



Università  
Ca' Foscari  
Venezia

Corso di Laurea Specialistica  
(ordinamento ex D.M. 509/1999)  
in Economia e Finanza

**Tesi di Laurea**

**Responsabilità amministrativa dell'ente:  
il legame tra attività bancaria, reati e  
segnalazioni**

**Relatore:**

Ch. Prof. Simone MAZZONETTO

**Correlatore:**

Ch. Prof. Renato RIZZINI

**Laureando:**

Andrea Rosin

Matricola 813295

**Anno Accademico**

2017/2018



*"La legge è legge  
e per quanto possa sembrare strano  
va rispettata."  
C. Pedersoli*



# Abstract

Il presente lavoro analizza quanto stabilito dal decreto legislativo 8 giugno 2001, n. 231. Nello specifico si affronta il tema con il quale il legislatore adegua la normativa interna alle convenzioni internazionali in merito alla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, attuando quanto richiesto dall'articolo 11 della legge 29 settembre 2000, n. 300.

Il primo capitolo, suddiviso in tre parti, analizza nel dettaglio il D.Lgs 231/01. Nella prima parte si procede con la definizione dei principi generali, si determina l'ambito di applicazione del decreto e successivamente si individuano i soggetti ai quali tale provvedimento si rivolge. Nella seconda parte, invece, vengono prese in considerazione le sanzioni previste per chi commette un reato che rientra nelle fattispecie disciplinate. Infine, la terza parte individua le diverse tipologie di reato che si possono commettere e che sono regolamentate dal D.Lgs 231/01.

Il secondo capitolo analizza come un ente, e in questo caso un istituto di credito, attua e predispone misure con l'obiettivo di sensibilizzare tutti coloro che operano per conto della banca affinché tengano comportamenti lineari e corretti durante lo svolgimento delle proprie mansioni.

Infine, il terzo capitolo identifica i reati contemplati dal D.Lgs 231/01 ed individua le diverse attività, svolte nel settore bancario, ad essi potenzialmente associabili.



# Nota per il lettore

Typeset by L<sup>A</sup>T<sub>E</sub>X

La tesi è stata redatta con L<sup>A</sup>T<sub>E</sub>X<sub>2 $\epsilon$</sub>  ([L<sup>A</sup>T<sub>E</sub>X home page](#)). Esso è un programma di composizione tipografica open source e realizzato da *Leslie Lamport*, impiegando come motore tipografico T<sub>E</sub>X che fu concepito da *Donald Ervin Knuth* e distribuito negli anni '90. Al giorno d'oggi, T<sub>E</sub>X è un marchio registrato dall'*American Mathematical Society* (AMS). Il programma utilizza numerose estensioni per ampliare le sue potenzialità ed esse vengono identificate con la simbologia  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X, che sta per "*L<sup>A</sup>T<sub>E</sub>X with  $\mathcal{A}\mathcal{M}\mathcal{S}$ 's extensions*".

L'utilizzo di L<sup>A</sup>T<sub>E</sub>X è stato integrato con delle estensioni che hanno permesso di inserire, all'interno della seguente tesi, riferimenti incrociati cliccabili. Attraverso il pacchetto, inoltre, è stato possibile produrre un indice generale, una lista delle figure e una lista delle tabelle con i relativi numeri di pagina. Con i pacchetti `hyperref` e `url`, si sono inseriti riferimenti ipertestuali come quelli utilizzati per rinviare alla *homepage* di L<sup>A</sup>T<sub>E</sub>X o alla pagina delle funzionalità sviluppate dall'*American Mathematical Society*.

Il presente lavoro mi ha, quindi, permesso di conoscere e approfondire l'uso di questo motore tipografico e far, così, comprendere al lettore le potenzialità, che qui sono solo accennate, del programma e l'impegno ad esso riservato dall'autore.





# Indice

<b>Introduzione</b>	<b>1</b>
<b>1 Disciplina della responsabilità amministrativa dell'ente</b>	<b>5</b>
1.1 Soggetti destinatari della normativa e ambito di applicazione . . . . .	5
1.2 Sanzioni: commisurazione ed esclusione della responsabilità dell'ente . . . . .	11
1.2.1 La sanzione pecuniaria . . . . .	11
1.2.2 La sanzione interdittiva . . . . .	12
1.2.3 Pubblicazione di sentenza e confisca . . . . .	15
1.3 I reati presupposto . . . . .	19
1.3.1 I reati commessi contro la pubblica amministrazione . . . . .	20
1.3.2 La falsità in monete, ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio . . . . .	21
1.3.3 I reati societari e gli abusi di mercato . . . . .	23
1.3.4 I reati informatici, contro l'industria e contro il commercio . . . . .	24
1.3.5 I reati con finalità di terrorismo e di criminalità organizzata . . . . .	27
1.4 L'attuazione delle sanzioni . . . . .	31
<b>2 L'attività bancaria: Mog, Odv e sistema di segnalazioni</b>	<b>35</b>
2.1 Il modello di organizzazione, gestione e controllo . . . . .	36
2.2 ODV, codice etico e sistema disciplinare . . . . .	47
2.2.1 ODV: composizione, funzioni e poteri . . . . .	47
2.2.2 Il codice etico . . . . .	51
2.2.3 Il sistema disciplinare . . . . .	56
2.3 Reati presupposto: la segnalazione . . . . .	61
2.3.1 Contenuti e modalità di segnalazione . . . . .	62
2.3.2 Il whistleblowing . . . . .	65
<b>3 Attività bancaria e reati connessi con la responsabilità amministrativa dell'ente</b>	<b>69</b>
3.1 L'approccio basato sul rischio e i protocolli preventivi . . . . .	70
3.1.1 L'approccio basato sul rischio . . . . .	72

---

3.1.2	I protocolli preventivi . . . . .	75
3.2	Il rischio inerente e il rischio residuo . . . . .	78
3.3	La matrice dei rischi . . . . .	82
3.4	Reati presupposto e processi bancari sensibili . . . . .	85
3.4.1	Area sensibile 1: reati commessi contro la pubblica amministrazione	85
3.4.2	Area sensibile 2: reati di falsità in moneta, riciclaggio e autoriciclaggio	92
3.4.3	Area sensibile 3: reati societari e abusi di mercato . . . . .	96
3.4.4	Area sensibile 4: reati informatici, contro l'industria e contro il commercio . . . . .	106
3.4.5	Area sensibile 5: reati con finalità di terrorismo e criminalità orga- nizzata . . . . .	110
	<b>Conclusione</b>	<b>113</b>
	<b>Bibliografia</b>	<b>119</b>
	<b>Ringraziamenti</b>	<b>125</b>

# Elenco delle figure

1	White collar crimes . . . . .	1
1.1	I soggetti . . . . .	8
2.1	Contenuto del MOG . . . . .	38
2.2	L'idoneità del MOG . . . . .	40
2.3	Sentenza del Tribunale di Milano . . . . .	43
2.4	L'organismo di vigilanza . . . . .	49
2.5	Il codice etico: principi . . . . .	52
2.6	L'etica . . . . .	55
2.7	La via della segnalazione . . . . .	63
2.8	Il whistleblowing . . . . .	65
3.1	Il process oriented e risk based . . . . .	72
3.2	Realizzazione di protocolli . . . . .	75
3.3	Rischio inerente e rischio residuo . . . . .	79
3.4	La soglia di accettabilità: determinazione . . . . .	81
3.5	La matrice dei rischi . . . . .	84



# Elenco delle tabelle

1.1	I reati contro la pubblica amministrazione . . . . .	20
1.2	La falsità in monete . . . . .	22
1.3	Gli abusi di mercato . . . . .	23
1.4	I reati societari . . . . .	24
1.5	I reati informatici . . . . .	25
1.6	I reati contro l'industria e il commercio . . . . .	26
2.1	Le sanzioni disciplinari . . . . .	59
2.2	Le sanzioni disciplinari in funzione 231/01 . . . . .	60
3.1	La determinazione del rischio residuo . . . . .	80
3.2	Processi associati ai reati previsti dall'articolo 24 e 24-bis . . . . .	90
3.3	Processi associati ai reati previsti dall'articolo 25 . . . . .	91
3.4	Processi associati ai reati previsti dagli articoli 25-bis e 25-octies . . . . .	96
3.5	Processi associati ai reati previsti dall'articolo 25-ter . . . . .	104
3.6	Processi associati ai reati previsti dall'articolo 25-ter . . . . .	105
3.7	Processi associati ai reati previsti dall'articolo 25-ter e 25 sexies . . . . .	106
3.8	Processi associati ai reati previsti dagli articoli 24-bis, 25-bis-1 e 25-novies . . . . .	110
3.9	Processi associati ai reati previsti dagli articoli 24-ter, 25-quater e 25-quinquies	113



# Introduzione

Caro lettore il presente lavoro propone di analizzare quanto stabilito dal decreto legislativo 8 giugno 2001, n. 231. Nello specifico si affronta il tema con il quale il legislatore adegua la normativa interna alle convenzioni internazionali in merito alla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, attuando quanto richiesto dall'articolo 11 della legge 29 settembre 2000, n. 300. Tale decreto introduce nel nostro ordinamento giuridico una serie di norme e regole che disciplinano la responsabilità amministrativa a carico degli enti per tutti quei reati che vengono commessi a vantaggio o nell'interesse dell'ente stesso. Più precisamente il decreto in questione fa riferimento a tutti quei reati commessi da persone fisiche che all'interno dell'ente rivestono funzioni di rappresentanza, amministrazione e direzione o che esercitano funzioni di gestione e controllo.

La responsabilità amministrativa degli enti è stata introdotta con l'obiettivo di regolamentare i crimini commessi dai colletti bianchi: i cosiddetti white collar crimes. Si tratta di un fenomeno, sorto negli anni 30 e di origini americane<sup>1</sup>, caratterizzato per il fatto che il crimine viene commesso durante lo svolgimento di un'attività lavorativa da persone di elevata condizione sociale: in modo particolare si fa riferimento a reati, di natura colposa o dolosa, che traggono ispirazione esclusivamente da moventi di tipo economico.



Figura 1: **White collar crimes**  
(Fonte: *FerraraItalia.it*)

Questa tipologia di crimini riguarda sia le imprese che svolgono attività illecite sia enti che, in apparenza, sono caratterizzati da un oggetto sociale lecito ma che viene perseguito con attività aziendali non consentite quali la corruzione, la truffa, la lesione di interessi patrimoniali pubblici e così via.

---

<sup>1</sup>Il fenomeno si è sviluppato in Europa a partire dagli anni '70 e ha colpito con una frequenza elevata l'Italia sul finire degli anni '90. Basti pensare a scandali imprenditoriali come Cirio e Parmalat.

