Processi e funzioni coinvolti nell'erogazione di servizi sanitari e assistenziali alla persona, ed in particolare a minori;
- Selezione, assunzione e gestione del personale, specie se minorenni.

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 e delle aree

aziendali a rischio, con particolare riferimento ai soggetti autorizzati ad intrattenere rapporti con utenti minorenni destinatari di servizi della cooperativa;

- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta erogazione dei servizi istituzionali, soprattutto a favore di utenti minorenni (es. compilazione di schede informative, riunioni formali con la Direzione, corsi di formazione professionali);
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle attività svolte all'interno delle aree sensibili individuate, nel rispetto della riservatezza dell'utente (dati degli utenti, servizi erogati, anomalie e criticità riscontrate, dati dei sanitari intervenuti, accertamento dell'esigenza terapeutica).

Art. 600ter c.p. Pornografia minorile.

Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche è punito con la reclusione da sei a dodici anni e con la multa da euro 25.822 a euro 258.228.

Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.

Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.

Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.

Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.

Osservazioni

Rientrano in tale reato le seguenti condotte.

1) Lo sfruttamento di minori al fine della realizzazione di esibizioni pornografiche o di produzione di materiale di tale tipo: la norma parla letteralmente di "sfruttamento" e non di mero utilizzo, pertanto occorre che il minore venga inserito in una organizzazione e che vi sia una pluralità e non occasionalità di impieghi nelle attività illecite; l'esibizione allude ad una partecipazione dal vivo ad attività pornografica, la produzione può

realizzarsi tanto con foto (su carta, floppy, disk, file ecc.) e con registrazioni (videocassette, audiocassette, dvd, ecc).

2) Commercio di materiale pornografico: ossia alienazione del materiale in questione per fini di lucro, svolta con un'organizzazione di impresa.

3) Diffusione di materiale pornografico o di notizie finalizzate all'adescamento o sfruttamento sessuale di minori: le condotte in questione possono essere poste con ogni mezzo, anche telematico.

4) Cessione di materiale pornografico prodotto mediante lo sfruttamento di minori, sia a titolo gratuito che oneroso.

L'articolo 600^{ter} c.p. prevede al primo comma addirittura un reato di pericolo concreto, finalizzato a garantire una tutela anticipata della libertà sessuale del minore, reprimendo quei comportamenti prodromici che, anche se non necessariamente a fine di lucro, ne mettono a repentaglio il libero sviluppo personale con la mercificazione del corpo e l'immissione nel circuito della pedofilia.

Le condotte criminose previste da tale norma (e dal precedente art. 600^{bis} c.p.) potrebbero astrattamente ipotizzarsi in quelle realtà cooperative che gestiscono comunità alloggio per minori disagiati, affidati ai servi sociali o semplicemente bisognosi di assistenza sanitaria. La concentrazione di un numero elevato di minori nella medesima struttura, l'alloggio permanente degli stessi, sono elementi che impongono ai vertici della struttura un'attenta attività di vigilanza al fine di scongiurare il verificarsi di condotte di reato finalizzate ad agevolare anche lontanamente la pornografia minorile. Per giurisprudenza costante configura la fattispecie *de quo* la trasmissione di un'immagine/videoripresa a contenuto pedopornografico ad esempio attraverso un telefono cellulare o altri dispositivi portatili, oppure la cessione occasionale di immagini di minori ipoteticamente finalizzate ad usi perversi.

Soggetto attivo	Chiunque
Condotta	<ol style="list-style-type: none"> 1) Sfruttamento di minori al fine della realizzazione di esibizioni pornografiche o di produzione di materiale di tale tipo; 2) Commercio di materiale pornografico; 3) Diffusione di materiale pornografico o di notizie finalizzate all'adescamento o sfruttamento sessuale di minori; 4) Cessione di materiale pornografico prodotto mediante lo sfruttamento di minori, sia a titolo gratuito che oneroso.
Elemento soggettivo	Dolo generico
Pena	<p>Hp 1) 2) Reclusione da 6 a 12 anni e multa da 25.822 a 258.228 euro.</p> <p>Hp 3) Reclusione da 1 a 5 anni e multa da 2.582 a 51.645 euro.</p> <p>Hp 4) Reclusione fino a 3 anni e multa da 1.549 a 5.164 euro.</p>

Aree aziendali esposte a rischio:

- Processi e funzioni coinvolti nell'erogazione di servizi sanitari e assistenziali alla persona, ed in particolare a minori;
- Selezione, assunzione e gestione del personale, specie se minorenni;
- Gestione dei sistemi informativi.

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 e delle aree aziendali a rischio, con particolare riferimento ai soggetti autorizzati ad intrattenere rapporti con utenti minorenni destinatari di servizi della cooperativa;
- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta erogazione dei servizi istituzionali, soprattutto a favore di utenti minorenni (es. compilazione di schede informative, riunioni formali con la Direzione, corsi di formazione professionali);
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Integrazione del sistema privacy aziendali con: esplicita previsione di sistemi di tutela della riservatezza dei dati sensibili inerenti utenti minorenni destinatari dei servizi della cooperativa; regolamentazione delle modalità di utilizzo degli elaboratori, della posta elettronica, della connessione internet, nonché di ogni altra strumentazione elettronica aziendale anche astrattamente idonea a registrare, conservare, riprodurre e trasferire suoni ed immagini;
- Previsione di appositi controlli sugli strumenti divulgativi in possesso della società;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle attività svolte all'interno delle aree sensibili individuate, nel rispetto della riservatezza dell'utente (dati degli utenti, servizi erogati, anomalie e criticità riscontrate, dati dei sanitari intervenuti, accertamento dell'esigenza terapeutica);
- Si rinvia altresì ai protocolli previsti nella sezione dedicata ai reati informatici ex art. 24bis D.Lgs 231/2001.

Art. 600^{quater} c.p. Detenzione di materiale pornografico.

Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli

anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.

La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

Osservazioni

E' la condotta di chi dispone o si procura materiale pedopornografico.

Procurarsi significa acquistare la disponibilità fisica del materiale pedopornografico; disporre vuol dire poter utilizzare il materiale stesso, pur non avendone necessariamente la materiale disponibilità (es. accesso ad archivi *on line* o a siti protetti).

Soggetto attivo	Chiunque (al di fuori delle ipotesi previste dall'art. 600 ter c.p.)
Condotta	Procurarsi Detenere materiale pedopornografico
Elemento soggettivo	Dolo generico
Pena	Reclusione fino a tre anni e multa non inferiore a 1.549 euro.

Aree aziendali esposte a rischio:

- Gestione dei sistemi informativi;
- Attività svolte con l'ausilio di strumentazione informatica aziendale (pc, sw, connessioni internet ecc).

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 e delle aree aziendali a rischio, con particolare riferimento ai soggetti autorizzati ad intrattenere rapporti con utenti minorenni destinatari di servizi della cooperativa;
- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta erogazione dei servizi istituzionali, soprattutto a favore di utenti minorenni (es. compilazione di schede informative, riunioni formali con la Direzione, corsi di formazione professionali);
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Integrazione del sistema privacy aziendali con: esplicita previsione di sistemi di tutela della riservatezza dei dati sensibili inerenti utenti minorenni destinatari dei

servizi della cooperativa; regolamentazione delle modalità di utilizzo degli elaboratori, della posta elettronica, della connessione internet, nonché di ogni altra strumentazione elettronica aziendale anche astrattamente idonea a registrare, conservare, riprodurre e trasferire suoni ed immagini;

- Previsione di appositi controlli sugli strumenti divulgativi in possesso della società;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle attività svolte all'interno delle aree sensibili individuate, nel rispetto della riservatezza dell'utente (dati degli utenti, servizi erogati, anomalie e criticità riscontrate, dati dei sanitari intervenuti, accertamento dell'esigenza terapeutica);
- Si rinvia altresì ai protocolli previsti nella sezione dedicata ai reati informatici ex art. 24bis D.Lgs 231/2001.

Art. 600quater, 1 c.p. Pornografia virtuale.

Le disposizioni di cui agli articoli 600ter e 600quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Osservazioni

Il reato stabilisce la punibilità delle condotte relative alla produzione, commercio, diffusione, cessione ed acquisto di materiale pornografico realizzato con l'utilizzo di minori degli anni diciotto, anche qualora le condotte in questione hanno ad oggetto immagini virtuali.

Le condotte criminose previste da tale norma potrebbero astrattamente ipotizzarsi, come già anticipato per la fattispecie di cui all'art. 600ter c.p., in quelle realtà cooperative che gestiscono comunità alloggio per minori disagiati, affidati ai servizi sociali o semplicemente bisognosi di assistenza sanitaria. La concentrazione di un numero elevato di minori nella medesima struttura, l'alloggio permanente degli stessi, sono elementi che impongono ai vertici della struttura un'attenta attività di vigilanza al fine di scongiurare il verificarsi di condotte di reato finalizzate ad agevolare anche lontanamente la pornografia minorile.

Il riferimento va anche a quelle imprese che svolgono, come attività principale o secondaria, la gestione di servizi pubblicitari, editoriali, cinematografici, commerciali *on line*, che potrebbero incorrere in una delle condotte sopra descritte facendo circolare ad esempio su siti, blog, forum, prodotti audiovisivi, immagini pornografiche aventi ad oggetto minori.

Aree aziendali esposte a rischio:

- Processi e funzioni coinvolti nell'erogazione di servizi sanitari e assistenziali alla persona, ed in particolare a minori;
- Selezione, assunzione e gestione del personale, specie se minorenni;
- Gestione dei sistemi informativi;
- Attività svolte con l'ausilio di strumentazione informatica aziendale (pc, sw, connessioni internet ecc).

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 e delle aree aziendali a rischio, con particolare riferimento ai soggetti autorizzati ad intrattenere rapporti con utenti minorenni destinatari di servizi della cooperativa;
- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta erogazione dei servizi istituzionali, soprattutto a favore di utenti minorenni (es. compilazione di schede informative, riunioni formali con la Direzione, corsi di formazione professionali);
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Integrazione del sistema privacy aziendali con: esplicita previsione di sistemi di tutela della riservatezza dei dati sensibili inerenti utenti minorenni destinatari dei servizi della cooperativa; regolamentazione delle modalità di utilizzo degli elaboratori, della posta elettronica, della connessione internet, nonché di ogni altra strumentazione elettronica aziendale anche astrattamente idonea a registrare, conservare, riprodurre e trasferire suoni ed immagini;
- Previsione di appositi controlli sugli strumenti divulgativi in possesso della società;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle attività svolte all'interno delle aree sensibili individuate, nel rispetto della riservatezza dell'utente (dati degli utenti, servizi erogati, anomalie e criticità riscontrate, dati dei sanitari intervenuti, accertamento dell'esigenza terapeutica);
- Si rinvia altresì ai protocolli previsti nella sezione dedicata ai reati informatici ex art. 24bis D.Lgs 231/2001.

Art. 600quinquies c.p. Iniziative turistiche volte allo sfruttamento della prostituzione minorile.

Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 e euro 154.937.

Osservazioni

Il reato punisce la condotta di chi organizza o propaganda viaggi finalizzati alla fruizione della prostituzione minorile (c.d. *sex tour*).

La punibilità è limitata agli organizzatori e propagandisti dei viaggi, non agli aderenti all'iniziativa come clienti, e colpisce vere e proprie attività "preparatorie" rispetto ai delitti di cui all'art. 600 bis c.p.

Le società concretamente esposte al rischio di commissione di tale reato sono principalmente quelle operanti nel settore turistico inteso in senso ampio (*tour operator*, agenzie di viaggio, agenzie specializzate nell'offerta di servizi *facility management* alle imprese per la gestione dei viaggi, incontri di lavoro ecc.); tuttavia è sufficiente anche l'organizzazione (o addirittura la mera propaganda) occasionale e sporadica di un solo viaggio, non essendo necessario che l'agente svolga l'attività di organizzazione professionalmente.