Fino a qualche anno fa, dal punto di vista normativo, nel nostro ordinamento giuridico, era difficile delimitare con precisione un'area all'interno della quale raccogliere le varie fattispecie di reato che potevano e che possono essere commessi tutt'ora dai colletti bianchi<sup>2</sup>. Per ovviare a questa problematica e per cercare di mettere ordine, interviene la Legge Delega n. 300/2000 con la quale si va a regolamentare, per la prima volta in Italia, la responsabilità amministrativa degli enti per gli illeciti dipendenti da reato. Si tratta di un vero e proprio punto di svolta per il nostro paese poiché si va a superare l'ostacolo posto dall'articolo 27 della nostra costituzione, in base al quale la responsabilità penale è personale; risultava dunque difficile, se non impossibile, estendere tale responsabilità anche agli enti. Dal lato pratico, il legislatore, vista l'esigenza di consolidare la cultura della trasparenza e con l'obiettivo di adottare un'efficace sistema di controllo sulla correttezza della conduzione di ogni attività aziendale, stravolge il concetto di ente che non viene più visto come un mero nucleo giuridico ma se ne prende in considerazione l'intero operato evitando quindi di agire solo nei confronti delle persone fisiche responsabili e correlate allo stesso.

Il motivo principale per cui procedo ad analizzare il decreto legislativo 231/01, sta nel fatto che, con la sua attuazione nel nostro ordinamento giuridico, viene introdotto un nuovo concetto di responsabilità: infatti, con questo provvedimento, alla responsabilità della persona fisica che materialmente ha commesso l'illecito, si aggiunge la responsabilità dell'ente: si parla nello specifico di una **“responsabilità amministrativa”** che ha forti analogie con la responsabilità penale. Sulla base di ciò, ne consegue che l'ente potrà essere dichiarato responsabile anche nel caso in cui la persona fisica che ha commesso l'illecito non venga individuata o il reato sia ad essa non imputabile; la responsabilità dell'ente assume, quindi, la caratteristica di “autonomia” rispetto a quella della persona fisica che ha commesso il reato stesso. L'obiettivo principale del provvedimento, di conseguenza, è quello di coinvolgere il patrimonio dell'ente e gli interessi economici dei soci in sede di contestazione giudiziale, cosa che, fino all'entrata in vigore della legge in esame, non era prevista.

Lo scopo principale di questo lavoro è quello di individuare quali sono le aree maggiormente sensibili e per le quali sussiste un elevato rischio di commissione dei reati disciplinati dal decreto in questione. In particolare, l'obiettivo è quello di redigere una lista di attività sensibili che vengono svolte durante l'esercizio dell'attività bancaria, e collegare a ciascuna attività individuata uno o più illeciti disciplinati dal decreto 231/01 che possono essere commessi durante lo svolgimento di quella stessa attività. Gli operatori del settore bancario, infatti, devono adottare misure tecniche ed organizzative adeguate con lo scopo di prevenire comportamenti che possono rientrare nella fattispecie degli illeciti disciplinati

<sup>2</sup>Attualmente esistono numerose ipotesi di reato disciplinate rispettivamente dal codice penale e civile, dalla legge fallimentare, dal TUB e dal TUF e da altri provvedimenti speciali.



dal D.Lgs 231/01. Si rende necessario dar vita, all'interno di ogni istituto di credito, ad un apposito modello organizzativo che sia in grado far ciò. In questo modo viene meno la responsabilità amministrativa dell'ente se lo stesso può dimostrare che il reato compiuto al suo interno è stato commesso eludendo in maniera fraudolenta il modello organizzativo.

Il presente lavoro si articola in tre capitoli.

Il primo capitolo, suddiviso in tre parti, analizza nel dettaglio il D.Lgs 231/01. Nella prima parte si procede con la definizione dei principi generali, si determina l'ambito di applicazione del decreto e successivamente si individuano i soggetti ai quali tale provvedimento si rivolge. Nella seconda parte, invece, vengono prese in considerazione le sanzioni previste per chi commette un reato che rientra nelle fattispecie disciplinate e si analizza tutto il procedimento di applicazione delle stesse. Infine, la terza parte individua le diverse tipologie di reato che si possono commettere e che sono regolamentate dal D.Lgs 231/01.

Il secondo capitolo analizza come un ente, e in questo caso un istituto di credito, attua e predispone misure con l'obiettivo di sensibilizzare tutti coloro che operano per conto della banca affinché tengano comportamenti lineari e corretti durante lo svolgimento delle proprie mansioni. In questo capitolo si introduce il concetto di modello di organizzazione e si individua quali sono le finalità, la struttura e i destinatari dello stesso. Si procede, successivamente, con la definizione di organismo di vigilanza e se ne individuano i compiti, le funzioni e i poteri che gli vengono attribuiti. Infine, viene analizzato tutto il sistema di segnalazioni che gli operatori bancari sono tenuti a rispettare nel caso in cui si verifichi un illecito disciplinato dal D.Lgs 231/01.

Infine, nel terzo capitolo si fornisce, dapprima, una definizione dettagliata dei reati contemplati dal D.Lgs 231/01, suddivisi per tipologie di illecito. Successivamente si individuano le diverse tipologie di attività svolte all'interno di una banca e se ne dà una definizione, poi si procede ad attribuire per ogni attività bancaria individuata quali sono i possibili reati che potenzialmente possono essere commessi durante l'esercizio di quella specifica attività.



## Capitolo 1

# Disciplina della responsabilità amministrativa dell'ente

Nel panorama internazionale la criminalità economica è ben organizzata e si sta sviluppando sempre più, incentrando la propria attenzione sugli enti, sulle società che detengono ingenti capitali e che sono portatrici di grandi interessi economici. Reati societari, corruzione, crimini comunitari, frodi economiche e così via, vengono regolarmente messi in atto da soggetti più importanti delle persone fisiche: **gli enti**. Infatti l'amministratore di una società viene nominato di volta in volta, soprattutto in relazione alla tipologia di affari che si andranno a svolgere, può essere sostituito, affiancato da professionisti e revocato quando non è considerato più utile o affidabile. In situazioni di questo tipo l'ente assume un ruolo di primaria importanza a discapito della persona fisica che riveste un ruolo marginale all'interno del mercato economico.

### 1.1 Soggetti destinatari della normativa e ambito di applicazione

Il decreto legislativo 8 giugno 2001 n. 231 è stato emanato in attuazione degli obblighi comunitari e, come stabilito dall' **articolo 1 al comma 2**, si applica a tutti gli enti forniti di personalità giuridica, alle società ed associazioni anche prive di personalità giuridica. Sono, quindi, numerosi i destinatari di questo decreto:

- Società di capitali;
- Società di persone;
- Enti e associazioni forniti di personalità giuridica;
- Società cooperative;

- Enti pubblici economici;
- Enti privati che concedono servizio pubblico;
- Comitati ed associazioni prive di personalità giuridica;
- Associazioni, riconosciute e non riconosciute;
- Fondazioni.

Pertanto sono da ritenersi soggetti appartenenti all'ambito di applicazione del decreto in questione le Spa, le Sapa, le Srl<sup>1</sup>, le Spa con partecipazione statale o di enti pubblici, le società estere con sede secondaria nel territorio dello Stato, le Sim, le Sicav, le società di investimento e di gestione di fondi comuni di investimento, le società di revisione, le società sportive, le mutue assicuratrici, le società semplici le Snc e le Sas, le società di fatto e quelle irregolari.

Il campo del decreto colpisce anche enti pubblici economici, ossia persone giuridiche il cui obiettivo principale è quello di gestire un'impresa industriale o commerciale operando nel rispetto di quanto stabilito dal diritto privato e si estende a fondazioni bancarie, a società private appaltatrici di opere pubbliche e cessionarie di finanziamenti statali.

Infine sono sottoposte al decreto in questione le cosiddette società miste e quelle pubbliche nonché le Onlus.

Sono da ritenersi, invece, escluse le imprese individuali, anche familiari, così come precisato dalla Corte di Cassazione n. 18941/04: *“L'ambito soggettivo di applicazione della recente disciplina in tema di responsabilità amministrativa delle persone giuridiche non può essere esteso anche alle imprese individuali. Invero il divieto di analogia “in malam partem” impedisce una lettura della normativa in esame che ne estenda le previsioni anche alle “ditte individuali”, si tratterebbe infatti di interpretazione chiaramente contraria all'art. 25 comma 2 cost.*<sup>2</sup>

Sono espressamente esclusi dall'ambito di applicazione del decreto lo Stato, gli enti pubblici territoriali, gli enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale.

---

<sup>1</sup>Rientrano anche le Srl a socio unico così come stabilito dal Tribunale di Milano con ordinanza 12 marzo 2008.

<sup>2</sup>La sentenza è stata impugnata con provvedimento del Tribunale di Roma, il quale ha ritenuto la stessa erronea perché l'interpretazione sistematica e razionale del decreto 231 e un elementare omogeneità di trattamento avrebbero dovuto indurre all'applicazione della disciplina nei confronti di tutti i soggetti economici e quindi anche nei confronti delle imprese individuali. La Cassazione ha richiamato il tenore letterale dell'art. 1 e ha sottolineato che la nuova responsabilità amministrativa è aggiuntiva e non sostitutiva di quella delle persone fisiche, escludendo infine ogni disparità di trattamento per l'evidente diversità dei soggetti economici.

Per quanto concerne la responsabilità dell'ente l'**articolo 2** disciplina il cosiddetto principio di legalità in base al quale l'ente non è da considerarsi responsabile per un fatto commesso che rappresenta un reato se la sua responsabilità amministrativa e le relative sanzioni in merito a quel reato non sono espressamente previste da una legge entrata in vigore prima della commissione del reato. Nel caso invece di successione di leggi l'ente non è considerato responsabile per un fatto che secondo una legge posteriore non costituisce più reato o in relazione al quale non è più prevista la responsabilità amministrativa dell'ente<sup>3</sup>. Inoltre nel caso di condanna gli effetti giuridici e l'esecuzione della stessa cessano. Se poi la legge del tempo in cui l'illecito è stato commesso è diversa dalle modifiche successive, **il comma 2 dell'articolo 3** prevede l'applicazione di disposizioni più favorevoli per l'ente, purché non sia intervenuta pronuncia irrevocabile<sup>4</sup>.

Infine la responsabilità dell'ente sussiste quando:

- non viene identificato l'autore del reato;
- non è possibile imputare il reato ad un soggetto specifico;
- il reato commesso si estingue per una causa diversa dall'amnistia<sup>5</sup>.

La norma afferma, altresì, che tutte le disposizioni previste siano applicate ad enti forniti di personalità giuridica oppure a società o associazioni che ne sono prive<sup>6</sup>.

Affinché l'ente sia da considerarsi responsabile, e quindi soggetto a sanzioni, si devono individuare ulteriori criteri che vanno ad integrare i requisiti normativi. Questi criteri si distinguono in *oggettivi e soggettivi*.

Per quanto concerne il criterio **oggettivo**, il reato deve essere commesso a vantaggio o nell'interesse dell'ente e da un soggetto che riveste al suo interno un rapporto qualificato<sup>7</sup>.

A tal proposito si possono fare due distinzioni:

- Soggetti in posizione apicale;
- Soggetti subordinati.

Nella prima tipologia di soggetti rientrano tutte quelle persone che svolgono un ruolo di rappresentanza, amministrazione o direzione dell'ente o di una sua entità autonoma

---

<sup>3</sup>Articolo 3 comma 1.