Pertanto, tutte le società cooperative presentano in ogni caso una rischiosità residuale per quanto riguarda l'organizzazione di trasferte, viaggi di lavoro e viaggi premio a favore di dipendenti, collaboratori, clienti, fornitori, amministratori, soprattutto se verso particolari paesi esteri ecc.

Soggetto attivo	Chiunque (purchè disponga di una minima struttura organizzativa)
Condotta	Organizzare o anche solo propagandare viaggi finalizzati alla fruizione di attività di prostituzione minorile.
Elemento soggettivo	Dolo generico
Pena	Reclusione da 6 a 12 anni e multa da 15.493 a 154.937 euro.

Aree aziendali esposte a rischio:

- Gestione economico-finanziaria;
- Gestione trasferte, viaggi di lavoro, premi aziendali ecc;
- Partnership commerciali con aziende operanti nel settore turistico.

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 e delle aree aziendali a rischio;
- Diffusione di regolamenti, procedure e prassi aziendali inerenti la corretta gestione delle trasferte aziendali;
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di eventuali anomalie e/o sospette violazioni del Codice etico;
- Documentazione, archiviazione, tracciabilità delle trasferte lavorative svolte dal personale della cooperativa, specialmente in zone geografiche notoriamente esposte a tali rischi;
- In caso di cooperative che operano nel settore turistico (*tour operator*, agenzie di viaggio, agenzie specializzate nell'offerta di servizi *facility management* alle imprese per la gestione dei viaggi, incontri di lavoro ecc.), occorre prevedere un apposito sistema di controllo sulla gestione dei siti internet, dei veicoli pubblicitari, della registrazione degli utenti.

Art. 601 c.p. Tratta di persone.

Chiunque commette tratta di persona che si trova nelle condizioni di cui all'articolo 600 ovvero, al fine di commettere i delitti di cui al primo comma del medesimo articolo, la induce mediante inganno o la costringe mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno, è punito con la reclusione da otto a venti anni.

La pena è aumentata da un terzo alla metà se i delitti di cui al presente articolo sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Soggetto attivo	Chiunque
Condotta	1)Tratta di persone 2)induzione o costrizione al trasferimento, mediante violenza, minaccia o altre azioni intimidatorie
Elemento soggettivo	Dolo generico
Pena	Reclusione da 8 a 20 anni.

Aree aziendali esposte a rischio:

- Selezione, assunzione e gestione del personale, soprattutto se stagionale ed addetto ad attività lavorative tipicamente esposte a rischi di sfruttamento illecito (lavori socialmente utili, lavori stagionali ad esempio nel settore agricolo, assistenza anche domiciliare a malati ed anziani, settore edile, ecc.);
- Esecuzione contratti di appalto e subappalto.

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;
- Inserimento nello Statuto sociale e nel Codice Etico di principi di massima tutela della dignità e libertà della persona umana, nonché di principi esplicitamente finalizzati a vietare qualsiasi condotta di causazione o agevolazione di comportamenti che integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25 quinquies D.Lgs 231/2001;
- 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 e delle aree aziendali a rischio;
- Diffusione di regolamenti, procedure e prassi aziendali sulla corretta gestione delle attività di procacciamento della forza lavoro, gestione del personale, rispetto della normativa sul lavoro vigente, da diffondere eventualmente anche a partners e fornitori;
- Garanzia della corretta gestione dei rapporti sindacali, anche al fine di agevolare eventuali controlli su corretta applicazione normativa e contrattualistica in materia di lavoro all'interno della cooperativa;
- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di sospette violazioni del Codice etico o di eventuali anomalie/atipicità (es. assunzione personale minorenni).

Art. 602 c.p. Acquisto e alienazione di schiavi.

Chiunque, fuori dei casi indicati nell'articolo 601, acquista o aliena o cede una persona che si trova in una delle condizioni di cui all'articolo 600 è punito con la reclusione da otto a venti anni.

La pena è aumentata da un terzo alla metà se la persona offesa è minore degli anni diciotto ovvero se i fatti di cui al primo comma sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Soggetto attivo	Chiunque
Condotta	Acquisto alienazione, cessione persona in stato di schiavitù o servitù
Elemento soggettivo	Dolo generico
Pena	Reclusione da 8 a 20 anni.

Osservazioni

Entrambe le fattispecie relative al traffico di schiavi sono apparentemente di residuale rilevanza nel mondo cooperativo. In realtà i reati potrebbero essere celati in tutte le attività di reclutamento illegale di forza lavoro, purtroppo diffuse in realtà societarie in cui i lavoratori stagionali rappresentano una grossa percentuale del personale impiegato (si pensi alle cooperative agricole o alle cooperative di produzione lavoro). Inoltre, le ipotesi di reato sopra richiamate potrebbero essere imputate alla cooperativa a causa di comportamenti criminosi posti in essere da appaltatori, subappaltatori, partner, fornitori ecc.

Aree aziendali esposte a rischio:

- Selezione, assunzione e gestione del personale, soprattutto se stagionale ed addetto ad attività lavorative tipicamente esposte a rischi di sfruttamento illecito (lavori socialmente utili, lavori stagionali ad esempio nel settore agricolo, assistenza anche domiciliare a malati ed anziani, settore edile, ecc.);
- Esecuzione contratti di appalto e subappalto.

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;
- Inserimento nello Statuto sociale e nel Codice Etico di principi di massima tutela della dignità e libertà della persona umana, nonché di principi esplicitamente finalizzati a vietare qualsiasi condotta di causazione o agevolazione di comportamenti che integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25 quinquies D.Lgs 231/2001;
- 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 e delle aree aziendali a rischio;
- Diffusione di regolamenti, procedure e prassi aziendali sulla corretta gestione delle attività di procacciamento della forza lavoro, gestione del personale, rispetto della normativa sul lavoro vigente, da diffondere eventualmente anche a partners e fornitori;
- Garanzia della corretta gestione dei rapporti sindacali, anche al fine di agevolare eventuali controlli su corretta applicazione normativa e contrattualistica in materia di lavoro all'interno della cooperativa;

- Audit e/o incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di informative immediate in caso di riscontro di sospette violazioni del Codice etico o di eventuali anomalie/atipicità (es. assunzione personale minorenni).

ART. 25 SEXIES D.LGS. 231/2001 – ABUSI DI MERCATO.

In relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla parte V, titolo I-bis, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, si applica all'ente la sanzione pecuniaria da quattrocento a mille quote.

Se, in seguito alla commissione dei reati di cui al comma 1, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.

T.U.F., art.184. Abuso di informazioni privilegiate.

1. È punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;

c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

2. La stessa pena di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.

3. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

3-bis. Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numero 2), la sanzione penale è quella dell'ammenda fino a euro centotremila e duecentonovantuno e dell'arresto fino a tre anni.

4. Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'articolo 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'articolo 180, comma 1, lettera a).

T.U.F., art.185. Manipolazione del mercato.

1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.

2. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

2-bis. Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numero 2), la sanzione penale è quella dell'ammenda fino a euro centotremila e duecentonovantuno e dell'arresto fino a tre anni.

Osservazioni

Abuso di informazioni privilegiate (articolo 184 del d.lgs. 58/1998).

La fattispecie si realizza quando:

chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio; ovvero chiunque, essendo in possesso di informazioni privilegiate, a motivo della preparazione o esecuzione di attività delittuose:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;

c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

E' previsto un aggravamento della pena nel caso di rilevante offensività del fatto in ragione delle qualità personali del colpevole o dell'entità del prodotto o del profitto conseguito dal reato.

Manipolazione del mercato (articolo 185 del d.lgs. 58/1998).

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Anche in questo caso è previsto un aggravamento della pena nell'ipotesi di rilevante offensività del fatto in ragione delle qualità personali del colpevole o dell'entità del prodotto o del profitto conseguito dal reato.

Le due norme penali sanzionano le condotte di *insider trading* (abuso di informazioni privilegiate) e di truffa finanziaria (manipolazioni di mercato).

Condotta	Acquisto, vendita e qualsiasi altra operazione avente ad oggetto strumenti finanziari negoziati su mercati
----------	--

	<p>regolamentati, utilizzando informazioni privilegiate (<i>insider trading</i>);</p> <p>comunicazione di tali informazioni ad altri, al di fuori della normale attività lavorativa;</p> <p>raccomandazione o induzione di altri, sulla base delle informazioni privilegiate, ad effettuare operazioni sospette. (art.184).</p> <p>Sensibile alterazione del prezzo di strumenti finanziari mediante comportamenti truffaldini (operazioni simulate o altri artifici). (art.185)</p>
Elemento soggettivo	Dolo generico (coscienza e volontarietà della condotta).

Gli illeciti amministrativi richiamati dall'articolo 187-*quinquies* del d.lgs. 58/1998.

L'art. 187-*bis* e ss. del T.U. della finanza, introduce un sistema a “doppio binario” in base al quale alle sanzioni tipicamente penali comminate per la commissione dei reati di *market abuse*, si aggiungono specifiche sanzioni amministrative di natura pecuniaria, irrogate dalla Consob, per il caso in cui le pressoché medesime condotte realizzate o tentate colposamente, non configurino un reato, bensì un semplice illecito amministrativo (abuso di informazioni privilegiate - art. 187-*bis* T.U. della finanza e manipolazione del mercato – art. 187-*ter* T.U. della finanza).

Qualora tale illecito amministrativo sia stato commesso da persone riconducibili alle categorie dei “soggetti apicali” e dei “soggetti sottoposti all'altrui direzione o vigilanza”, nell'interesse o a vantaggio di una società, in base all'art. 187-*quinquies* del T.U. della finanza, tale società può essere, altresì, ritenuta responsabile del pagamento di una somma pari all'importo della sanzione amministrativa pecuniaria irrogata alla persona fisica autrice dell'illecito.

Abuso di informazioni privilegiate (articolo 187-bis del d.lgs. 58/1998).

La fattispecie si realizza quando chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio; ovvero chiunque, essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose; ovvero chiunque, in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse:

- a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi su strumenti finanziari utilizzando le informazioni medesime;
- b) comunica informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
- c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

E' previsto un aggravamento della pena in ragione delle qualità personali del colpevole ovvero dell'entità del prodotto o del profitto conseguito dall'illecito.

Manipolazione del mercato (articolo 187-ter del d.lgs. 58/1998).

La fattispecie si realizza quando chiunque: – tramite mezzi di informazione, compreso

INTERNET o ogni altro mezzo, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari; ovvero pone in essere:

a) operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari, salvo che dimostri di avere agito per motivi legittimi e in conformità alle prassi di mercato ammesse nel mercato interessato;

b) operazioni od ordini di compravendita che consentono, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale, salvo che dimostri di avere agito per motivi legittimi e in conformità alle prassi di mercato ammesse nel mercato interessato;

c) operazioni od ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno o di espediente;

d) altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

E' previsto un aggravamento della pena in ragione delle qualità personali del colpevole, dell'entità del prodotto o del profitto conseguito dall'illecito ovvero degli effetti prodotti sul mercato. Il Ministero dell'economia e delle finanze, sentita la CONSOB ovvero su proposta della medesima, può individuare, con proprio regolamento, le fattispecie, anche ulteriori rispetto a quelle sopra descritte, rilevanti ai fini dell'applicazione della disposizione in commento.

La CONSOB rende noti, con proprie disposizioni, gli elementi e le circostanze da prendere in considerazione per la valutazione dei comportamenti idonei a costituire manipolazioni di mercato (La CONSOB, con la Comunicazione n. DME/5078692 del 29 novembre 2005, ha fornito gli esempi di manipolazione del mercato e di operazioni sospette indicati dal *Committee of European Securities Regulators (CESR)* nel documento "*Market Abuse Directive. Level 3 - First set of Cesr guidance and information on the common operation of the Directive*").