<sup>4</sup>Tali disposizioni non trovano applicazione se si tratta di leggi eccezionali o temporanee.

<sup>5</sup>L'articolo 8 prevede che l'ente non possa rinunciare all'amnistia e nel caso in cui questa sia concessa non si deve procedere nei confronti dell'ente.

<sup>6</sup>Questo è previsto dall'articolo 1 in base al quale sono esclusi dal provvedimento lo Stato, gli enti pubblici territoriali, altri enti pubblici non economici nonché enti che svolgono funzioni di rilievo costituzionale.

<sup>7</sup>Articolo 5 comma 1.

nonché da persone che gestiscono o controllano, anche soltanto di fatto, l'ente stesso. Pertanto, appartengono a questa categoria, persone dotate di poteri che gli consentono di prendere decisioni, di qualsiasi tipo, in nome e per conto dell'ente. Tra questi soggetti troviamo, ad esempio, il legale rappresentante, l'amministratore delegato, il direttore di una unità organizzativa autonoma legata all'ente, e tutti quelle persone che sono delegate dagli amministratori a svolgere attività gestionali all'interno dell'ente o all'interno di sedi distaccate<sup>8</sup>.

Nella seconda tipologia di soggetti, invece, rientrano tutti coloro che sono sottoposti alla direzione e vigilanza dei soggetti apicali. Quindi, fanno parte di questa categoria i dipendenti, i collaboratori e tutte quelle persone che svolgono mansioni sotto la direzione di soggetti apicali<sup>9</sup>.



Figura 1.1: **I soggetti**  
(Fonte: Federcasa.it)

In conclusione la condizione necessaria per poter parlare di responsabilità amministrativa degli enti è legata al fatto che il reato presupposto sia stato commesso a vantaggio o nell'interesse dell'ente. In questo modo la responsabilità dell'ente è prevista non solo quando lo stesso ha tratto vantaggio dalla commissione dell'illecito ma anche nel caso in cui l'operazione illecita abbia avuto un esito negativo: proprio per questa ragione il legislatore ha volutamente indicato in modo disgiunto il riferimento all'interesse e al vantaggio.

La Suprema Corte di Cassazione (Cassazione penale, Sez. II, 20 dicembre 2005, n. 3615) ha inoltre chiarito che: *“Il requisito oggettivo che il reato sia commesso ‘nell’interesse o nel vantaggio dell’ente’ che l’art. 5 D.Lgs. n. 231/2001 indica quale condizione*

<sup>8</sup>Sulla base dell'articolo 5 comma 2, l'ente non risponde se tali soggetti agiscono esclusivamente nel proprio interesse o per quello di terzi.

<sup>9</sup>Si fa riferimento anche a soggetti che non fanno parte del personale assunto come ad esempio consulenti e promotori che possono compiere, su mandato, operazioni per conto dell'ente.

*essenziale per l'applicazione della sanzione, esprime due concetti giuridicamente diversi, potendosi distinguere un interesse 'a monte' della società ad una locupletazione prefigurata, pur se di fatto, eventualmente non più realizzata rispetto ad un vantaggio obiettivamente conseguito all'esito del reato, perfino se non espressamente divisato 'ex ante' dall'agente. E' configurabile il vantaggio per l'ente anche nell'ipotesi di successiva distrazione su conti personali dell'amministratore di somme erogate alla società dallo Stato, in quanto il momento realizzativi del profitto coincide con l'accreditamento delle somme alla società: ciò che avviene dopo resta condotta 'post factum' che non elide il dato storico del profitto già conseguito dall'ente".*

Relativamente ai criteri **soggettivi**, questi si riferiscono a tutti gli strumenti che l'ente ha in dotazione e il cui obiettivo è quello di prevenire la commissione dei reati previsti dal decreto. È di fatto esclusa la responsabilità dell'ente se lo stesso dimostra che<sup>10</sup>:

- a) L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi;
- b) Il compito di vigilare sul funzionamento e sull'osservanza dei modelli e di curarne il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;
- c) Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione;
- d) Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di predetto ente.

Tuttavia, è necessario che queste condizioni si verifichino congiuntamente affinché si possa escludere la responsabilità dell'ente.

La normativa disciplina anche i principi generali che devono essere adottati dagli enti e che devono caratterizzare i modelli organizzativi di cui alla lettera a). Si tratta di principi a carattere generale che non si soffermano su quelli che devono essere per forza i connotati specifici di ciascun modello. Pertanto spetta all'ente stesso adottare un modello personalizzato ed efficacemente attuato nelle procedure aziendali che risulti, tuttavia, idoneo a prevenire i reati indicati nel decreto in questione. Nello specifico il modello deve rispondere alle esigenze richieste dall'**articolo 6 comma 2**. Infatti, spetta al modello:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

---

<sup>10</sup>Articolo 6 comma 1 lettere a, b, c, d.

- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

A corollario di tutto questo è necessario sia previsto un sistema disciplinare idoneo affinché il modello sia attuato in maniera precisa ed efficace. Questo sistema prevede misure quali verifiche periodiche e modifiche tempestive nel caso si verificassero cambiamenti o violazione di regole aziendali.



## 1.2 Sanzioni: commisurazione ed esclusione della responsabilità dell'ente

Ciò che rappresenta un forte oggetto di discussione per quanto concerne il decreto legislativo 231/2001 è il riferimento alla natura amministrativa della responsabilità dell'ente. Infatti, pur essendo definita in modo formale "*responsabilità amministrativa*", nella realtà siamo molto più vicini ad una "*responsabilità penale*". In merito a ciò, il decreto analizzato, individua quattro macroaree nelle quali far ricadere la responsabilità dell'ente attribuendo a ciascuna di esse una determinata fattispecie di sanzione. Nello specifico, così come stabilito dall'**articolo 9**, in caso di illecito si possono applicare all'ente le seguenti sanzioni:

- La sanzione pecuniaria;
- Le sanzioni interdittive;
- La confisca;
- La pubblicazione di condanna.

### 1.2.1 La sanzione pecuniaria

La sanzione "*pecuniaria*", disciplinata dall'**articolo 10**, rappresenta la sanzione di base applicata quando l'illecito amministrativo è legato al compimento di un reato. Si tratta di una sanzione attuata qualora il giudice ritenga l'ente responsabile del reato commesso e del cui pagamento risponde l'ente stesso con il proprio patrimonio.

Il sistema che porta alla determinazione della sanzione pecuniaria si articola in due fasi:

- Nella prima fase si determina l'ammontare delle quote, che non può mai essere inferiore a cento né superiore a mille. Spetta al giudice stabilire il numero delle quote in base alla valutazione da lui espressa e legata alla gravità del reato, alla responsabilità dell'ente nonché al tipo di misure intraprese per porvi rimedio a seguito della commissione dell'illecito<sup>11</sup>.
- Nella seconda fase il giudice stabilisce il valore monetario di ogni singola quota: tale valore viene determinato in base alle condizioni economiche e patrimoniali dell'ente e deve essere compreso in un range che va da euro 258,23 a euro 1.549,37. La sanzione si determina moltiplicando il numero di quote per il singolo valore monetario delle stesse con la conseguenza che la sanzione oscillerà tra un importo minimo di euro

<sup>11</sup>Articolo 11. Nello specifico si fa riferimento al fatto che il modello organizzativo, il codice etico e i sistemi disciplinari adottati siano idonei a prevenire illeciti amministrativi.

25.823,00 e un importo massimo di euro 1.549.370,00. In casi del genere, quando trovano applicazione le sanzioni pecuniarie, si può facilmente notare come un'impresa di grandi dimensioni sia in grado di ammortizzare un importo massimo come quello indicato, mentre appare diverso il caso opposto: per un'impresa di piccole dimensioni l'importo minimo, stabilito dalla normativa, potrebbe essere sproporzionato e mettere in seria difficoltà la sopravvivenza dell'ente.

Quindi, a parità di illecito risulta evidente che la sanzione commisurata potrebbe essere gravosa e fatale per un ente di modeste dimensioni, fino al raggiungimento della soglia di non sopportabilità economica, e diventare, invece, inefficace nei riguardi di enti di grandi dimensioni dotati di notevoli risorse economiche e patrimoniali. Proprio per questa ragione, e per evitare il rischio di rendere inefficace la sanzione, il nostro legislatore ha stabilito casi di riduzione della stessa.

Infatti, in base a quanto stabilito dall'**articolo 12** la sanzione pecuniaria è ridotta della metà e non può essere superiore a euro 103.291,38 se si verificano i seguenti casi:

- L'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- Il danno patrimoniale cagionato è di particolare tenuità.

La sanzione viene altresì ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado:

- L'ente ha risarcito integralmente il danno e ha eliminato integralmente le conseguenze dannose o pericolose del reato ovvero si è comunque adoperato efficacemente in tal senso;
- È stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati delle specie di quello verificatosi.

Se queste due condizioni si manifestano congiuntamente allora la sanzione viene ridotta dalla metà ai due terzi e mai potrà essere inferiore a euro 10.329,14.

### 1.2.2 La sanzione interdittiva

Le sanzioni "*interdittive*" si applicano, in aggiunta alle sanzioni pecuniarie, se e solo se sono espressamente previste per quella tipologia di reato per il quale l'ente viene condannato. Data la loro natura inibitoria questa tipologia di sanzioni è stata introdotta dal legislatore con l'obiettivo di contrastare in modo più efficace le condotte gravose e illecite commesse all'interno dell'ente.

Le sanzioni interdittive sono previste dall'**articolo 9 comma 2** e sono le seguenti:

- Interdizione dall'esercizio dell'attività;
- Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionale alla commissione dell'illecito;
- Divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- Esclusione da agevolazioni, contributi, finanziamenti, o sussidi e l'eventuale revoca di quelli già concessi;
- Divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive hanno una durata limitata che non deve essere inferiore ai tre mesi né superiore ai due anni e non si applicano nei casi previsti dall'**articolo 12 comma 1**.

Per quanto riguarda, invece, i presupposti di applicazione, questi sono regolamentati dall'**articolo 13** il quale stabilisce che le sanzioni si applicano soltanto se si verificano una delle seguenti condizioni:

- L'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- In caso di reiterazione di illeciti (commissione di un illecito dipendente da reato nei cinque anni dalla sentenza definitiva di condanna per un altro precedente).

Nell'applicare le sanzioni interdittive il giudice deve tener conto di tre criteri: **adeguatezza, proporzionalità e gradualità** <sup>12</sup>.

Per quanto concerne "*l'adeguatezza*", le sanzioni interdittive devono essere scelte in modo tale da prevenire il tipo di illecito che si è verificato, favorendo, se necessario, l'applicazione congiunta di più sanzioni.

In base al criterio della "*proporzionalità*", invece, il giudice deve tener conto di quanto stabilito dall'**articolo 11 comma 1** e quindi deve considerare la gravità del fatto, quale sia la responsabilità dell'ente e le attività svolte per eliminare o quantomeno attenuare le conseguenze del reato commesso.

Infine la "*gradualità*" è un criterio che prevede l'applicazione della sanzione massima interdittiva, **inibizione dall'esercizio dell'attività**, soltanto se tutte le altre sanzioni risultassero essere inadeguate alla tipologia di reato commesso.

---

<sup>12</sup>Criteri prontamente stabiliti dall'articolo 14. Va altresì ricordato che il divieto di contrattare con la pubblica amministrazione può essere limitato a determinati tipi di contratto o a determinate amministrazioni.

Oltre a ciò, esistono situazioni particolari per le quali la sanzione interdittiva viene applicata in modo definitivo e tombale; queste situazioni sono disciplinate dall'**articolo 16** il quale prevede quanto segue:

- quando l'ente è stato condannato per almeno 3 volte negli ultimi 7 anni all'interdizione temporanea dall'esercizio dell'attività;
- quando all'ente è stato applicato il divieto di contrattare con la pubblica amministrazione ovvero il divieto di pubblicizzare bene o servizi per almeno 3 volte negli ultimi 7 anni;
- quando l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o a agevolare la commissione di reati<sup>13</sup>.

Infine, fermo restando l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non sempre vengono commisurate. Infatti, l'**articolo 17** disciplina le riparazioni delle conseguenze del reato: in altri termini se prima della dichiarazione di apertura del dibattimento di primo grado, concorrono determinate condizioni, le sanzioni interdittive non sono applicabili.

Le condizioni stabilite dal decreto sono le seguenti:

- L'ente ha risarcito integralmente il danno e ha eliminato integralmente le conseguenze dannose o pericolose del reato ovvero si è comunque adoperato efficacemente in tal senso;
- È stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati delle specie di quello verificatosi.

Nei confronti dell'ente si applicano soltanto le sanzioni interdittive stabilite nel presente decreto legislativo anche quando diverse disposizioni di legge prevedono, in conseguenza della sentenza di condanna per il reato, l'applicazione nei confronti dell'ente di sanzioni amministrative di contenuto identico o analogo. Inoltre, se in conseguenza dell'illecito, all'ente è già stata applicata una sanzione amministrativa di contenuto identico a analogo a quella interdittiva prevista dal presente decreto legislativo, la durata della sanzione già sofferta è computata ai fini della determinazione della durata della sanzione amministrativa dipendente da reato<sup>14</sup>.

Un'alternativa all'applicazione delle sanzioni interdittive è rappresentata dal commissario giudiziale<sup>15</sup>. In luogo dell'applicazione di una sanzione interdittiva e per un periodo pari alla durata della sanzione stessa, il giudice ha la facoltà di disporre il proseguimento dell'attività dell'ente da parte di un commissario quando ricorre una delle seguenti casistiche:

---

<sup>13</sup>In situazioni di questo tipo non trovano mai applicazione le disposizioni previste dall'articolo 17.

<sup>14</sup>Articolo 83: concorso di sanzioni.

<sup>15</sup>Disposizione stabilita dall'articolo 15.

- L'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- L'interruzione dell'attività dell'ente può provocare, date le sue dimensioni e condizioni economiche del territorio in cui opera, rilevanti ripercussioni sull'occupazione.

Dopo aver accertato l'esistenza di una delle suddette situazioni, il giudice, con propria sentenza e tenendo presente l'illecito commesso, determina la prosecuzione dell'attività dell'ente, stabilisce quali sono i compiti e i poteri del commissario e soprattutto vigila l'operato dello stesso con particolare attenzione al fatto che venga adottato un idoneo modello organizzativo atto a prevenire reati della specie di quello verificatosi.

Infine, va specificato che il profitto derivante dalla prosecuzione dell'attività dell'ente deve essere sempre confiscato. Infatti, pur cercando di tutelare la collettività e la stabilità economica di un territorio, si ricorda che il commissario giudiziale è un'alternativa alla sanzione interdittiva e proprio per questa ragione deve mantenere un carattere sanzionatorio.

### 1.2.3 Pubblicazione di sentenza e confisca

Quando il giudice applica nei confronti dell'ente una sanzione interdittiva ha inoltre la possibilità di disporre la "*pubblicazione della sentenza di condanna*"<sup>16</sup>. Si tratta di una misura che trova applicazione qualora siano commessi reati molto gravi tali da legittimare l'interesse del pubblico alla conoscenza della condanna. La pubblicazione di sentenza è uno strumento a disposizione del giudice che va ad integrare quanto previsto dalle sanzioni interdittive e che, se applicato, può avere un impatto negativo sull'immagine dell'ente.

La pubblicazione di sentenza, una volta disposta dal giudice, avviene sulla base di quanto stabilito dall'**articolo 36** del codice penale unitamente all'affissione nel comune dove l'ente ha la sede principale. Per quanto concerne tale articolo, questo prevede che la sentenza di condanna sia pubblicata nel sito internet del Ministero della giustizia e con durata, stabilita dal giudice, non superiore a trenta giorni<sup>17</sup>. La sentenza, infine, può anche essere pubblicata, per intero o per estratto, in uno o più giornali ovvero nel comune in cui l'illecito è stato commesso<sup>18</sup>.

Ai sensi dell'**articolo 19** del decreto legislativo 231/01, è sempre disposta, con la sentenza di condanna, la "*confisca*" del prezzo (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del profitto (utilità economica immediata ricavata del reato) salvo per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede. Quando non è possibile

<sup>16</sup> Articolo 18 comma 1.

<sup>17</sup> In mancanza di disposizione del giudice la durata di pubblicazione è fissata in 15 giorni.

<sup>18</sup> La pubblicazione è eseguita a cura della cancelleria del giudice e a spese dell'ente. Articolo 18 comma 3.

eseguire la confisca a norma del comma 1, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

In base a quanto stabilito dall'**articolo 19** emerge in primo luogo che la confisca è una sanzione amministrativa che si distingue dalle altre: infatti, non ha un limite di valore ben definito.

In secondo luogo emerge una duplice configurazione della stessa:

**Confisca tradizionale:**

- Colpisce il prezzo del reato, definito dalla cassazione come il compenso dato o promesso ad un soggetto per l'esecuzione dell'illecito
- Colpisce il profitto del reato da intendersi come insieme di vantaggi economici ottenuti con la commissione dell'illecito.

**Confisca equivalente:**

- Ha per oggetto somme di denaro, beni o altra utilità di valore equivalente al prezzo o al profitto.

Particolare attenzione merita il concetto di profitto, spesso al centro di controversie giurisprudenziali. Infatti, il profitto non deve intendersi come interesse o vantaggio dell'ente ma deve essere considerato l'oggetto della sanzione.

Il profitto deve presentare congiuntamente determinate caratteristiche:

- Deve avere natura patrimoniale;
- Deve risultare concreto;
- Deve essere direttamente e causalmente riconducibile al reato presupposto<sup>19</sup>.

Infine, il profitto si distingue in *confiscabile e non confiscabile*. Nel primo caso oggetto di confisca sarà esclusivamente il vantaggio economico derivante dalla commissione dell'illecito. Nel secondo caso, invece, non è da considerarsi oggetto di confisca tutto ciò che deriva dal compimento di una prestazione lecita a favore dell'ente.

Qualora il reato sia stato commesso da un soggetto in posizione apicale, in base all'**articolo 6 comma 5**, è prevista la confisca anche nel caso particolare in cui l'ente sia considerato non responsabile avendo adottato e attuato in maniera efficace tutte le misure precauzionali previste dalla norma stessa. In questa situazione specifica, non si deve considerare la confisca come una pura sanzione, visto il difetto di responsabilità dell'ente,

---

<sup>19</sup>Cassazione, sentenza 27 marzo 2008.

ma si deve considerare la stessa come lo strumento utilizzato per ristabilire l'equilibrio economico venuto meno a seguito della commissione dell'illecito. Nel caso di commissariamento dell'ente, al **comma 4 dell'articolo 15** si specifica che il profitto derivante dalla prosecuzione dell'attività venga confiscato. Si tratta di una misura straordinaria che va a sostituire la sanzione interdittiva, che se applicata, determinerebbe l'interruzione dell'attività dell'ente.





## 1.3 I reati presupposto

Il decreto legislativo 231 del 2001 fa riferimento ai cosiddetti “*reati presupposto*”. Con questo termine si individua quell’insieme di fatti criminosi posti in essere per la commissione di un altro reato. In altre parole il reato presupposto rappresenta l’antefatto essenziale che deve verificarsi affinché si concretizzi un’altra fattispecie di illecito. Richiamando il concetto di reati presupposto, il decreto in questione ha inteso sanzionare l’ente, dal punto di vista amministrativo, che ha permesso la realizzazione di un illecito da parte di uno o più dei suoi membri. Di conseguenza il fatto criminoso si ripercuoterà, sotto forma di sanzione, anche nei confronti della persona giuridica. In origine i reati presupposto erano disciplinati esclusivamente dagli **articoli 24 e 25** e l’elenco era assai ridotto.

Infatti con l’introduzione del decreto nel 2001 i reati previsti erano soltanto 5:

- Indebita percezione di erogazioni;
- Truffa in danno dello Stato o di un ente pubblico;
- Frode informatica in danno dello Stato o di un ente pubblico;
- Concussione;
- Induzione indebita a dare o promettere utilità e corruzione.

Ad oggi, grazie a successive integrazione e modifiche, i reati presupposto individuati sono oltre 130. Nello specifico è possibile suddividere i reati in aree sensibili in modo tale da poterli classificare in base alla tipologia di rischio sottostante. In riferimento al lavoro svolto non verranno trattati tutti i tipi di reato ma solamente le seguenti aree sensibili:

- Reati commessi contro la pubblica amministrazione;
- Reati di falsità in moneta, ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- Reati societari e abusi di mercato;
- Reati informatici, contro l’industria e il commercio;
- Reati con finalità di terrorismo e di criminalità organizzata.

### 1.3.1 I reati commessi contro la pubblica amministrazione

Gli articoli 24 e 25 del decreto prendono in considerazione una serie di reati disciplinati anche dal codice penale e che sono tra di loro accomunati dall'oggetto che tutelano: il buon andamento e l'imparzialità della pubblica amministrazione. Dal punto di vista penale si considera ente della pubblica amministrazione qualsiasi soggetto persona giuridica che persegua, realizzi o gestisca interessi di carattere pubblico. Rientrano in questa categoria, ad esempio, lo stato, le regioni, le province, i comuni, i ministeri, i dipartimenti, le commissioni, gli enti pubblici non economici, eccetera. Nella tabella sottostante si elencano i reati disciplinati dagli articoli 24 e 25 del decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>Malversazione ai danni dello Stato</b>	Art. 316-bis c.p.	-Pecuniaria fino a 500 quote. -Interdittiva art. 9 comma 2, lettere c, d ed e.
<b>Indebita percezione di erogazioni</b>	Art. 316-ter c.p.	-Pecuniaria fino a 500 quote. -Interdittiva art. 9 comma 2, lettere c, d ed e.
<b>Truffa ai danni dello Stato</b>	Art. 640, comma 2, n. 1 c.p.	-Pecuniaria fino a 500 quote. -Interdittiva art. 9 comma 2 lettere c, d ed e.
<b>Truffa aggravata</b>	Art. 640-bis c.p.	-Pecuniaria fino a 500 quote. -Interdittiva art. 9 comma 2 lettere c, d ed e.
<b>Frode informatica</b>	Art. 640-ter c.p.	-Pecuniaria fino a 500 quote. -Interdittiva art. 9 comma 2 lettere c, d ed e.
<b>Concussione</b>	Art. 317 c.p.	-Pecuniaria da 300 a 800 quote. -Interdittiva art. 9 comma 2.
<b>Induzione indebita a dare o promettere utilità</b>	Art. 319-quatern c.p	-Pecuniaria da 300 a 800 quote.
<b>Corruzione per l'esercizio della funzione</b>	Art. 318 c.p.	-Pecuniaria fino a 200 quote.
<b>Corruzione per un atto contrario ai doveri d'ufficio</b>	Art. 319 c.p.	-Pecuniaria da 300 a 800 quote. -Interdittiva art. 9 comma 2.
<b>Corruzione in atti giudiziari</b>	Art. 319-ter, comma 1, c.p.	-Pecuniaria da 200 a 600 quote. -Interdittiva art. 9 comma 2.
<b>Istigazione alla corruzione</b>	Art. 322 c.p.	-Pecuniaria fino a 200 quote. -Interdittiva art. 9 comma 2.