Cause di non punibilità (art. 183 Decreto legislativo 58/1998)

L'art. 183 Decreto legislativo 58/1998 prevede due cause di non punibilità, che stabiliscono l'inapplicabilità delle disposizioni relative agli illeciti (penali e amministrativi) di abuso di informazioni privilegiate e manipolazione dei mercati:

1 art. 183 comma 1, lettera a): non applicabilità a operazioni attinenti alla politica monetaria, alla politica valutaria o alla gestione del debito pubblico compiute dallo Stato italiano, da uno Stato membro dell'Unione europea, dal Sistema europeo delle Banche centrali, da una Banca centrale di uno Stato membro dell'Unione europea o da qualsiasi altro ente ufficialmente designato ovvero da un soggetto che agisca per conto degli stessi.

2 art. 183 comma 1, lettera b): non applicabilità alle "negoziazioni di azioni, obbligazioni e altri strumenti finanziari propri quotati, effettuate nell'ambito di programmi di riacquisto da parte dell'emittente o di società controllate o collegate", o "operazioni di stabilizzazione di strumenti finanziari che rispettino le condizioni stabilite dalla Consob con regolamento".

Le situazioni scriminanti sono integrate soltanto se le negoziazioni e le operazioni indicate sono realizzate nel rispetto delle prescrizioni dell'autorità di vigilanza (il contenuto di tali prescrizioni è già configurato nel Regolamento (CE) n. 2273/2003, che ha introdotto precise condizioni tecniche (consistenti in limiti operativi e in adempimenti informativi)).

Le fattispecie in esame si riferiscono a reati che presuppongono, ai sensi dell'art. 180

del TUF l'emissione di strumenti finanziari di cui all'art. 1 comma 2, ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di un altro Paese dell'Unione europea. Non risulta allo stato che vi siano enti aderenti a Confcooperative, tra quelli cui sono applicabili le presenti Linee Guida, che abbiano emesso azioni o altri strumenti finanziari quotati in mercati regolamentati o che abbiano fatto richiesta in tale senso. Nè risulta che ciò sia mai avvenuto dalla data di nascita di Confcooperative. Pertanto, non si ritiene di procedere ad indicazione di aree rischio né di protocolli per il contenimento o eliminazione del rischio poiché questo ultimo risulta allo stato inesistente rispetto a queste fattispecie di reato. Ciò anche in considerazione del fatto che le Banche di Credito Cooperativo, pur aderenti a Confcooperative, non fanno riferimento alle presenti Linee Guida. Nel caso, in futuro, una associata, dovesse fare richiesta di emettere strumenti finanziari di cui all'art 180 TUF, si procederà ad aggiornamento della presente parte, quando se ne avrà notizia.

ART. 25 SEPTIES D.LGS. 231/2001 - OMICIDIO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO.

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

Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi.

Art. 589 c.p. Omicidio colposo commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.

Si applica la pena della reclusione da tre a dieci anni se il fatto e' commesso con violazione delle norme sulla disciplina della circolazione stradale da:

- 1) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni;***
- 2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope.***

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

Osservazioni

La condotta consiste nel cagionare la morte di un uomo per negligenza o imperizia o inosservanza delle leggi antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Soggetto attivo	Chiunque (reato comune)
Condotta	Cagionare la morte di una persona per negligenza o imperizia o inosservanza delle leggi antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Elemento soggettivo	Colpa
Pena	Reclusione da 2 a 5 anni.

Art. 590 c.p. Lesioni colpose gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

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

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto e' commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi e' della reclusione da sei mesi a due anni e la pena per le lesioni gravissime e' della reclusione da un anno e sei mesi a quattro anni.

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

Osservazioni

L'articolo in questione punisce chi, con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, cagiona ad altri una malattia, nel corpo o nella mente, grave o gravissima.

Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazione per un periodo

superiore ai quaranta giorni, oppure un indebolimento permanente di un senso o di un organo.

Per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente della favella, la deformazione o lo sfregio permanente del viso.

Soggetto attivo	Chiunque (reato comune)
Condotta	Cagionare ad una persona una malattia, nel corpo o nella mente, grave o gravissima, con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
Elemento soggettivo	Colpa
Pena	Reclusione da tre mesi a un anno o multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

Entrambe le norme sopra richiamate richiedono che l'evento lesivo sia conseguenza della violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.

Vengono a tale proposito in considerazione il D.lgs 81 del 2008 ed altre leggi speciali (es. DPR 27/04/1955 n. 547 sulla prevenzione degli infortuni; il DPR 19/03/1956 n. 303 sull'igiene sul lavoro; il D.lgs 14/08/1996 n. 494 in tema di sicurezza dei cantieri ecc.).

In funzione di chiusura si richiama l'art. 2087 c.c. che impone al datore di lavoro di adottare nell'esercizio dell'impresa le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie a tutelare l'integrità fisica e morale dei lavoratori.

Le sanzioni pecuniarie a carico delle aziende per questa tipologia di reati, determinate tramite il meccanismo delle quote, possono variare da un minimo di € 25.822,84 ad un massimo di € 1.549.370,69.

Non meno pesanti le sanzioni interdittive accessorie alla pena pecuniaria: interdizione all'esercizio dell'attività, sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrarre con la P.A., esclusione da agevolazioni, contributi o sussidi ed eventuale revoca di quelli ottenuti, divieto di pubblicizzare beni e servizi.

L'introduzione di tali fattispecie nel D.lgs 231/2001 ad opera della L. 123/2007 ha, dunque, un effetto estremamente rilevante, soprattutto in considerazione della natura colposa di detti illeciti.

Infatti, tutti gli adempimenti direttamente o indirettamente stabiliti dalla normativa vigente in materia di tutela della salute e sicurezza dei lavoratori (TU 81/2008 e non solo) possono rappresentare per le società cooperative un'area di rischio ai sensi dell'art. 25 septies D.lgs 231/2001.

La natura colposa dei reati *de quo* ha suscitato diverse discussioni interpretative in dottrina ed in giurisprudenza su due aspetti in particolare:

1) compatibilità fra la natura colposa dei reati ed i criteri di imputazione oggettiva ex art. 5 D.Lgs 231/2001 (commissione dei reati presupposto da parte di un dipendente ed esistenza di un interesse o vantaggio dell'ente);

2) compatibilità fra natura colposa dei reati e criterio di imputazione soggettiva dell'"elusione fraudolenta" del Modello.

1-a) Compatibilità fra la natura colposa dei reati ed i criteri di imputazione oggettiva ex art. 5 D.Lgs 231/2001: l'interesse o vantaggio per l'ente.

Il problema fondamentale sta nella apparente contrapposizione fra un interesse o vantaggio dell'ente (requisito necessario ex D.Lgs 231/2001) ed una non volizione dell'evento (requisito essenziale di tutti reati colposi).

Le interpretazioni proposte in dottrina e giurisprudenza sono state molteplici: alcuni, al fine di evitare un'*interpretatio abrogans*, hanno concentrato la ricerca dell'interesse o vantaggio nei reati colposi al solo elemento della condotta; altri ritengono che per i reati *de quo* sia necessario e sufficiente procedere alla individuazione del solo vantaggio oggettivo, identificato *ex post*; altri, infine, ritengono che l'interesse dell'ente vada ricercato nelle condotte colpose in via mediata, cioè non nel reato in sé, ma nella più generale attività all'interno della quale viene tenuta la condotta criminosa.

A prescindere dalla corrente interpretativa condivisa, occorre prendere atto che con l'avvento dei reati colposi all'interno del D.Lgs 231/2001, il concetto di interesse ex art. 5 ha assunto un significato prettamente oggettivo, spostato più sul momento della condotta che su quello dell'evento; pertanto, in caso di lesioni o omicidio conseguenti a violazione delle norme sulla salute e sicurezza sul lavoro, l'interesse potrà essere inteso ad esempio come oggettivo guadagno/risparmio in termini di costi, in una maggiore celerità del processo produttivo, o in una gestione del lavoro più semplice e snella, a seguito della mancata applicazione delle misure di sicurezza necessarie.

1-b) Compatibilità fra la natura colposa dei reati ed i criteri di imputazione oggettiva ex art. 5 D.Lgs 231/2001: i soggetti autori della condotta materiale.

Il D.Lgs 231/2001 richiede come ulteriore requisito per l'imputazione oggettiva del reato all'ente che la condotta materiale sia stata realizzata da una figura apicale o subordinata ai sensi del D.lgs 231/2001.

Tale requisito va conciliato con le previsioni di cui al TU 81/2008 e alle altre norme esistenti in materia, che individuano una pluralità di funzioni e figure gravate di specifici obblighi di sicurezza, nonché criteri di delegabilità di alcune di queste funzioni.

E' chiaro che ciascun soggetto, dipendente o collaboratore, che agisca all'interno delle proprie funzioni potrebbe far sorgere una responsabilità della società ex art. 25 septies D.Lgs 231/2001: ma la distribuzione dell'onere probatorio sarà diversa a seconda che il soggetto autore sia identificato come figura apicale o subordinata.

Ad esempio senz'altro il datore di lavoro e i dirigenti per la sicurezza sono identificabili come figure apicali dotate di autonomi poteri di rappresentanza, amministrazione o direzione dell'ente ex art. 5, comma 1, lett. a) D.Lgs 231/2001.

Al contrario preposti e dipendenti, e forse anche il RSPP ed il medico competente, sarebbero persone sottoposte all'altrui direzione o vigilanza ex art. 5, comma 1, lett. b) D.Lgs 231/2001, con la conseguenza che, ai fini della responsabilità dell'ente, occorrerà dimostrare la violazione degli obblighi di direzione e vigilanza.

Progettisti, fabbricanti, fornitori e installatori rientrano, invece, nell'una o nell'altra categoria a seconda della funzione concretamente svolta all'interno dell'ente dall'autore del reato presupposto.

Va ricordato, infine, che la giurisprudenza dominante in materia ritiene che i reati in questione possano essere imputati al datore di lavoro ed all'impresa ex D.Lgs 231/2001, anche qualora la persona offesa non sia un lavoratore dipendente ma un soggetto estraneo.

2) *Compatibilità fra natura colposa dei reati e criterio di imputazione soggettiva dell'elusione fraudolenta del Modello ex art. 6 D.Lgs 231/2001.*

L'art. 6 D.Lgs 231/2001 dispone che, in caso di commissione dell'illecito da parte di figure apicali, l'ente non risponde se prova di aver efficacemente adottato ed attuato un idoneo Modello organizzativo e che l'autore materiale della condotta ha eluso fraudolentemente tale Modello.

Proprio il concetto di "elusione fraudolenta" risulta *prima face* apparentemente inconciliabile con il concetto stesso di reato colposo.

In realtà, l'unico modo anche in questo caso per evitare di giungere ad un'*interpretatio abrogans* è quello di intendere la volontarietà dell'elusione fraudolenta come volontà di tenere una "condotta" non conforme alle procedure, istruzioni e disposizioni interne finalizzate alla prevenzione dei reati di omicidio e lesioni colpose ex art. 25 septies D.Lgs 231/2001. In questo modo la prova liberatoria per l'ente si ridurrebbe all'adozione ed efficace attuazione del Modello Organizzativo.

Su tale Modello Organizzativo, come noto, deve vigilare un organismo di controllo interno appositamente nominato. Tuttavia, occorre chiarire che l'Organismo di Vigilanza è un organo distinto rispetto al Servizio di Prevenzione e Protezione e rispetto alle figure soggettive previste nel D.Lgs 81/2008 (datore di lavoro, dirigenti, preposti, responsabile del servizio di prevenzione e protezione, addetti al servizio di prevenzione e protezione ecc.).