Tabella 1.1: *I reati contro la pubblica amministrazione*

Le fattispecie di reato che rientrano in questa categoria implicano necessariamente una relazione tra un soggetto privato e un pubblico agente ossia una persona fisica che assume il titolo di "pubblico ufficiale" o "incaricato di pubblico servizio" così come stabilito dagli

articoli 357 e 358 del codice penale. Il pubblico ufficiale è colui che esercita una funzione pubblica legislativa, giudiziaria o amministrativa come per esempio l'ufficiale giudiziario, il curatore fallimentare, il consigliere comunale, il tabaccaio che riscuote le tasse automobilistiche, il notaio e così via. L'incaricato di pubblico servizio, invece, è colui che svolge attività di interesse pubblico. Si tratta di attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzate, dalla mancanza dei poteri tipici di quest'ultime, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale

Le mansioni sopra individuate, dal punto di vista normativo, non sempre richiedono l'impiego in un ente pubblico. Infatti, determinate attività svolte all'interno di un istituto bancario possono assumere una rilevanza tale da far riconoscere in capo a dipendenti o esponenti bancari la qualifica di pubblico ufficiale o incaricato di pubblico servizio.

### 1.3.2 La falsità in monete, ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

L'**articolo 25-bis** regola tutti quei reati che sono legati alla falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento. In particolare l'introduzione di questo articolo ha come obiettivo principale quello di tutelare la cosiddetta fede pubblica ovvero garantire la purezza di alcuni simboli di Stato. Sono, infatti, previsti dal codice penale una serie di reati che vanno a punire comportamenti che alterano l'integrità di particolari "oggetti di Stato" quali le monete, le banconote, le carte o le cedole al portatore emesse da istituti autorizzati, i valori bollati e le carte filigranate.

L'**articolo 25 octies** è stato introdotto a seguito dell'entrata in vigore del decreto antiriciclaggio del 21 novembre 2007. Questo articolo estende la responsabilità dell'ente ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio<sup>20</sup>.

L'obiettivo principale di questo articolo è quello di prevenire e soprattutto reprimere l'introduzione nel mondo economico di denaro, beni o utilità provenienti dalla commissione di attività delittuose rafforzando così la disciplina della responsabilità amministrativa degli enti. In questo modo si è cercato di rimuovere tutti quegli ostacoli che rendevano difficile l'individuazione dei reati e dei presunti colpevoli oltre che garantire l'integrità dei mercati e della libera concorrenza di cui godono gli operatori economici. Inoltre a carico di intermediari finanziari, banche e altri istituti obbligati sono applicate previsioni contenute nel decreto antiriciclaggio le cui finalità sono quelle di contrastare il riciclaggio e l'impiego di denaro, beni o utilità aventi provenienza illecita. In capo a questi soggetti sono previste una serie di attività quali l'adeguata verifica della clientela, la segnalazione di

<sup>20</sup>Tale reato è disciplinato dal codice penale e inserito tra i reati presupposto grazie alla legge 186/2014 entrata in vigore il primo gennaio 2015.

operazioni sospette, la conservazione di documenti e la comunicazione delle violazioni dei divieti in tema di denaro contante e titoli al portatore, che se non vengono poste in essere possono comportare sanzioni in capo all'ente ai sensi del decreto antiriciclaggio. Infatti è importante ricordare che se l'operatore di banca non rispettasse questi adempimenti e fosse consapevole della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato personalmente a rispondere per i predetti reati e potrebbe anche configurarsi la responsabilità amministrativa della banca sulla base del decreto 231/01.

Nella tabella sottostante si elencano i reati disciplinati dall'articolo 25-bis e dall'articolo 25-octies del decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>Falsificazione e alterazione di monete</b>	Art. 453 e 454 c.p.	-Pecuniaria da 300 a 800 quote per l'art. 453; -Pecuniaria fino a 500 per l'art. 454. -Interdittiva art. 9 comma 2 .
<b>Spendita e introduzione nello Stato di monte falsificate</b>	Art. 455 e 457 c.p.	-Pecuniaria da 300 a 800 quote per l'art.455; -Pecuniaria fino a 200 quote per l'art. 464; -Interdittiva art. 9 comma 2 .
<b>Falsificazione e uso di valori di bollo, contraffazione, fabbricazione e detenzione di carta filigranata</b>	Art. 459, 460, 461 e 464 c.p.	-Pecuniaria fino a 500 quote per l'art. 460 e 461; -Pecuniaria fino a 200 quote per l'art. 464; -Interdittiva art. 9 comma 2 con esclusione dell'art. 464.
<b>Ricettazione</b>	Art. 648 c.p.	-Pecuniaria da 200 a 800 quote; -Pecuniaria da 400 a 1000 quote se prevista reclusione superiore a 5 anni; -Interdittiva art. 9 comma 2 .
<b>Impiego di denaro, beni o utilità di provenienza illecita</b>	Art. 648-ter c.p.	-Pecuniaria da 200 a 800 quote; -Pecuniaria da 400 a 1000 quote se prevista reclusione superiore a 5 anni; -Interdittiva art. 9 comma 2 .
<b>Riciclaggio</b>	Art.648-bis c.p.	-Pecuniaria da 200 a 800 quote; -Pecuniaria da 400 a 1000 quote se prevista reclusione superiore a 5 anni; -Interdittiva art. 9 comma 2 .
<b>Autoriciclaggio</b>	Art. 648-ter.1 c.p.	-Pecuniaria da 200 a 800 quote; -Pecuniaria da 400 a 1000 quote se prevista reclusione superiore a 5 anni; -Interdittiva art. 9 comma 2 .

Tabella 1.2: *La falsità in monete*

### 1.3.3 I reati societari e gli abusi di mercato

Per quanto concerne gli abusi di mercato la responsabilità amministrativa dell'ente a fronte delle diverse tipologie di reato disciplinate dagli art. 184 e 185 del TUF, è sancita dall'**articolo 25-sexies** del decreto 123/01. I reati societari, invece, sono presi in considerazione dall'**articolo 25-ter** ed hanno ad oggetto diversi ambiti di applicazione tra i quali assumono importanza particolare la formazione del bilancio, le comunicazioni esterne, determinate operazioni di capitale e l'ostacolo all'esercizio della vigilanza.

Si tratta di due fattispecie di reato strettamente connesse tra di loro e che il legislatore ha disciplinato introducendo due articoli al fine di garantire la trasparenza, l'integrità, la correttezza e l'efficienza del contesto economico nel quale partecipano i diversi operatori di mercato. Nello specifico è stato ritenuto necessario garantire il principio in base al quale tutti i soggetti economici debbono operare in condizioni di uguaglianza sotto il profilo dell'accesso all'informazione e della conoscenza delle informazioni pubbliche.

Nella tabella sottostante si elencano i reati disciplinati dall'articolo 25-sexies del decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>Illecita influenza sull'assemblea</b>	Art 2636 c.c.	-Pecuniaria da 150 a 330 quote.
<b>Aggiotaggio</b>	Art. 2637 c.c	-Pecuniaria da 200 a 500 quote.
<b>Falso in prospetto</b>	Art. 173-bis D.lgs 58/1998	-Pecuniaria da 200 a 330 quote.
<b>Abuso di informazioni privilegiate</b>	Art. 184 TUF	-Pecuniaria da 400 a 1000 quote.
<b>Manipolazione di mercato</b>	Art. 185 TUF	-Pecuniaria da 400 a 1000 quote.

Tabella 1.3: *Gli abusi di mercato*

Considerando l'attività svolta dalla banca, particolare attenzione va data al cosiddetto abuso di mercato per il quale i rischi maggiori legati alla commissione di illeciti si manifestano quando vengono diffuse notizie false o fuorvianti ovvero vengono utilizzate a scopo personale informazioni privilegiate. In situazioni di questo tipo e in presenza di operazioni che fanno sospettare la commissione di un illecito rientrante in questa categoria, esiste un obbligo di segnalazione per l'intermediario finanziario così come previsto dall'articolo 187-nonies del TUF.

Per quanto riguarda le attività criminali legate ai reati societari e con particolare riferimento all'operatività bancaria, si ricorda che la banca stessa si trova in una posizione assai privilegiata relativamente alla prevenzione e alla corretta attuazione dei precetti normativi in quanto è sottoposta ad una disciplina speciale che prevede una serie di obblighi ed adempimenti in relazione ai rapporti con le diverse autorità di vigilanza.

Nella tabella sottostante, invece, si elencano i reati disciplinati dall'articolo 25-ter del decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>False comunicazioni sociali</b>	Art 2621 c.c. e art. 2622 c.c.	-Pecuniaria da 200 a 400 quote; art. 2621; -Pecuniaria da 400 a 600 quote art. 2622.
<b>Falsità nelle relazione della società di revisione</b>	Art. 27 D.lgs 39/2010	-Pecuniaria da 100 a 130 quote.
<b>Impedito controllo</b>	Art. 2625 comma 2 c.c.	-Pecuniaria da 100 a 180 quote.
<b>Indebita restituzione dei conferimenti</b>	Art. 2626 c.c.	-Pecuniaria da 100 a 180 quote.
<b>Illegale ripartizione degli utili e delle riserve</b>	Art. 2627 c.c.	-Pecuniaria da 100 a 130 quote.
<b>Illecite operazioni su azioni o quote sociali</b>	Art. 2628 c.c.	-Pecuniaria da 100 a 180 quote.
<b>Operazioni in pregiudizio dei creditori</b>	Art. 2629 c.c.	-Pecuniaria da 150 a 330 quote.
<b>Ommessa comunicazione del conflitto di interessi</b>	Art. 2629-bis c.c.	-Pecuniaria da 200 a 500 quote.
<b>Formazione fittizia del capitale</b>	Art. 2632 c.c.	-Pecuniaria da 100 a 180 quote.
<b>Indebita ripartizione dei beni sociali</b>	Art. 2633 c.c.	-Pecuniaria da 150 a 330 quote.

Tabella 1.4: *I reati societari*

### 1.3.4 I reati informatici, contro l'industria e contro il commercio

Il rischio informatico rappresenta per le aziende e soprattutto per gli enti come gli istituti bancari uno dei rischi più temuti e più pericolosi in quanto oltre a creare un danno economico, può portare all'interruzione dell'attività e dei servizi offerti alla clientela.

Oggi giorno la maggior parte delle aziende e degli enti è dotata di computer connessi alla rete e il patrimonio aziendale è integralmente dematerializzato. Risulta pertanto necessario salvaguardare tutte quelle informazioni di natura economica e strategica e rendere sicura l'operatività aziendale riducendo il più possibile il rischio di subire un attacco informatico da parte di soggetti esterni all'impresa.

Infatti, subire un reato informatico comporta un triplice danno in quanto l'azienda da un lato deve sostenere un costo per cercare di riattivare o sostituire le risorse colpite e dall'altro deve far fronte ad una riduzione del patrimonio informatico aziendale. Infine l'impresa o l'ente che ha subito un reato informatico deve sostenere un costo, di difficile determinazione, per far fronte al danno di immagine.

Dal punto di vista giuridico la sensibilità legislativa per quanto riguarda il tema dei delitti informatici inizia con la pubblicazione in Gazzetta Ufficiale della legge 18 marzo 2008, n. 48. Si tratta di una normativa il cui obiettivo è quello di promuovere la cooperazione tra i vari Stati del mondo al fine di contrastare e ridurre il più possibile la diffusione di reati che arrecano danni informatici. La riforma della disciplina della criminalità informatica

oltre a modificare il codice penale e il codice di procedura penale, introduce nel decreto legislativo 231 del 2001 nuove fattispecie di reato informatico e di trattamento illecito di dati. Nello specifico l'articolo 7 della suddetta legge aggiunge al decreto studiato l'**articolo 24-bis** che elenca una serie di reati informatici che possono dar luogo alla responsabilità amministrativa degli enti. Per quanto riguarda le modifiche del codice penale e del codice di procedura penale queste sono state introdotte con l'obiettivo essenziale di agevolare le indagini e tutte quelle operazioni di perquisizione e sequestro dei dati informatici. Le Autorità competenti, infatti, sono tenute ad adottare misure tecniche volte ad assicurare la conservazione dei dati originali ed ad impedirne la loro alterazione<sup>21</sup>.

Nella tabella sottostante si elencano i reati disciplinati dall'articolo 24-bis decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>Accesso abusivo ad un sistema telematico o informatico</b>	Art. 615-ter c.p.	-Pecuniaria da 100 a 500 quote; -Interdittiva art. 9 comma 2, lettere a), b) ed e).
<b>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche</b>	Art. 617-quater e art. 617-quinquies c.p.	-Pecuniaria da 100 a 500 quote; -Interdittiva art. 9 comma 2, lettere a), b) ed e).
<b>Danneggiamento di informazioni, dati e programmi informatici</b>	Art. 653-bis e 635-ter c.p.	-Pecuniaria da 100 a 500 quote; -Interdittiva art. 9 comma 2, lettere a), b) ed e).
<b>Danneggiamento di sistemi informatici o telematici</b>	Art. 635-quarter e 635-quinquies c.p.	-Pecuniaria da 100 a 500 quote; -Interdittiva art. 9 comma 2, lettere a), b) ed e).
<b>Detenzione o diffusione abusiva di codici di accesso</b>	Art. 615-quarter e 615-quinquies c.p.	-Pecuniaria fino a 300 quote; -Interdittiva art. 9 comma 2, lettere b) ed e).
<b>Falsità di documenti informatici</b>	Art. 419-bis c.p.	-Pecuniaria fino a 400 quote; -Interdittiva art. 9 comma 2, lettere c), d) ed e).
<b>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica</b>	Art. 640 quinquies c.p.	-Pecuniaria fino a 400 quote; -Interdittiva art. 9 comma 2, lettere c), d) ed e).

Tabella 1.5: *I reati informatici*

Per quanto riguarda i reati contro l'industria e il commercio questi sono disciplinati dall'**articolo 25-bis 1**. Questo particolare articolo è stato introdotto nel decreto a seguito dell'entrata in vigore della legge 23 luglio 2009 n. 99 (disposizioni per lo sviluppo e l'internazionalizzazione delle imprese), pubblicata sul supplemento ordinario 136 della Gazzetta

<sup>21</sup>Le autorità competenti, a seguito dell'integrazione dell'articolo 132 del codice della privacy, possono ordinare ai fornitori e agli operatori di servizi informatici di conservare per un periodo, non superiore ai 6 mesi, i dati relativi al traffico telematico.

Ufficiale n. 176 del 31 luglio 2009. Nello specifico detta legge ha inserito nel corpo del decreto 231/01 numerose norme penali dalla stessa emanate o riformulate.

Nella tabella sottostante si elencano i reati disciplinati dall'articolo 25-bis 1 decreto 231/01:

REATO	RIFERIMENTO	SANZIONE
<b>Contraffazione o alterazione di marchi di prodotti industriali</b>	Art. 473 c.p.	-Pecuniaria fino a 500 quote.
<b>Commercio nello Stato di prodotti con segni falsi</b>	Art. 474 c.p.	-Pecuniaria fino a 500 quote.
<b>Turbata libertà dell'industria e del commercio</b>	Art. 513 c.p.	-Pecuniaria fino a 500 quote.
<b>Illecita concorrenza</b>	Art. 513-bis c.p.	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Frodi contro le industrie nazionali</b>	Art. 514 c.p.	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Frode nell'esercizio del commercio</b>	Art. 515 c.p.	-Pecuniaria fino a 500 quote.
<b>Vendita di sostanze alimentari non genuine</b>	Art. 516 c.p.	-Pecuniaria fino a 500 quote.
<b>Vendita di prodotti industriali con segni mendaci</b>	Art. 517 c.p.	-Pecuniaria fino a 500 quote.
<b>Fabbricazione di beni realizzati usurpando titoli di proprietà industriale</b>	Art. 517-ter c.p.	-Pecuniaria fino a 500 quote.
<b>Contraffazioni di prodotti agroalimentari</b>	Art. 517-quater c.p.	-Pecuniaria fino a 500 quote.
<b>Immissione abusiva in rete di opere protette</b>	Art. 171, comma 1 lettera a-bis, legge 633/1941	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Uso abusivo aggravato di opere protette</b>	Art. 171, comma 3, legge 633/1941	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Abusi concernenti software e banche dati</b>	Art. 171-bis, legge 633/1941	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Abusi concernenti opere audiovisive o letterarie</b>	Art. 171-ter, legge 633/1941	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.
<b>Omesse o false comunicazioni SIAE</b>	Art. 171-septies, legge 633/1941	-Pecuniaria fino a 800 quote; -Interdittiva art. 9 comma 2.

Tabella 1.6: *I reati contro l'industria e il commercio*

Si tratta di precetti che hanno come scopo principale quello di punire condotte truffaldine a danno del sistema economico e del sistema di scambi commerciali.

Questa fattispecie di illecito può essere commessa da tutti quei soggetti che svolgono una qualsiasi attività commerciale e il reato si configura nel momento in cui viene consegnato



o scambiato un oggetto avente natura diversa rispetto a quella pattuita per provenienza, origina o qualità.

### 1.3.5 I reati con finalità di terrorismo e di criminalità organizzata

Relativamente al sistema della responsabilità amministrativa degli enti, nel corso degli anni, sono state introdotte diverse classi di illeciti il cui obiettivo comune è quello di contrastare fenomeni di criminalità che suscitano particolare allarmismo a livello nazionale ed internazionale. Nel caso specifico ci si riferisce a reati che possono avere natura politico-terroristica oppure legata al settore della criminalità organizzata. Negli ultimi decenni il settore bancario ha dedicato particolare attenzione alla salvaguardia del sistema cercando di prevenire da un lato i fenomeni criminali che possono manifestarsi nel mercato finanziario e dall'altro contrastando fenomeni di terrorismo. Con riguardo al tema dei reati con finalità di terrorismo, il decreto 231/01 ne dà regolamento all'**articolo 25-quater**, introdotto dalla legge 7/2003 di ratifica ed esecuzione delle Convenzione internazionale per la repressione del finanziamento del terrorismo, adottata il 9 dicembre 1999 dall'assemblea generale delle nazioni unite, a New York. Si tratta di una norma particolare in quanto, a differenza degli altri articoli del decreto, in questo caso non vi è un elenco dettagliato e preciso delle fattispecie di reato; l'articolo, infatti si riferisce ad un qualsiasi reato penale che sia caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico commesso dal soggetto agente<sup>22</sup>. A tal proposito possiamo individuare 2 macro aree:

- **A) Delitti con finalità di terrorismo o eversione dell'ordine democratico**

Rientrano in questa categoria tutte le tipologie di reato che portano movente politico e cioè contro la personalità interna ed internazionale dello Stato, contro i diritti politici del cittadino ovvero contro gli Stati esteri e i loro capi. Per quanto concerne la responsabilità degli enti e nello specifico lo svolgimento dell'attività bancaria potrebbero manifestarsi le seguenti fattispecie di reato:

- Finanziamento di condotte con finalità di terrorismo;
- Sottrazione di beni o denaro sottoposti a sequestro;
- Partecipazione a prestiti a favore del nemico;

---

<sup>22</sup>L'art. 270-sexies del c.p. considera finalità di terrorismo tutte quelle condotte che possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e che sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici a compiere o ad astenersi dal compiere un qualsiasi atto, o di destabilizzare le strutture politiche fondamentali, costituzionali, economiche e sociali, nonché le altre condotte previste da norme internazionali. Secondo la giurisprudenza, Cassazione penale. n. 39504/2008, l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

- Sequestro di persona a scopo di terrorismo o di eversione;
- Associazioni con finalità di terrorismo o eversione dell'ordine democratico.
- **B) Delitti con finalità di terrorismo previsti dalla Convenzione di New York del 9 dicembre 1999**

**L'articolo 25-quater, al comma 4**, richiama tale convenzione con l'obiettivo principale di evitare possibili lacune in quanto con essa si promuove la cooperazione e la collaborazione internazionale per la repressione di condotte di raccolta di finanziamenti, in qualunque forma, destinati ad atti di terrorismo in genere. In particolare l'attenzione cade sui reati che possono causare un danno patrimoniale, come il riciclaggio o l'impiego di denaro di provenienza illecita, che vengono commessi esclusivamente con finalità di terrorismo o eversione dell'ordine democratico.

In merito alle sanzioni applicate all'ente l'articolo in questione prevede quanto segue:

- a) Se il delitto è punito con la pena della reclusione inferiore ai 10 anni, la sanzione pecuniaria varia da 200 a 700 quote;
- b) Se il delitto è punito con la pena della reclusione non inferiore a 10 anni o con l'ergastolo, la sanzione pecuniaria varia da 400 a 1000 quote.