Il ruolo di vigilanza dell'O.d.V. resta parallelo alle funzioni attribuite dal D.Lgs 81/2008 ai soggetti sopra indicati e considerati "garanti" della salute e della sicurezza in azienda, *in primis* il datore di lavoro, i dirigenti ed i preposti.

L'O.d.V. vigila sulla corretta adozione ed attuazione del Modello 231 e dei Protocolli di prevenzione dei reati di omicidio e lesioni personali, in esso contenuti o richiamati; i "garanti" della salute e sicurezza in azienda vigilano e rispondono della corretta applicazione delle disposizioni e misure antinfortunistiche previste dal D.Lgs 81/2008 e da altra normativa di settore.

Si tratta di due livelli di controllo, che necessitano anche di competenze professionali e di esperienze diverse, destinati ad integrarsi ma mai a sovrapporsi.

L'O.d.V. può effettuare controlli sul rispetto ed applicazione dei requisiti normativi, senza entrare in valutazioni tecniche di competenza di altri soggetti.

L'O.d.V., pertanto, sarà chiamato a svolgere le seguenti attività di vigilanza:

a) verifiche periodiche sul rispetto dei protocolli previsti dal Modello 231 in materia di salute e sicurezza; tali verifiche potranno essere svolte direttamente da componenti dell'O.d.V. in possesso di specifiche competenze professionali, o, in mancanza di esse, potranno essere delegate ad altri soggetti appositamente incaricati;

- b) proposta di modifiche ai suddetti protocolli e alle altre misure preventive adottate in azienda, al verificarsi di violazioni significative delle norme e procedure in materia di salute e sicurezza sul lavoro, in caso di modifiche significative dell'organizzazione aziendale, e all'introduzione di modifiche legislative rilevanti;
- c) richiesta ed esame delle segnalazioni in merito a violazioni, anche presunte, del Modello;
- d) esame delle informazioni messe a disposizione dal Responsabile del Servizio di prevenzione e protezione, dal resto dei componenti del SPP e dagli altri soggetti individuati dalla normativa vigente in materia (es. reportistica periodica in materia di salute e sicurezza sul lavoro);
- e) proposta di applicazione di sanzioni in caso di violazioni alle procedure di sicurezza che si concretizzino al tempo stesso come violazioni del Modello organizzativo e del Codice Etico.

Per quanto riguarda l'individuazione delle **aree aziendali** maggiormente **esposte al rischio** di commissione dei reati *de quo*, non è possibile procedere ad un'elencazione che risulterebbe di per sé non esaustiva: infatti, le condotte punite dall'art. 25 septies D.Lgs 231/2001 possono essere astrattamente ascrivibili a qualsiasi attività, funzione, processo aziendale. A tale proposito, in sede di mappatura delle aree a rischio sarà importante individuare in modo specifico le funzioni, attività o aree aziendali in cui sono ipotizzabili (anche per ragioni di storicità) condotte o fatti pregiudizievoli.

In relazione ai **protocolli di contenimento/eliminazione del rischio** sarà prima di tutto essenziale procedere ad un'attenta integrazione fra il Modello Organizzativo ed il "sistema di sicurezza aziendale", costituito da tutti quegli adempimenti cogenti e volontari finalizzati ad una corretta gestione della salute e sicurezza sui luoghi di lavoro, e più in particolare finalizzati a garantire:

- il rispetto degli *standards* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- un'adeguata valutazione dei rischi e la predisposizione delle misure di prevenzione e protezione conseguenti;
- la realizzazione di tutte le attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- la sorveglianza sanitaria;
- le attività di informazione e formazione dei lavoratori;
- la vigilanza continua sul rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge;
- le verifiche periodiche sull'efficacia e l'applicazione delle procedure;
- la registrazione di tutti gli adempimenti sopra elencati.

A tali adempimenti si aggiungono poi, alcuni protocolli più generali, quali:

- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio da parte dei destinatari;

- Diffusione e accettazione del Codice Etico, del Modello 231 e del sistema sanzionatorio anche da parte di *partners*, agenti, fornitori, controparti contrattuali, collaboratori, soggetti terzi con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- 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);
- Articolazione di funzioni adeguata a natura, dimensioni e attività gestite dall'ente, ed in ogni caso adeguata ad assicurare le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- Identificazione di figure aziendali deputate alla gestione degli adempimenti inerenti la sicurezza nell'ambito di contratti di appalto, pubblici e non; si rammenta che l'eventuale applicazione di una sanzione interdittiva ex art. 9, comma 2, lett. c D.Lgs 231/2001 a carico di un ente costituisce senz'altro una delle cause di esclusione dalla "partecipazione alle procedure di affidamento delle concessioni e degli appalti di lavori, forniture e servizi" a norma dell'art. 38 D.Lgs 163/2006);
- Pubblicizzazione di specifico organigramma della sicurezza e di eventuale mansionario allegato;
- Identificazione di una funzione dedicata all'aggiornamento e alla diffusione della normativa antinfortunistica e di igiene e salute sul lavoro;
- Documentazione, archiviazione e tracciabilità degli atti e delle operazioni inerenti investimenti in materia di sicurezza;
- Previsione di un canale comunicativo specifico con l'O.d.V. e trasmissione a quest'ultimo di relazioni periodiche, reportistica periodica e segnalazioni inerenti eventuali violazioni di legge e del Codice Etico in materia di sicurezza;
- Previsione di momenti formativi specifici sul Modello 231 e sulle sue applicazioni in materia antinfortunistica;
- Analisi dettagliata della casistica di infortuni sul lavoro, malattie professionali e mancati infortuni condotta per ciascuna unità produttiva e per mansioni; indagine sulle probabili cause; esame di eventuali prescrizioni impartite dalle autorità competenti (es. ASL) ed indagine sulla capacità di tali prescrizioni di prevenire determinati infortuni/malattie/incidenti; confronto fra i risultati dell'analisi effettuata e quanto riportato nel Documento di valutazione dei rischi onde valutarne l'effettivo aggiornamento e congruità con la realtà aziendale.
- Incontri periodici e/o *audit* fra O.d.V. e funzioni aziendali esposte al rischio *de quo*, anche delegando le attività di verifica a specifiche figure professionalmente competenti (RSPP, preposti, consulenti esterni ecc.);
- Previsione nel Modello organizzativo di un adeguato sistema di controllo sull'attuazione del Modello stesso e sulla sua idoneità nel corso del tempo; intervento tempestivo dell'O.d.V., insieme alle funzioni aziendali competenti, per i necessari aggiornamenti al Modello.

Occorre ricordare inoltre quanto dispone l'art. 30 del D.Lgs 81/2008 nell'ipotesi in cui una cooperativa abbia effettivamente attuato, ed eventualmente certificato, un Sistema di gestione della sicurezza sul lavoro conforme alle Linee Guida UNI-INAIL e/o al Brithis Standard OHSAS 18001:2007: *“i Modelli di Organizzazione aziendale definiti conformemente alle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al Brithis Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti”*.

Ai sensi dell'art. 30 D.Lgs 81/2008, dunque, laddove l'ente abbia adottato ed efficacemente attuato un modello di organizzazione conforme ai requisiti di cui all'art. 6 del D.Lgs. n. 231/2001 e all'art. 30 del D.Lgs. n. 81/2008, oltre alla potenziale efficacia esimente della responsabilità amministrativo-penale per i reati presupposto dettati in materia di sicurezza sul lavoro (art. 25-*septies*, D.Lgs. n. 231/2001), si configurerà anche la presunzione (relativa) di adempimento da parte del datore di lavoro dell'obbligo di vigilanza nei confronti del soggetto da egli delegato (art. 16 comma 3 D.Lgs 81/2008).

ART. 25 OCTIES D.LGS. 231/2001 - RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA.

In relazione ai reati di cui agli articoli 648, 648-bis e 648-ter del codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote.

Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore a due anni.

Art. 648 c.p. Ricettazione.

Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.

La pena è della reclusione sino a sei anni e della multa sino a euro 516, se il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Art.648bis c.p. Riciclaggio.

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.

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

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.

Art.648ter c.p. Impiego di denaro, beni o utilità di provenienza illecita.

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.

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

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

Si applica l'ultimo comma dell'articolo 648.

Osservazioni

Le tre figure delittuose in commento sono tra loro in rapporto di specialità (l'art.648^{ter} rispetto al 648^{bis}, e quest'ultimo rispetto al 648).

In particolare, il riciclaggio si differenzia dalla ricettazione sia quanto all'elemento oggettivo (alla condotta di acquisto o ricezione si aggiunge il compimento di atti diretti ad ostacolare l'identificazione della provenienza criminale), sia quanto all'elemento soggettivo (è sufficiente il dolo generico laddove nella ricettazione è richiesto l'intento specifico del conseguimento d'un profitto).

La fattispecie di cui all'art.648^{ter}, a sua volta, si distingue dal riciclaggio non tanto per il carattere delle attività "economiche o finanziarie" in essa contemplate (susceptibili di essere pure ricomprese nel termine *operazioni* di cui all'art. 648^{bis}), quanto per il fatto che mentre il riciclaggio si pone in immediata continuità cronologica col reato presupposto, l'impiego di proventi illeciti va invece a collocarsi in un momento successivo e ulteriore, ad opera di un soggetto diverso dal primo riciclatore, soggetto il quale reimpiega beni o denaro già riciclati ma di persistente provenienza illecita.

E' esclusa, nell'ordinamento italiano, la punibilità dell'autoriciclaggio, vale a dire l'impiego, la sostituzione od il trasferimento di beni o denaro commessi dal medesimo autore del reato presupposto (tanto si deduce dalla clausola d'esclusione presente nell'*incipit* delle disposizioni in commento: «fuori dai casi di concorso nel reato»). Quanto ora detto non vale, tuttavia, ai fini della disciplina speciale di cui al D.Lgs. n. 231/2007 (su cui v. *infra*).

Si badi che autore del reato è anche il concorrente, cioè colui il quale fornisce un contributo determinante, fattuale o psicologico, alla commissione del delitto, al momento della consumazione di questo o in epoca precedente.

Sia la ricettazione, che il riciclaggio e l'impiego di proventi illeciti sono compatibili con lo stato soggettivo di dolo eventuale (commissione del fatto nonostante il dubbio sulla provenienza illecita dei beni o del denaro).

Aree a rischio:

- Amministrazione e Finanza;
- Gestione gare e appalti;
- Sistemi Informativi;
- Accordi commerciali con clienti e fornitori;
- Gestione omaggi e sponsorizzazioni;

- Gestione operazioni di investimento, acquisizione societaria, creazione società di scopo, creazione *joint-ventures*.

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;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Previsione di una procedura per la gestione delle risorse finanziarie con distribuzione di compiti e responsabilità (segregazione dei compiti);
- Tracciabilità e controllo formale e sostanziale dei flussi finanziari in entrata (controlli controparte, istituti credito utilizzati, eventuali schermi societari o società fiduciarie utilizzate, etc);
- Previsione di una procedura per la gestione degli acquisti ed in particolare per la selezione dei fornitori e controlli formali e sostanziali dei pagamenti;
- Tracciabilità degli accordi con *partners* e fornitori;
- Previsione di specifiche clausole per terzi/agenti per il rispetto del Codice etico e Modello;
- Formazione periodica sui reati di ricettazione e riciclaggio e sulle procedure aziendali in essere;
- Segnalazione operazioni anomale o ad alto indice di rischio all'O.d.V.;
- Verifiche sull'affidabilità commerciale e professionale dei fornitori, degli altri *partners* commerciali/finanziari e dei clienti sulla base di alcuni indici rilevanti (es. protesti, procedure concorsuali, entità del prezzo sproporzionata rispetto ai normali valori di mercato ecc);
- Verifica della regolarità dei pagamenti, in relazione alla piena coincidenza tra destinatari dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- Previsione di controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi ed ai pagamenti/operazioni infragruppo o all'interno di reti consortili, tramite modalità non tracciate. Tali controlli devono aver riguardo alla sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun paese) e ad eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.