Sono previste, inoltre, sanzioni interdittive disciplinate dall'articolo 9 comma 2, per una durata non inferiore all'anno. Se, invece, l'ente o una sua unità organizzativa, viene stabilmente utilizzato con lo scopo unico o prevalente di consentire o agevolare la commissione dei reati con finalità di terrorismo o eversione dell'ordine democratico, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività così come stabilito ai sensi dell'articolo 16 comma 3.

Relativamente ai delitti di criminalità organizzata il decreto 231/01 tratta la questione all'**articolo 24-ter**. Questo articolo è stato introdotto dalla legge 94/2009 e suddivide i reati di criminalità organizzata in quattro tipologie differenti:

- Associazione per delinquere generica (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-bis e 416-ter);
- Associazione per delinquere finalizzata alla commissione di delitti in tema di schiavitù, di tratta di persone e di immigrazione clandestina (art. 416 c.p.);
- Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti (art. 74 DPR 309/1990).

In merito al tema affrontato in questo lavoro va sottolineato il fatto che la sola cosciente partecipazione ad una associazione criminosa da parte di un dipendente dell'ente o di un suo esponente potrebbe determinare la responsabilità amministrativa dell'ente stesso, purché la partecipazione all'associazione risulti funzionale all'interesse dell'ente oppure al perseguimento di un vantaggio per il medesimo.

L'articolo in questione si riferisce anche ad una categoria di delitti molto più generica, di qualsiasi tipo, commessi avvalendosi del metodo mafioso a con lo scopo primario di favorire un'associazione mafiosa. La prima fattispecie di illeciti si verifica quando un soggetto pone in essere una condotta intimidatoria avvalendosi del nome di organizzazioni criminali operanti in un territorio ben circoscritto. La seconda circostanza di reati si verifica quando un soggetto agisce con l'obiettivo di agevolare una qualsiasi attività di stampo mafioso.



## 1.4 L'attuazione delle sanzioni

Il decreto legislativo 231/01, all'articolo 34, stabilisce che le sanzioni amministrative siano attuate tenendo in considerazione quanto stabilito dal codice di procedura penale, purché compatibile. Quando un ente viene condannato la fase di attuazione delle sanzioni è suddivisa in due momenti: il primo, considerato come necessario, fa riferimento all'efficienza di quanto stabilito in sentenza, il secondo, considerato come eventuale, è legato alla verifica riguardo la "fungibilità" della sanzione. Tuttavia si osserva che relativamente al primo momento possono verificarsi situazioni che rendono impossibile l'applicazione delle sanzioni (basti pensare a modificazioni subite dall'ente o al venir meno dell'oggetto della sanzione interdittiva), mentre per quanto riguarda il secondo momento sono previste vie di fuga che consentono all'ente la conversione delle sanzioni<sup>23</sup>. Per quanto riguarda la concreta esecuzione delle sanzioni, analogamente a quanto previsto per l'esecuzione penale ai sensi dell'articolo 655 c.p.p., spetta al giudice penale competente conoscere gli illeciti amministrativi dell'ente, sulla base di quanto stabilito dall'articolo 36. Tale articolo, al secondo comma, afferma altresì che per il procedimento di accertamento dell'illecito si devono osservare le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende. Quando il pubblico ministero acquisisce la notizia dell'illecito amministrativo è tenuto ad annotare il fatto nel registro di cui all'articolo 355 del codice di procedura penale. Inoltre, in tale registro devono essere annotati gli elementi identificativi dell'ente unitamente alla generalità del suo legale rappresentante, se possibile<sup>24</sup>. Una volta annotato e accertato l'illecito, il pubblico ministero ne deve dare contestazione<sup>25</sup> all'ente sulla base degli atti indicati dall'articolo 405, comma 1, del codice di procedura penale. Nello specifico la contestazione deve riportare gli elementi identificativi dell'ente e l'enunciazione, in forma chiara e precisa, che il fatto può comportare l'applicazione di sanzioni amministrative: articolo 59 del decreto legislativo<sup>26</sup>. La contestazione dell'illecito amministrativo all'ente avviene mediante notifica ai sensi dell'articolo 154, comma 3, del codice di procedura penale. Sono da ritenersi in ogni caso valide le notifiche eseguite attraverso consegna al legale rappresentante anche se lo stesso è imputato del reato. Una volta conclusa la fase di raccolta delle informazioni e la relativa notifica all'ente si può procedere con l'apertura del dibattito. In questo lasso di tempo che va dalla notifica all'apertura del procedimento l'ente può chiedere al giudice competente di disporre la sospensione del processo se è in grado di dar corso alle attività previste dall'articolo 17 (riparazione delle conseguenze del reato). In questo caso, se il giu-

<sup>23</sup>In questo caso ci si riferisce a quanto stabilito dall'articolo 17 del decreto.

<sup>24</sup>Questo in base all'articolo 55 il quale stabilisce che l'annotazione sia comunicata all'ente o al suo difensore che ne faccia richiesta.

<sup>25</sup>La contestazione non è prevista nel caso in cui il reato sia estinto per prescrizione.

<sup>26</sup>Se non si procede con la contestazione, il pubblico ministero emette decreto motivato di archiviazione degli atti, comunicandolo al procuratore generale presso la corte d'appello. Il procuratore può, tuttavia, svolgere gli accertamenti del caso e, se ricorrono le condizioni, contestare all'ente le violazioni amministrative conseguenti al reato entro sei mesi dalla comunicazione.

dice accoglie la richiesta, può impartire all'ente il pagamento di una somma di denaro a titolo di cauzione<sup>27</sup>.

Nel momento in cui prende avvio il procedimento, l'ente vi partecipa con il proprio rappresentante legale purché lo stesso non sia imputato nel reato considerato. La partecipazione al procedimento richiede che l'ente depositi presso la cancelleria dell'autorità giudiziaria competente, una dichiarazione contenente i seguenti dati:

- a) La denominazione dell'ente e le generalità del suo legale rappresentante;
- b) Il nome ed il cognome del difensore e l'indicazione della procura;
- c) La sottoscrizione del difensore;
- d) La dichiarazione o l'elezione del domicilio<sup>28</sup>.

Infine se il legale rappresentante non compare, l'ente costituito è rappresentato dal difensore e in caso di mancanza è assistito da un difensore d'ufficio<sup>29</sup>.

Relativamente alla sentenza di condanna emessa dal giudice, possono verificarsi situazioni differenti:

- **Esclusione delle responsabilità dell'ente se l'illecito non sussiste:** il giudice in questo caso ne dichiara il motivo e la causa nella sentenza. È esclusa inoltre la responsabilità nel momento in cui la prova dell'illecito amministrativo manca, è insufficiente oppure contraddittoria.
- **Sentenza di non doversi procedere:** questo si verifica quando la sanzione o il reato da cui dipende l'illecito si sono estinti per prescrizione.
- **Responsabilità dell'ente:** il giudice applica le sanzioni previste dalla legge e condanna l'ente al pagamento delle spese processuali<sup>30</sup>.
- **Vicende modificative dell'ente:** in caso di trasformazione, fusione o scissione, il giudice dichiara che la sentenza è pronunciata nei confronti degli enti risultanti da trasformazione o fusione ovvero beneficiari della scissione, indicando l'ente originariamente responsabile.

La sentenza di condanna deve essere pubblicata a spese dell'ente osservando le disposizioni di cui all'articolo 694, commi 2,3 e 4 del codice di procedura penale. Nello specifico il direttore e il vice direttore del giornale designato sono tenuti a pubblicare la sentenza se la richiesta perviene dal giudice o da persona autorizzata.

Con riguardo all'esecuzione delle sanzioni amministrative va osservato quanto segue:

---

<sup>27</sup> Articolo 65 del decreto.

<sup>28</sup> Articolo 39 del decreto.

<sup>29</sup> Questo in base all'articolo 40.

<sup>30</sup> Se trovano applicazione le sanzioni interdittive, nel testo della sentenza si devono indicare l'attività o le strutture oggetto della sanzione.

- Nel caso di **sanzioni pecuniarie** trova applicazione quanto stabilito dall'articolo 200 e successivi, del D.P.R. del 30 maggio 2002, il quale ha abrogato l'articolo 75 del decreto 231/01. In particolare il pagamento deve essere eseguito entro un mese dalla irrevocabilità della sentenza, decorso il quale si dovrà procedere alla riscossione a mezzo dei ruoli esattoriali. Tuttavia se l'ente si trova in temporanea difficoltà ha facoltà di chiedere sia la rateizzazione di quanto dovuto, con un massimo di sessanta rate mensile, sia la sospensione del pagamento. Una disciplina particolare e specifica è invece prevista per tutti quegli illeciti derivanti da abusi di mercato: in questo caso, infatti, trovano applicazione sanzioni pecuniarie ulteriori rispetto a quelle di "base".
  
- Nel caso di **sanzioni interdittive** l'esecuzione è disciplinata dall'articolo 77 in base al quale l'organo competente all'attuazione delle stesse è il pubblico ministero. Il magistrato è tenuto a darne notifica all'ente attraverso un estratto contenente l'indicazione delle attività e delle strutture oggetto della sanzione. In caso di interdizioni parziali su singoli contratti o attività, il giudice competente dovrà nominare un perito che determinerà le attività ed i settori nei quali l'ente potrà operare. Infine, con l'obiettivo di garantire il conseguimento della legalità quale primo risultato prefissato dal decreto, vi sono situazioni particolari che consentono all'ente di convertire le sanzioni interdittive. In virtù dell'articolo 78 al comma 1, l'ente che ha posto in essere tardivamente le condotte di cui all'articolo 17, può richiedere la conversione della sanzione interdittiva in sanzione pecuniaria. Tale conversione, tuttavia, non è possibile nel caso in cui siano state applicate sanzioni interdittive in via definitiva così come stabilito dall'articolo 16 al comma 3. La richiesta di conversione, motivata e contenente le ragioni di tale tardività, dovrà essere presentata al giudice *in executivis* entro venti giorni dalla notificazione dell'estratto della norma. Ricevuta la richiesta di conversione, il giudice, entro i dieci giorni successivi, fissa l'udienza in camera di consiglio ed esprimerà il proprio parere circa l'ammissibilità della richiesta; se la richiesta non presenta elementi ostativi si procede alla sospensione dell'esecuzione della sanzione attraverso decreto motivato revocabile. In caso di accoglimento la sanzione interdittiva verrà convertita in sanzione pecuniaria che si aggiungerà a quella già assegnata con sentenza di condanna. Va precisato che l'importo della sanzione stabilito dalla conversione non potrà essere inferiore né superiore al doppio della sanzione pecuniaria ordinaria in quanto la normativa ha come obiettivo quello di non incentivare condotte strumentali dell'ente. Infatti il giudice nel momento in cui determina l'importo dovrà tener conto da un lato della gravità dell'illecito commesso e dall'altro le ragioni che hanno determinato il tardivo adempimento delle condotte di cui all'articolo 17. Operando in tal senso il giudice distingue i casi di reale difficoltà nell'adempiere tempestivamente da quelli che evidenziano la volontà dell'ente di ritardare il più possibile l'adempimento di quanto dovuto.