Normativa antiriciclaggio ex D.Lgs. 21 novembre 2007, n. 231

Il 29 dicembre 2007 è entrato in vigore il Decreto Legislativo n. 231/2007, recante “Attuazione 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”.

Destinatari degli obblighi antiriciclaggio

La disciplina introdotta prevede una serie di obblighi in capo a:

- intermediari finanziari ed altri soggetti esercenti attività finanziaria;
- professionisti;
- altri soggetti esercenti attività subordinate al possesso di licenze, autorizzazioni, iscrizioni in albi o registri.

Con riguardo ai professionisti, i soggetti destinatari della disciplina risultano essere (artt. 12 e 13):

- soggetti iscritti nell'albo dei dottori commercialisti e degli esperti contabili e nell'albo dei consulenti del lavoro;
- ogni altro soggetto che rende i servizi forniti da periti, consulenti e altri soggetti che svolgono in maniera professionale, anche nei confronti dei propri associati o iscritti, attività in materia di contabilità e tributi, ivi compresi associazioni di categoria di imprenditori e commercianti, CAF e patronati;
- notai ed avvocati;
- prestatori di servizi relativi a società o trust, che già non rientrino nelle precedenti categorie;
- società di revisione iscritte all'albo speciale previsto dall'art.161 del TUF;
- soggetti iscritti nel registro dei revisori contabili.

I centri servizi di assistenza contabile, fiscale e di elaborazione dati di Confcooperative operanti ai sensi del D.lgs. n. 241 del 1997 e quelli convenzionanti con questi ultimi e promossi da articolazioni territoriali di Confcooperative ai sensi dell'articolo 11 del D.M. n. 164 del 1999 e che operano a favore degli enti aderenti alle stesse, rientrano nella seconda categoria, e sono pertanto soggetti agli obblighi antiriciclaggio di cui al D.Lgs. n. 231 /2007 ed alle procedure e protocolli di seguito descritti.

Gli obblighi

La normativa antiriciclaggio è imperniata su tre obblighi gravanti sui suoi destinatari; essi sono:

- obbligo di adeguata verifica della clientela (artt. 15 ss.);
- obbligo di registrazione (artt. 36 ss.);
- obbligo di segnalazione delle operazioni sospette (artt. 41 ss.).

L'obbligo di adeguata verifica della clientela si sostanzia, oltre che nell'accertamento dell'identità del soggetto che richiede la prestazione, in un dovere di *informarsi* sulla natura e sullo scopo della prestazione richiesta e in un dovere di *monitoraggio costante* nel corso dell'esecuzione della prestazione stessa o dell'eventuale rapporto continuativo.

L'obbligo in parola sussiste (art.16, d.lgs. n.231/2007):

- quando la prestazione professionale richiesta ha ad oggetto mezzi di pagamento, beni od utilità di valore pari o superiore a 15.000 euro;
- quando vengano eseguite prestazioni professionali occasionali che comportino la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che siano effettuate con un'operazione unica o con più operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata;³
- tutte le volte che l'operazione sia dia valore indeterminato o non determinabile;⁴
- quando vi è sospetto di riciclaggio, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un cliente.

Ai fini dell'assolvimento dell'obbligo il destinatario della disciplina deve (art.18):

- identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- identificare l'eventuale titolare effettivo e verificarne l'identità;
- *ottenere informazioni sullo scopo e sulla natura prevista del rapporto continuativo o della prestazione professionale;*
- *svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale.*

Come si vede, il D.Lgs. n. 231/2007 ha introdotto un adempimento obbligatorio alquanto pregnante caratterizzato, oltre che dall'accertamento dell'identità del soggetto che richiede una data prestazione, da un *dovere di informarsi* sulla natura e sullo scopo della prestazione richiesta e da un *dovere di monitoraggio costante* nel corso dell'esecuzione della prestazione stessa o dell'eventuale rapporto continuativo.

L'adempimento dell'obbligo di adeguata verifica deve avvenire secondo le seguenti modalità (art. 19):

3

Il d.lgs. n.231/2007 (art.1, co.2, lett.m)) definisce l' "**operazione frazionata**" come l'operazione unitaria sotto il profilo economico, di valore pari o superiore ai limiti stabiliti dal decreto, posta in essere attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi ed in un circoscritto periodo di tempo fissato in sette giorni ferma restando la sussistenza dell'operazione frazionata quando ricorrano elementi per ritenerla tale.

Il *collegamento* tra le operazioni assume pertanto rilievo al fine di stabilire l'esistenza di un'operazione in realtà unitaria ma artificialmente frazionata onde restare al di sotto delle soglie antiriciclaggio.

4 Ai fini dell'obbligo di adeguata verifica della clientela, la costituzione, gestione o amministrazione di società, enti, trust o soggetti giuridici analoghi integra in ogni caso un'operazione di valore non determinabile.

- *Identificazione del cliente*

L'identificazione e la verifica dell'identità del cliente e del titolare effettivo è svolta mediante un documento di identità non scaduto.

Qualora il cliente sia una società o un ente occorre verificare l'effettiva esistenza del potere di rappresentanza e vanno acquisite le informazioni necessarie per individuare e verificare l'identità dei relativi rappresentanti delegati alla firma per l'operazione richiesta.

- *Identificazione e verifica del titolare effettivo*

Per "titolare effettivo" deve intendersi la persona fisica per conto della quale è realizzata un'operazione o un'attività, ovvero, nel caso di entità giuridica, la persona o le persone fisiche che, in ultima istanza, possiedono o controllano tale entità, ovvero ne risultano beneficiari secondo i criteri stabiliti nell'allegato tecnico al D.Lgs. n. 231/2007.⁵ (art.1, c.1, lett. u)).

L'identificazione e la verifica del titolare effettivo è effettuata contestualmente all'identificazione del cliente e, per le persone giuridiche, è diretta alla comprensione della struttura proprietaria e di controllo dell'ente.

A fini pratici, si consiglia di chiedere una dichiarazione scritta da parte del cliente, dichiarazione scritta che egli ha l'obbligo di rendere sotto la propria responsabilità: ai sensi dell'art.55, c.2 del decreto, il cliente che omette di indicare le generalità del soggetto per conto del quale egli eventualmente opera o le indica false è punito con pena detentiva e pecuniaria.

A prescindere dall'atteggiamento collaborativo o meno del cliente, tuttavia, il destinatario della disciplina antiriciclaggio è comunque tenuto a procedere ad autonoma verifica delle informazioni ricevute; il decreto enuncia, a titolo esemplificativo e non tassativo, alcune modalità per il compimento di tale verifica, tra cui, *in primis*, il ricorso a pubblici registri (si pensi al registro delle imprese), elenchi, atti o documenti pubblici.

- *Controllo costante (customer due diligence)*

Il controllo costante nel corso del rapporto continuativo o della prestazione professionale si attua analizzando le transazioni concluse durante tutta la durata di tale rapporto al fine di verificarne la compatibilità con il profilo del cliente,

5 Per titolare effettivo s'intende:

a) in caso di società:

1) la persona fisica o le persone fisiche che, in ultima istanza, possiedono o controllino un'entità giuridica, attraverso il possesso o il controllo diretto o indiretto di una percentuale sufficiente delle partecipazioni al capitale sociale o dei diritti di voto in seno a tale entità giuridica, anche tramite azioni al portatore, purché non si tratti di una società ammessa alla quotazione su un mercato regolamentato e sottoposta a obblighi di comunicazione conformi alla normativa comunitaria o a standard internazionali equivalenti; tale criterio si ritiene soddisfatto ove la percentuale corrisponda al 25 per cento più uno di partecipazione al capitale sociale;

2) la persona fisica o le persone fisiche che esercitano in altro modo il controllo sulla direzione di un'entità giuridica;

b) in caso di entità giuridiche quali le fondazioni e di istituti giuridici quali i trust, che amministrano e distribuiscono fondi:

1) se i futuri beneficiari sono già stati determinati, la persona fisica o le persone fisiche beneficiarie del 25 per cento o più del patrimonio di un'entità giuridica;

2) se le persone che beneficiano dell'entità giuridica non sono ancora state determinate, la categoria di persone nel cui interesse principale è istituita o agisce l'entità giuridica;

3) la persona fisica o le persone fisiche che esercitano un controllo sul 25 per cento o più del patrimonio di un'entità giuridica.

avendo riguardo all'origine dei fondi e tenendo aggiornati documenti, dati e informazioni possedute.

Si consiglia di chiedere una dichiarazione scritta al cliente con assunzione da parte di costui dell'obbligo di comunicare tempestivamente ogni variazione dei dati precedentemente forniti.

Si consiglia altresì di programmare la verifica e/o l'aggiornamento delle informazioni possedute in corrispondenza di eventi rilevanti (scadenza documenti identificativi, rinnovo delle cariche sociali, etc...).

Il cliente, inteso come colui che entra in contatto con il professionista, ha comunque l'obbligo di fornire tutte le informazioni necessarie e *aggiornate* per consentire al professionista stesso di adempiere agli obblighi di adeguata verifica (art.21).

Ai sensi dell'art.55, c.1 del decreto, il cliente che non fornisce informazioni sullo scopo e natura della prestazione richiesta o le fornisce false, è punito con l'arresto da sei mesi a tre anni e con la multa da 5.000 a 50.000 euro.

Obbligo di astensione

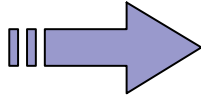
Qualora non sia possibile procedere nei modi anzidetti alla verifica della clientela, il professionista è tenuto ad astenersi dall'instaurare il rapporto continuativo o dall'eseguire la prestazione professionale ovvero a porre fine ai rapporti già in essere, valutando al contempo se effettuare la segnalazione del cliente interessato.

Analogo obbligo di astensione sussiste in tutti i casi in cui la prestazione richiesta o il rapporto già in essere veda coinvolte, direttamente o indirettamente, società fiduciarie, trust, società anonime o controllate mediante azioni al portatore aventi sede nei Paesi facenti parte della *black list* individuata dal Ministero dell'economia e delle finanze alla stregua dell'art.28, co.7**bis** del decreto. Indipendentemente dalla denominazione delle entità giuridiche coinvolte ed aventi sede in tali Paesi, il destinatario della disciplina anticiclaggio deve astenersi dal procedere ogniqualvolta non sia comunque possibile identificare il titolare effettivo di tali entità e verificarne l'identità (art. 28, co. 7**ter**).

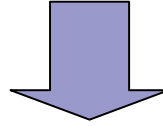
Approccio basato sul rischio

«Gli obblighi di adeguata verifica della clientela sono assolti commisurandoli al rischio associato al tipo di cliente, rapporto continuativo, prestazione professionale, operazione, prodotto o transazione di cui trattasi».

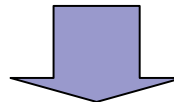
I destinatari della normativa *«devono essere in grado di dimostrare che la portata delle misure adottate è adeguata all'entità del rischio di riciclaggio».*



E' richiesto in sostanza uno *screening* della clientela volto a determinare per ciascun cliente il rischio di collegamenti con operazioni di riciclaggio.



All'esito di tale *screening*, a ciascun cliente andrà associato un profilo di rischio riciclaggio (basso, medio, alto) in funzione del quale calibrare l'adempimento degli obblighi.



Con l'aumentare del rischio, le verifiche sul cliente, sull'eventuale titolare effettivo e sulla natura-scopo dell'operazione richiesta si faranno più rigorose (es: ricorso a documentazione ulteriore, richiesta di contatto diretto con il titolare effettivo, valutazioni più rigorose da parte del professionista)

**Aumento del
rischio**



Con l'aumentare del rischio, il controllo costante andrà effettuato a intervalli viepiù ravvicinati e frequenti (es: non attendere la comunicazione da parte del cliente di eventi modificativi della situazione giuridica, quale in ipotesi il mutamento dell'assetto proprietario di un ente, ma accertare autonomamente il verificarsi di tali eventi secondo una tempistica prefissata, ad esempio mediante il ricorso periodico a visure camerali aggiornate).

L'obbligo di registrazione.

I documenti e le informazioni adoperate per l'assolvimento dell'obbligo di adeguata verifica della clientela debbono essere conservati e registrati per un periodo di dieci anni (art.36).

Costituiscono oggetto di registrazione e conservazione, in particolare:

- 1) con riferimento ai rapporti continuativi ed alla prestazione professionale: la data di instaurazione, i dati identificativi del cliente e del titolare effettivo, unitamente alle generalità dei delegati a operare per conto del titolare del rapporto ed il codice del rapporto ove previsto;
- 2) con riferimento a tutte le operazioni di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che si tratti di un'operazione unica o di più

operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata: la data, la causale, l'importo, la tipologia dell'operazione, i mezzi di pagamento ed i dati identificativi del soggetto che effettua l'operazione e del soggetto per conto del quale eventualmente opera.

Tempistica

La registrazione delle informazioni *de quo* deve essere tempestiva e, comunque, deve avvenire non oltre il trentesimo giorno successivo al compimento dell'operazione ovvero all'apertura, alla variazione e alla chiusura del rapporto continuativo ovvero all'accettazione dell'incarico professionale, all'eventuale conoscenza successiva di ulteriori informazioni, o al termine della prestazione professionale.

Modalità di registrazione per i professionisti

A differenza degli altri destinatari della disciplina (quali, *in primis*, gli intermediari finanziari) i professionisti e i soggetti assimilati possono optare per la tenuta dell'archivio unico antiriciclaggio sia in forma informatica che in forma cartacea.

Nel secondo caso essi dovranno istituire il *registro della clientela a fini antiriciclaggio*, numerato progressivamente e siglato in ogni pagina, con indicazione finale del numero di pagine e firma del soggetto obbligato.

Nel *registro* dovranno essere registrati i dati identificativi del cliente, nel mentre la documentazione e gli ulteriori dati e informazioni dovranno essere conservati nel fascicolo relativo a ciascun cliente.

Esenzioni dagli obblighi di adeguata verifica e di registrazione.

L'articolo 12, c.3 del Decreto stabilisce due esenzioni dagli obblighi di adeguata verifica della clientela e dagli obblighi di registrazione, entrambe rilevanti per i Centri Servizi; gli obblighi in parola non si applicano:

- 1) **allo svolgimento della mera attività di redazione e/o di trasmissione delle dichiarazioni derivanti da obblighi fiscali.**
- 2) **agli adempimenti in materia di amministrazione del personale di cui all'articolo 2, c.1., della legge 11 gennaio 1979, n.12.**

I Centri Servizi aderenti a Confcooperative, pertanto, sono esonerati dagli adempimenti antiriciclaggio per quel che concerne tutti gli incarichi relativi a paghe e contributi previdenziali ed assistenziali, ad eccezione dell'obbligo di segnalazione di operazioni comunque sospette.

Le esenzioni hanno **carattere tassativo**: qualunque attività (ad es. consulenze) che esuli dal loro campo di applicazione resta soggetta agli obblighi antiriciclaggio.

L'obbligo di segnalazione.

Pilastro di tutta la normativa antiriciclaggio, sia vecchia che nuova, è l'obbligo di segnalazione delle operazioni sospette.

Nuovo destinatario delle segnalazioni è l'UIF (Unità di informazione finanziaria), istituito presso la Banca d'Italia.

Ai sensi dell'art.41 del d.lgs. n.231/2007, i soggetti destinatari della disciplina antiriciclaggio *inviando alla UIF una segnalazione di operazione sospetta quando fanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo.*

Tre sono dunque gli stati soggettivi che debbono indurre l'operatore alla segnalazione:

- la conoscenza del compimento o del tentativo di compimento di attività di riciclaggio;
- il semplice sospetto;
- l'esistenza di motivi ragionevoli per sospettare.

A questi presupposti, tuttavia, ancorchè non contemplati dalla norma, vanno aggiunti la diligenza, la razionalità e la buona fede.

La valutazione dell'operatore, alla stregua dell'art.41, comma 1, dev'essere fondata sui seguenti parametri:

- caratteristiche, entità e natura dell'operazione richiesta;
- ogni circostanza conosciuta in ragione delle funzioni o dell'attività esercitata;
- capacità economica e attività svolta dal cliente o dal titolare effettivo;
- ogni altro elemento a disposizione del segnalante, acquisito nell'ambito dell'attività svolta o a seguito del conferimento dell'incarico.

Come si vede, trattasi di parametri omnicomprensivi, riferibili ad una conoscenza diretta del cliente ovvero ricavabile *aliunde* rispetto al rapporto professionale.

Un indice specifico di operazione sospetta, espressamente introdotto nel testo del decreto dal D.L. n. 78/2010 (art.36), è quello concernente l'uso frequente o ingiustificato del contante.

“E' un elemento di sospetto il ricorso frequente o ingiustificato a operazioni in contante, anche se non in violazione dei limiti di cui all'articolo 49, e, in particolare, il prelievo o il versamento in contante con intermediari finanziari di importo pari o superiore a 15.000 euro” (D.Lgs. n. 231/2007, art. 41, co.1, ult. periodo).

Tempistica e modalità delle segnalazioni

Le segnalazioni devono essere effettuate senza ritardo, ove possibile prima di eseguire l'operazione, appena il soggetto obbligato viene a conoscenza degli elementi di sospetto.

Come per il passato, l'obbligo di segnalazione sussiste a prescindere dal valore della prestazione, non essendo ancorato ad alcuna soglia.

Obbligo di astensione

Ai sensi dell'art.41, comma 5 d.lgs. n.231/2007:

i soggetti tenuti all'obbligo di segnalazione si astengono dal compiere l'operazione finchè non hanno effettuato la segnalazione, tranne che detta astensione non sia possibile tenuto conto della normale operatività, o possa ostacolare le indagini.

Ancorché esclusi dagli obblighi di adeguata verifica e di registrazione, sono invece soggetti all'obbligo di segnalazione, al ricorrere dei presupposti, anche gli adempimenti in materia di amministrazione del personale e l'attività di redazione e trasmissione delle dichiarazioni fiscali.

E' il caso, ad esempio, del Centro Servizi che da un anno all'altro constati che il proprio cliente ha notevolmente ed inspiegabilmente aumentato il reddito dichiarato.

Riciclaggio, autoriciclaggio e concorso nel reato

E' necessario, a questo punto, evidenziare una circostanza fondamentale.

Il D.Lgs. n.231/2007, all'art.2, contiene una definizione del reato di riciclaggio autonoma e distinta rispetto a quella contenuta nel codice penale.

Costituiscono riciclaggio, se commesse intenzionalmente:

- **la conversione o il trasferimento di beni, essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;**
- **l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;**
- **l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;**
- **la partecipazione ad uno degli atti di cui ai numeri precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione.**

Come si vede, trattati di una definizione del reato *sui generis*, valevole ai soli fini del D.Lgs. n.231/2007, e comprendente, a ben vedere, ipotesi delittuose distinte anche se affini o complementari rispetto al classico reato di riciclaggio contemplato dall'art.648bis c.p.; in particolare: il favoreggiamento personale, la ricettazione, l'associazione a delinquere, l'istigazione a delinquere.

Nella definizione autonoma del riciclaggio contenuta nel decreto risalta l'assenza della clausola sul concorso viceversa contenuta nel codice penale: "*Fuori dei casi di concorso nel reato*".

Ciò introduce, ai soli fini del decreto, l'ipotesi delittuosa di autoriciclaggio.

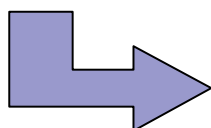


Circ. n. 1/2008

**Guardia di
Finanza**

Per l'estensione dell'obbligo di segnalazione di operazioni sospette anche all'autoriciclaggio, argomentando dall'assenza dell'inciso "*fuori dai casi di concorso*", si è espresso altresì il Com. Generale della Guardia di Finanza.

Il reato di autoriciclaggio comunque, a quanto risulta, dovrebbe presto trovare ingresso anche nel codice penale.



Alla luce di ciò, le operazioni sospette andranno segnalate anche allorché il richiedente coincida con l'autore o il coautore del reato base, proprio perchè, per il decreto, l'autoriciclaggio è riciclaggio, nel mentre, ad oggi, esso non lo è per il codice penale, alla cui stregua le operazioni compiute dall'autore di un crimine sui suoi proventi restano in esso assorbite.

Concorso

Sempre ai sensi del decreto, costituisce altresì riciclaggio il fatto di aiutare o consigliare qualcuno, intenzionalmente, a porre in essere operazioni di riciclaggio ovvero il fatto di agevolare l'esecuzione.

La posizione del professionista e dei soggetti assimilati si fa qui molto delicata.

Il compimento di un'operazione sospetta senza rispetto degli obblighi di astensione e di segnalazione, ben oltre il semplice inadempimento agli obblighi del decreto, rischia di configurare un'ipotesi di concorso nel reato di riciclaggio.

La sussistenza di elementi oggettivi idonei a generare il sospetto, ed il compimento dell'operazione da parte del professionista *tamquam non esset*, rischia di costargli molto caro, nella specie un'imputazione penale per concorso in riciclaggio, e ciò, si badi bene, sia che il professionista fosse certo della provenienza illecita dei beni e ciò nonostante abbia compiuto la prestazione richiestagli (stato soggettivo intenzionale di dolo), sia che semplicemente sospettasse, pur non essendone certo, e ciò nonostante abbia agito (stato soggettivo di dolo eventuale).

Obblighi dell'Organismo di Vigilanza e Responsabile Antiriciclaggio

Ai sensi dell'articolo 52 del D.Lgs. n.231/2007, l'Organismo di Vigilanza, così come gli altri Organi di controllo dei destinatari della normativa diversi dalle persone fisiche (ciascuno nell'ambito delle proprie attribuzioni e competenze), ha, in primo luogo, un generale dovere di vigilanza sul rispetto degli obblighi antiriciclaggio.

Sull'O.d.V. incombono, altresì, i seguenti *obblighi specifici*:

- obbligo di comunicare al legale rappresentante dell'ente o a un suo delegato, senza ritardo, eventuali infrazioni degli obblighi di segnalazione, di cui abbia notizia;
- obbligo di comunicare all'Autorità di vigilanza di settore, entro trenta giorni, eventuali infrazioni agli obblighi di registrazione, di cui abbia notizia;
- *obbligo di comunicare al MEF, entro trenta giorni, eventuali infrazioni alle norme sull'uso del contante o di titoli al portatore, di cui abbia notizia.*

Si tenga presente che l'omissione delle comunicazioni prescritte dall'art.52 da parte degli organi di vigilanza e controllo delle società o enti destinatari del decreto è punita con la reclusione fino a un anno e con la multa da 100 a 1.000 euro.

In caso di O.d.V. collegiale, così come per il Collegio Sindacale, parte degli studiosi ritiene che possa avere efficacia esimente per il singolo componente (o il singolo Sindaco) l'eventuale annotazione a verbale del proprio dissenso rispetto alla delibera collegiale di non procedere a comunicazione. Ciò è a dire il vero dubbio: i doveri di comunicazione incombono sia sull'O.d.V. (o sul Collegio Sindacale) quale organo, sia sui singoli sindaci *uti singuli*. Quantunque, pertanto, l'Organismo stabilisca di non intervenire, il singolo componente potrebbe comunque essere tenuto a procedere, da solo, alle comunicazioni prescritte.

Si suggerisce agli aderenti alla Confederazione tenuti al rispetto della normativa antiriciclaggio di valutare, compatibilmente alle dimensioni e alla struttura organizzativa degli enti coinvolti, secondo i principi più volte espressi, la nomina di un soggetto responsabile (cd. *compliance officer*) cui affidare la cura e la conservazione di tutta la documentazione inerente (in primis, il registro della clientela o l'archivio informatico).

Tale figura sarà poi soggetta ad un obbligo di relazione costante nei confronti dell'Organismo di Vigilanza, nel corso di riunioni periodiche volte altresì a fare il punto sul rispetto della normativa e su eventuali ipotesi di miglioramento del sistema di *compliance* interno.

Sempre al Responsabile Antiriciclaggio dovrebbe essere assegnata la predisposizione di un adeguato programma di formazione rivolto al personale del Centro Servizi e

finalizzato alla corretta applicazione delle disposizioni in materia da parte dei singoli operatori coinvolti.

Uso del contante e titoli al portatore

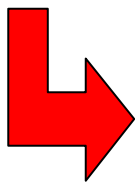
Il decreto legislativo n. 231 del 2007 aveva in origine stabilito in € 5.000 la soglia massima di liceità dell'uso del contante e dei titoli al portatore nelle transazioni a qualsiasi titolo tra soggetti diversi. La soglia, riportata ad € 12.500 dal decreto legge n. 112/2008, è stata nuovamente abbassata ad € 5.000 dal decreto legge n. 78/2010.

Sono oggi da considerarsi leciti i pagamenti effettuati in contante o con titoli al portatore purché inferiori alla soglia dei 5.000 euro.

E' bene precisare che il limite si applica anche alle operazioni frazionate, ossia quelle operazioni unitarie sotto il profilo economico, poste in essere attraverso più operazioni, singolarmente inferiori al limite, effettuate in momenti diversi ed in circostanziate periodo di tempo fissato in sette giorni, ferma restando l'esistenza di un'operazione frazionata quando ricorrano elementi per ritenerla tale.

Nota MEF

12.06.2008



Il Ministero ha chiarito che, al fine di stabilire l'esistenza di un'operazione frazionata, occorre fare riferimento al criterio della **cumulabilità**: due o più operazioni effettuate a distanza di tempo costituiscono un'unica operazione frazionata se sono tra loro cumulabili, com'è il caso dei dividendi societari superiori alla soglia limite per il socio i quali vengano distribuiti in più tranches inferiori a quella soglia e a distanza di tempo superiore ai sette giorni.

Non sono invece cumulabili, e non rappresentano pertanto frazionamenti di un'unica operazione soggetta ai divieti antiriciclaggio, i trasferimenti relativi a distinte ed autonome operazioni, ovvero alla medesima operazione quando il frazionamento è connaturato all'operazione stessa (ad es. contratto di somministrazione) oppure è la conseguenza di un preventivo accordo tra le parti (ad es. pagamenti rateizzati).

Il Ministero ha ribadito poi che determinante sarà, caso per caso, l'eventuale intento elusivo delle parti, manifestatosi in un frazionamento artificioso posto in essere con l'unico scopo di eludere la disciplina in materia.

Un prestito sociale effettuato da un socio di una società cooperativa, complessivamente superiore ai 5.000 euro, effettuato in contanti e in più tranches singolarmente inferiori a quella cifra, in un periodo di tempo pur superiore ai 7 giorni ma comunque in momenti ravvicinati, rischia di configurarsi quale operazione frazionata di finanziamento posta in essere in violazione di legge.

Si tenga presente che la sanzione per chi pone in essere l'operazione in

spregio al divieto può arrivare fino al 40% dell'importo trasferito.

Assegni

A seguito della modifica apportata dal D.I. n.78/2010, tornano ad essere liberi esclusivamente gli assegni al portatore inferiori ai 5.000 euro: tali assegni non dovranno per forza contenere il nome o la ragione sociale del beneficiario e la clausola di non trasferibilità.

Sempre per gli assegni trasferibili non è più richiesto, come originariamente previsto dal D.lgs. n.231/2007, l'indicazione del codice fiscale o della partita IVA del girante.

Si tenga presente, tuttavia, che le banche e la posta sono ormai tenute a rilasciare, di *default*, carnet di assegni già muniti della clausola di non trasferibilità: l'ottenimento di un carnet di assegni trasferibili è subordinato a richiesta scritta ed espone il richiedente a possibili accertamenti da parte dell'amministrazione finanziaria.

Obbligo di comunicazione di eventuali infrazioni incombente sui soggetti destinatari della normativa antiriciclaggio

I destinatari degli obblighi antiriciclaggio hanno l' OBBLIGO di riferire al Ministero dell'economia e finanze, entro trenta giorni, di eventuali infrazioni alle norme sull'uso del contante o di titoli al portatore, di cui abbiano notizia in relazione ai loro compiti di servizio e nei limiti delle loro attribuzioni o attività.

Analogo obbligo incombe, per espressa disposizione di legge (art.52, c.2., lett.c), sull'Organismo di Vigilanza e sul Collegio Sindacale dei destinatari degli obblighi antiriciclaggio costituiti in forma societaria, tra cui i Centri Servizi aderenti a Confcooperative.

SANZIONI APPLICABILI AI DESTINATARI DEGLI OBBLIGHI ANTIRICICLAGGIO

SANZIONI PENALI (art.55)

Violazione dell'obbligo di identificazione.	Multa da 2.600 a 13.000 euro.
Registrazione omessa, tardiva o incompleta	Multa da 2.600 a 13.000 euro.

Identificazione o registrazioni fraudolente compiute mediante mezzi idonei ad ostacolare l'individuazione del soggetto che ha effettuato l'operazione.	Multa da 5.200 a 26.000 euro.
Violazione del divieto di comunicazione dell'avvenuta segnalazione.	Arresto da sei mesi ad un anno ed ammenda da 5.000 a 50.000 euro.
Omissione delle comunicazioni prescritte dall'art.52, c.2 da parte degli organi di vigilanza e controllo delle società od enti destinatari del decreto.	Reclusione fino ad un anno e multa da 100 a 1.000 euro.

SANZIONI AMMINISTRATIVE (artt.56 e 57)

Violazione dell'obbligo di astensione nei casi previsti dall'art. 28, co. 7 ^{Ter} (coinvolgimento di società o altre entità giuridiche aventi sede in Paesi a rischio)	<ul style="list-style-type: none"> • operazioni fino a 50.000 euro: sanzione pecuniaria pari a 5.000 euro; • operazioni superiori ai 50.000 euro: sanzione pecuniaria dal 10% al 40% dell'importo dell'operazione; • operazioni di importo non determinato o non determinabile: sanzione pecuniaria da 25.000 a 250.000 euro.
Omessa istituzione del registro della clientela	Sanzione pecuniaria da 5.000 a 50.000 euro.
Omessa segnalazione di operazioni sospette	Sanzione pecuniaria dall'1% al 40% dell'importo dell'operazione non segnalata e nei casi più gravi pubblicazione del provvedimento sanzionatorio su due quotidiani.
Non rispetto degli obblighi informativi nei confronti dell'UIF	Sanzione pecuniaria da 5.000 a 50.000 euro.
Mancato rispetto del provvedimento di sospensione di operazioni sospette eventualmente emanato dall'UIF	Sanzione pecuniaria da 5.000 a 200.000 euro.
Violazione dell'obbligo di comunicazione di infrazioni alle norme sull'uso del contante e altri titoli al portatore	Sanzione pecuniaria dal 3% al 30% dell'importo dell'operazione.

SANZIONI APPLICABILI AI CLIENTI (art.55)

Omessa o falsa indicazione del soggetto per conto del quale eventualmente si esegue l'operazione	Reclusione da sei mesi a un anno e multa da 500 a 5.000 euro
Omessa o falsa fornitura di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale richiesta	Arresto da sei mesi a tre anni e ammenda da 5.000 a 50.000 euro

ART. 25 NOVIES D.LGS 231/2001 - DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE.

In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941.

Art. 171, c.1, lett. a-bis) e c. 3, L. 22 aprile 1941, n. 633.

[1] Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

omissis

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

omissis

[3] La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

omissis

Osservazioni

La condotta punita consiste nel mettere a disposizione del pubblico, tramite immissione in rete telematica con qualsiasi connessione, opere dell'ingegno protette.

La norma mira a tutelare la paternità dell'opera e il diritto del suo titolare a non veder frustrati i propri interessi economici.

E' prevista un'aggravante in caso di: opere altrui non pubbliche; usurpazione della paternità dell'opera; deformazione, mutilazione o modificazione dell'opera, purchè vi sia offesa all'onore e alla reputazione dell'autore.

La condotta può essere realizzata sia dal soggetto che materialmente diffonde telematicamente e senza autorizzazione l'opera, sia da eventuali gestori di server attraverso cui avviene tale diffusione.

Art. 171 bis, L. 633/1941

Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

Osservazioni

La norma è stata introdotta dal l. 489/1992 (e modificato dalla l. 169/99 e successivamente dalla l. 248/2000) e ha come oggetto materiale di tutela le diverse tipologie di beni qualificabili come programmi per elaboratore, o più genericamente software.

Le condotte punite sono di due tipologie:

c.1) l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore, o l'importazione, la distribuzione, la vendita, la detenzione a scopo commerciale o imprenditoriale o la concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; e ancora, qualsiasi condotta finalizzata a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

c.2) la riproduzione, su supporti non contrassegnati SIAE, il trasferimento su altro supporto, la distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies; ovvero l'esecuzione, l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero la distribuzione, vendita o concessione in locazione di una banca di dati.

Il comma 1 fa riferimento specifico ai software, e punisce ogni duplicazione, ancorché non finalizzata alla vendita, purchè volte ad ottenere un profitto, nonché ogni attività di intermediazione (importazione, distribuzione, ecc.) avente ad oggetto software abusivamente duplicati. Lo stesso comma prevede, inoltre, la punibilità di ogni azione finalizzata a rimuovere dispositivi di sicurezza sui software in questione.

Le condotte di cui al comma 2 sono poste a tutela delle c.d. banche dati.

Le condotte descritte fanno, comunque, riferimento all'esercizio "abusivo" di vari tipi di utilizzazione economica dell'opera dell'ingegno.

Il bene giuridico protetto è individuato negli interessi patrimoniali del titolare del diritto di sfruttamento economico del software.

Alcuni esempi di condotte rilevanti ai sensi dell'art. 171-bis l. 633/1941:

- Utilizzo di una copia concessa in licenza per installare un programma "monoutente" su più computer;
- Copia materiale di *floppy*, cd, ecc finalizzata all'installazione e alla distribuzione di programmi senza la necessaria licenza;
- Utilizzo abusivo di versioni di aggiornamento senza possesso della versione primaria;
- Violazione delle condizioni di licenza *client-server*;
- Azioni di pirateria internet (es. reti *peer to peer* per trasferimento non autorizzato di programmi protetti da un diritto d'autore);
- Installazione di copie illegali di *software*;
- Utilizzo fraudolento di programmi *shareware*, appositamente modificati al fine di mantenere gli stessi funzionanti oltre la scadenza.

In termini di condotta dei soggetti che operano nell'ente, in quanto parte dell'organigramma aziendale, societario, e consulenti:

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dalla Direzione e dall'Amministratore di sistema; non è consentito utilizzare strumenti e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio PC;
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come per esempio i modem); sui PC dotati di scheda audio e/o lettore cd non è consentito l'ascolto di programmi, file audio o musicali se non ai fini prettamente lavorativi;
- è severamente vietata la copia di Compact Disc audio, musicali, giochi e dati protetti dai diritti d'autore
- non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa; tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'Amministratore di sistema l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisti o installati

Art. 171 ter, L. 633/1941.

È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

È punito con la reclusione da uno a quattro anni e con la multa da da euro 2.582 a euro 15.493 chiunque:

a)riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b)esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

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

La condanna per uno dei reati previsti nel comma 1 comporta:

a)l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b)la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

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

Osservazioni

Il reato sussiste se la condotta è posta in essere per un uso non personale e se sussiste il dolo specifico di lucro.

La norma tutela una globalità di opere dell'ingegno inglobate in una serie indefinita di supporti (fonogrammi o videogrammi di opere letterarie, cinematografiche e audiovisive o sequenze di immagini in movimento, supporti per fruizione di servizi pay-tv ecc.).

Le condotte di reato del comma 1 sono descritte in modo dettagliato ed articolate in otto forme, al cui interno è ricompresa un molteplicità di comportamenti.

Questi ultimi, affinché assumano una rilevanza penale, devono essere posti in essere "per uso non personale" e "a fini di lucro".

Non rientra pertanto nelle condotte incriminate l'ipotesi di duplicazione di un'opera finalizzata ad un uso puramente privato, a prescindere dal fatto che tale utilizzo venga posto in essere dal soggetto autore del reato o da terzi.

La lettera f-bis) anticipa la soglia di tutela degli interessi protetti al punto da punire meri atti prodromici rispetto all'aggressione compiuta; in modo simile la lettera h) sanziona un mero reato di pericolo.

Il comma dell'art. 171-ter descrive, invece, tre circostanze aggravanti delle diverse fattispecie generali di cui al comma 1.

Incorre, ad esempio, nel reato in questione chi mette in vendita videocassette recanti contrassegno SIAE con la dicitura "abbinamento editoriale" sprovviste della relativa pubblicazione.

In termini di condotta dei soggetti che operano nell'ente o per conto dello stesso, in quanto parte dell'organigramma aziendale, societario, o consulenti:

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dalla Direzione e dall'Amministratore di sistema; non è consentito utilizzare strumenti e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio PC;
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come per esempio i modem); sui PC dotati di scheda audio e/o lettore cd non è consentito l'ascolto di programmi, file audio o musicali se non ai fini prettamente lavorativi;
- è severamente vietata la copia di Compact Disc audio, musicali, giochi dati protetti dai diritti d'autore
- non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa; tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'Amministratore di sistema l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquistati o installati

Art. 171septies, L. 633/1941.

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

- a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;***
- b) salvo che il fatto non costituisca più grave reato, a chiunque dichiarare falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181bis, comma 2, della presente legge.***

Osservazioni

La norma tutela la funzione pubblicistica e di garanzia della SIAE.

L'art. 171septies punisce:

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

b) chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181**bis**, comma 2, della presente legge.

Art. 171 octies, L. 633/1941.

Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi . visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

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

Osservazioni

La condotta prevista e punita consiste nel:

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

Es. di condotte: sblocco di servizi televisivi criptati, uso altrui credenziali per accedere a trasmissioni a pagamento, sblocco e modifica fraudolenta tessere *pay tv* ecc.

Per tutte le fattispecie di reato richiamate dall'art. 25novies D.Lgs 231/2001 si indicano di seguito, in via esemplificativa e non esaustiva, le aree aziendali a maggior rischio ed alcuni protocolli consigliati.

Aree aziendali esposte a rischio:

- 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 trasmissione comunicazioni ed informazioni per via elettronica;
- Gestione, utilizzo e diffusione di opere dell'ingegno protette.

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 a rischio (responsabile IT, amministratore di sistema, responsabile del trattamento ecc.);
- *Audit*/incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Previsione di un canale comunicativo specifico con l'O.d.V. e segnalazione allo stesso di qualsiasi violazione, anche ipotetica, al Codice Etico, ai regolamenti aziendali interni e alla politica di sicurezza informatica aziendale;
- Pianificazione e realizzazione di adeguato sistema di *risk analysis* dei sistemi informativi aziendali, della piattaforma IT, e delle procedure di sicurezza informatica aziendale; una proposta potrebbero essere la seguente:
 - a) ricognizione ed esame di tutte le componenti (*hardware* e *software*) della piattaforma IT che necessitano di strumenti di protezione contro reati informatici e reati in violazione del diritto d'autore rilevanti ex D.Lgs 231/2001;
 - b) valutazione oggettiva del livello di esposizione al suddetto rischio;
 - c) ricognizione ed verifica di protocolli, strumenti e procedure di controllo e di sicurezza esistenti ed attivi;
 - d) *gap analysis* sui suddetti protocolli, strumenti e procedure di sicurezza;
 - e) proposta di implementazione di un nuovo sistema organico di controllo e protezione del sistema informatico aziendale;
- Diffusione di una policy interna sul corretto utilizzo dei S.I. e della strumentazione informatica aziendale, con esplicitazione della tipologia di controlli applicati, nel rispetto dei diritti dei lavoratori, del D.Lgs 196/2003 e dei provvedimenti dell'Autorità Garante emanati in merito;
- Applicazione dei protocolli previsti nella sezione dedicata ai c.d. reati informatici (art. 24 bis D.Lgs 231/2001).

ART. 25 NOVIES D.LGS 231/2001 - INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA.

In relazione alla commissione del delitto di cui all'articolo 377-bis del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

Art. 377bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

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

Osservazioni

L'articolo in questione sanziona le condotte poste in essere da chiunque, con violenza, minaccia, o offerta di denaro o altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci tutti coloro che sono chiamati a rendere dichiarazioni in un procedimento penale e possono avvalersi della facoltà di non rispondere.

Il reato era già previsto e punito indirettamente dal D.Lgs. n. 231/2001, ma solo come reato transnazionale, ai sensi dell'art. 10, L. n. 146 del 16 marzo 2006.

L'art. 4 della Legge 3 agosto 2009, n. 116 introduce l'art 25novies nel D.lgs 231, trattasi però di un refuso, in quanto esiste già un art. 25novies (delitti in materia di violazione del diritto d'autore).

Aree aziendali esposte a rischio:

- Gestione dei rapporti con il personale, ed in particolare con soggetti coinvolti in procedimenti giudiziari;
- Attività della funzione Legale;
- Gestione rapporti con Legali esterni.

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 a rischio;
- Audit/incontri periodici fra O.d.V. e funzioni aziendali esposte al rischio *de quo*;
- Esplicitazione all'interno del Codice Etico dell'assoluto rifiuto e divieto di condotte o pratiche finalizzate ad influenzare eventuali soggetti (dipendenti, collaboratori, partners, concorrenti ec.) chiamati a rendere dichiarazioni di fronte all'autorità giudiziaria;
- Previsione di un canale comunicativo specifico con l'O.d.V. e segnalazione immediata allo stesso di qualsiasi notizia o notifica di indagine giudiziaria in corso.

ART.10

- 1. In relazione alla responsabilità amministrativa degli enti per i reati previsti dall'articolo 3, si applicano le disposizioni di cui ai commi seguenti.**
- 2. Nel caso di commissione dei delitti previsti dagli articoli 416 e 416-bis del codice penale, dall'articolo 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, e dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica all'ente la sanzione amministrativa pecuniaria da quattrocento a mille quote.**
- 3. Nei casi di condanna per uno dei delitti indicati nel comma 2, si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231, per una durata non inferiore ad un anno.**
- 4. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 2, si applica all'ente la sanzione amministrativa dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3, del decreto legislativo 8 giugno 2001, n. 231.**
- 5. Nel caso di reati concernenti il riciclaggio, per i delitti di cui agli articoli 648-bis e 648-ter del codice penale, si applica all'ente la sanzione amministrativa pecuniaria da duecento a ottocento quote.**
- 6. Nei casi di condanna per i reati di cui al comma 5 del presente articolo si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231, per una durata non superiore a due anni.**
- 7. Nel caso di reati concernenti il traffico di migranti, per i delitti di cui all'articolo 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione amministrativa pecuniaria da duecento a mille quote.**
- 8. Nei casi di condanna per i reati di cui al comma 7 del presente articolo si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231, per una durata non superiore a due anni.**
- 9. Nel caso di reati concernenti intralcio alla giustizia, per i delitti di cui agli articoli 377-bis e 378 del codice penale, si applica all'ente la sanzione amministrativa pecuniaria fino a cinquecento quote.**
- 10. Agli illeciti amministrativi previsti dal presente articolo si applicano le disposizioni di cui al decreto legislativo 8 giugno 2001, n. 231.**

Osservazioni

La L. 16 marzo 2006, n. 146 ha dato esecuzione alla Convenzione ed ai protocolli aggiuntivi delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 ed il 31 maggio 2001, ampliando altresì il catalogo dei reati rilevanti ai fini della responsabilità amministrativa degli enti ex D.lgs 231/2001.

La tecnica normativa utilizzata dal legislatore è stata diversa da quella utilizzata nell'introduzione delle altre fattispecie; infatti, anziché integrare il decreto nella parte relativa ai reati-presupposto, si è preferito disciplinare direttamente le nuove fattispecie e rinviare al D.lgs 231/2001 per la disciplina dei requisiti generali di imputazione della responsabilità all'ente.

A tal fine il legislatore ha innanzitutto offerto 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.

Partendo dalla necessaria configurazione transnazionale degli illeciti ivi previsti, e della necessità di tutti i requisiti di cui al D.Lgs. n. 231/2001 (in particolare interesse o vantaggio dell'ente e condotta di una sua figura apicale o subordinata), si può ritenere che **i processi/attività a maggiore rischiosità** per le cooperative risultano essere:

- Gestione contenziosi e accordi di transazione internazionali;
- Transazioni economiche commerciali e finanziarie internazionali;
- Selezione, assunzione e gestione del personale soprattutto straniero;
- Gestione contratti di appalto e subappalto;
- Rapporti con società controllate o partners estere;
- Operazioni fra enti appartenenti ad un unico gruppo societario;
- Attività import-export;
- Attività con altri soggetti terzi, localizzati in Paesi stranieri.

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, ed in particolare da parte di *partners*, fornitori, controparti contrattuali, collaboratori, enti destinatari di finanziamenti con cui si intrattengono stabilmente rapporti (eventuale inserimento in contratti, accordi e lettere di incarico di specifica clausola di risoluzione contrattuale in caso di condotte non in linea con i principi etici aziendali);
- Adozione del Codice Etico, del Modello 231 e del sistema sanzionatorio anche da parte di eventuali società estere di un Gruppo societario;
- Applicazione dei protocolli previsti dal Modello per i reati contro la P.A., i reati societari e di market abuse;

- Diffusione di prassi e procedure interne finalizzate alla corretta selezione e gestione di fornitori, controparti contrattuali, collaboratori, enti da sostenere e finanziare, in base a specifici requisiti di professionalità e onorabilità (es. richiesta preventiva certificato antimafia, DURC, iscrizione CCIA, legale rappresentanza, ecc.).
- Previsione di clausole con partner commerciali che vietino o regolamentino la cessione del contratto o il subappalto;
- 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 a rischio;
- Previsione di specifici flussi informativi tra le funzioni coinvolte in un'ottica di collaborazione, vigilanza reciproca e coordinamento;
- Predisposizione di rendiconti periodici all'O.d.V. ;
- Diffusione di apposite liste nominative ed elenco dei paesi a rischio individuati dall'O.d.V. ;
- Previsione di procedura per la verifica preventiva del c.d. "rischio paese" in fase di attuazione iniziative economiche/commerciali in determinate aree geografiche (es. liste UIF);
- Documentazione, archiviazione, tracciabilità degli atti e delle operazioni soprattutto finanziarie (intese sia come controprestazioni contrattuali che come omaggi o liberalità);
- Segnalazione all'O.d.V. di operazioni anomale o ad alto indice di rischio;
- Previsione di sistemi di controllo conformi alle disposizioni antiriciclaggio ex D.Lgs 231/2007 in caso di trasferimenti in denaro verso e provenienti da enti in rapporto di collaborazione/partenariato.