Infine può sopraggiungere la necessità di disporre il commissariamento dell'ente nel caso in cui si verifichi una delle condizioni previste dall'articolo 15. In situazioni di questo tipo il giudice indicherà i compiti ed i poteri che spettano al commissario chiamato a proseguire l'attività dell'ente<sup>31</sup>. Spetta poi al commissario porre in essere tutte quelle attività atte a prevenire la commissione di reati della stessa specie di quello verificatosi e a compiere funzioni di straordinaria amministrazione, se autorizzato dal giudice. Il commissario, in virtù di quanto stabilito dall'articolo 79 al secondo comma, deve riferire ogni tre mesi, al giudice di esecuzione e al pubblico ministero, sull'andamento della gestione e, terminato l'incarico, trasmettere una relazione dettagliata in merito all'attività svolta. L'eventuale profitto ottenuto dal commissario durante l'esercizio delle sue funzioni verrà confiscato dal giudice con le forme dell'articolo 667 comma 4 del c.p.p. al fine di evitare che l'ente possa addirittura trarre vantaggio a seguito della sanzione interdittiva. Infine l'ente è tenuto a pagare ogni spesa relativa all'attività svolta dal commissario nonché il suo compenso che, visto il silenzio della norma, sarà stabilito direttamente dal giudice dell'esecuzione.

---

<sup>31</sup>La normativa non si esprime per quanto concerne un'eventuale revoca o sostituzione del commissario che non adempia al proprio mandato in modo idoneo. La dottrina ritiene che tale potere spetti al giudice esecutivo.



## Capitolo 2

# L'attività bancaria: Mog, Odv e sistema di segnalazioni

Con riferimento all'attività bancaria, l'autorità di vigilanza preposta, ha posto in essere un sistema di controlli che influenza e coinvolge una serie di soggetti diversi. Sindaci, società di revisione, ufficio controlli, internal auditing devono sempre più interagire fra di loro, seguendo le disposizioni contenute nelle istruzioni di vigilanza, con l'obiettivo di dotare la banca di procedure e strutture atte a garantire il principio della sana gestione che rappresenta il cuore di quanto normato dal decreto 231 del 2001.

Per raggiungere questo obiettivo gli istituti di credito devono operare in modo tale da garantire la separatezza tra mansioni operative e mansioni di controllo, misurare e identificare tutti i rischi che si possono assumere, adottare sistemi di informazione sicuri e in grado di riferire qualsiasi anomalia riscontrata nello svolgimento dell'attività bancaria nonché attuare controlli su ogni livello operativo.

Nel caso specifico, le banche danno vita ad una rete di controlli e verifiche che può essere benissimo utilizzata per la prevenzione di reati, compresi quelli individuati dal decreto 231 del 2001. Si tratta, tuttavia, di un sistema che deve essere costantemente monitorato e, se del caso, aggiornato e modificato al fine di stare al passo con lo sviluppo del mercato economico.

Per dar vita a questo complesso sistema di controlli, in grado di prevenire la commissione di illeciti disciplinati dal decreto in esame, monitorando l'operatività bancaria in ogni settore e livello operativo, le banche adottano uno o più modelli di organizzazione.

## 2.1 Il modello di organizzazione, gestione e controllo

Il decreto 231 del 2001 oltre a disciplinare la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato, così come stabilito dall'articolo 1, prevede anche che gli stessi adottino modelli di organizzazione che abbiano come scopo quello di prevenire i misfatti<sup>1</sup>.

I modelli in questione si possono definire come un insieme di norme, regole comportamentali, strutture organizzative e procedure operative, finalizzato a garantire lo svolgimento dell'attività della società nel rispetto della legge, individuando ed eliminando in maniera tempestiva le situazioni di rischio.

I modelli, in modo particolare, devono rispettare determinate **caratteristiche** e rispondere a particolari **esigenze**:

- a) Identificare le aree cosiddette sensibili, ossia le attività nel cui dominio possono essere commessi gli illeciti;
- b) Prevedere protocolli specifici volti a programmare l'attuazione delle decisioni dell'ente;
- c) Stabilire come impiegare le risorse disponibili volte ad impedire la commissione del crimine;
- d) Prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
- e) Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello<sup>2</sup>.

In base poi all'ordinanza 4728 del Gip del Tribunale di Milano *"...il modello organizzativo deve scaturire da una visione realistica ed economica dei fenomeni aziendali; il modello deve dunque necessariamente tener conto della storia della società alla quale si riferisce in quanto l'analisi della stessa è indispensabile per l'individuazione dei cosiddetti fattori di rischio;...deve necessariamente tener conto della specificità dell'ente"*.

---

<sup>1</sup>Al riguardo la legge regionale n. 15/2008, collegata alla manovra finanziaria regionale della Calabria, sancisce l'obbligo di adozione dei modelli previsti dal Decreto 231/2001 per le imprese che operano in regime di convenzione con la Regione. La Regione Calabria, fortemente a rischio per i numerosi casi di infiltrazione della criminalità organizzata, ha voluto promuovere la trasparenza delle realtà imprenditoriali che, in un contesto pubblico, forniscono servizi ai cittadini.

<sup>2</sup>Questo è previsto dall'articolo 6 del decreto. In base a tale articolo i modelli in questione possono essere adottati sulla base di codici di comportamento redatti da associazioni rappresentative degli enti e comunicati al ministero della giustizia che, di concerto con i ministeri competenti, entro 30 giorni può formulare osservazioni sulla idoneità dei modelli stessi. Sulla base di ciò nel corso degli anni sono state emanate diverse linee guida da parte di associazioni di categoria. Si pensi alle linee guida di Confindustria approvate nel marzo del 2002 ovvero alle linee guida di ABI o dell'ANIA.

Infatti, analizzare la storia dell'ente e dei suoi trascorsi, anche giudiziari, può risultare importante al fine di stabilire i reati che possono essere commessi con facilità maggiore all'interno della società.

Infine i modelli organizzativi devono essere sottoposti anche ad un *“progressivo aggiornamento per garantire il costante adeguamento a sopravvenuti mutamenti operativi, organizzativi e normativi”*<sup>3</sup>. Nello specifico l'aggiornamento costante dei modelli deve avvenire secondo le disposizioni e le segnalazioni pervenute da parte dell'organismo di vigilanza o di un altro organo di controllo, in virtù delle variazioni organizzative o normative (come ad esempio può essere l'introduzione di un nuovo reato presupposto) o di qualsiasi altro evento che influenzi l'attività dell'ente.

Per quanto concerne la **struttura e il contenuto** del modello organizzativo, secondo quanto stabilito dalle disposizione del decreto legislativo, è necessario riscontrare i seguenti elementi:

- **Codice etico e di comportamento:** il modello adottato deve contenere i principi e i valori su cui si fonda la cultura e la filosofia aziendale nonché le principali regole comportamentali che ogni dipendente deve rispettare durante lo svolgimento delle proprie mansioni e nei rapporti con interlocutori interni ed esterni all'ente stesso;
- **Procedure organizzative preventive:** il modello deve definire i comportamenti operativi legati ai processi aziendali inclusi i controlli procedurali su attività ritenute sensibili ad eventuali condotte illecite;
- **Sistema delle deleghe e firme autorizzate:** il modello determina l'organizzazione aziendale per quel che riguarda la struttura, le attività e i soggetti responsabili rispettando il principio di separazione funzionale e di contrapposizione degli interessi; inoltre il modello determina chi è titolare di poteri aziendali e a chi sono state attribuite deleghe, sempre nel rispetto del principio di separazione delle responsabilità;
- **Sistema disciplinare:** il modello determina le sanzioni che possono essere comminate a tutti coloro che violano le norme aziendali;
- **Piano di formazione e comunicazione:** il modello adottato deve identificare le attività di comunicazione a tutti coloro che sono portatori d'interesse delle norme principali che compongono il modello stesso. L'obiettivo è quello di sensibilizzare, da un lato il rischio della commissione di reati e dall'altro promuovere la trasparenza per quel che concerne i comportamenti ritenuti corretti dalla filosofia manageriale;
- **Funzione e operatività dell'organismo di vigilanza:** il modello deve identificare il soggetto preposto a vigilare sull'osservanza e sul funzionamento di quanto in esso stabilito.

---

<sup>3</sup>Ordinanza del Tribunale di Napoli del 26/06/2007.

Si tratta di contenuti necessari che devono essere inclusi nel modello di organizzazione che verrà adottato dall'ente altrimenti lo stesso non potrà considerarsi idoneo a prevenire i reati previsti dal decreto 231/01.

Il modello, inoltre, deve indicare al suo interno una sezione che indichi come l'ente è strutturato ed organizzato. Nello specifico il modello deve riportare il sistema di governance dell'ente, il sistema di controllo adottato e deve indicare chi detiene i poteri di firma e autorizzativi all'interno dello stesso<sup>4</sup>. Relativamente al sistema di governance il modello deve indicare qual'è l'organo sociale dell'ente, la sua composizione, durata e competenze nonché chi detiene i poteri di rappresentanza. È necessario che il sistema di governance sia chiaro e aggiornato con indicazione specifica dei compiti e delle mansioni che i vari soggetti devono svolgere all'interno dell'ente.

Per quanto riguarda il sistema di controllo in base alla tipologia dell'ente e all'organizzazione dello stesso si possono individuare 3 livelli di controllo differenti:

- un **primo livello** che definisce i controlli di linea volti a garantire un corretto svolgimento delle diverse attività interne all'ente;
- un **secondo livello** che effettua un controllo sui rischi operativi;
- un **terzo livello** volto a individuare violazioni nelle procedure.

Si tratta di un sistema che deve rispettare determinati principi così come stabilito dalle linee guida di Confindustria:

- Ogni operazione deve essere verificabile, documentata, coerente e congrua;
- Nessuno può gestire in autonomia un intero processo. Ciò significa che nessun soggetto è dotato di poteri illimitati, le diverse funzioni devono essere tra di loro separate<sup>5</sup>, i poteri devono essere ben definiti e coerenti con le mansioni da svolgere;
- I controlli devono essere documentati.

Infine relativamente ai poteri di firma è preferibile che l'ente disponga un organigramma all'interno del quale indicare i poteri, le responsabilità, le deleghe e le procure che sono



Figura 2.1: **Contenuto del MOG**  
(Fonte: *Lentepubblica.it*)

<sup>4</sup>Si tratta di suggerimenti forniti direttamente dalle linee guida di Confindustria.

<sup>5</sup>Ad esempio chi autorizza un'operazione deve essere un soggetto diverso da colui che la contabilizza.

attribuite ai diversi soggetti. Tale schema deve essere costantemente aggiornato a seguito di cambiamenti interni all'azienda ovvero a seguito di cambiamenti normativi.

Come già accennato il modello organizzativo ha come **obiettivo** principale quello di dar vita ad una struttura integrata di principi, protocolli e procedure volte a prevenire il compimento di reati presupposto. In particolare la finalità del modello è quella di rendere l'ente non responsabile in caso di commissione di reati previsti dal decreto 231/01. I principali destinatari del modello e delle sue previsioni sono i dipendenti dell'ente, i componenti degli organi sociali e tutti quei soggetti che collaborano con l'ente per il conseguimento degli obiettivi stabiliti.

In merito alla **realizzazione** del modello, generalmente si possono individuare 5 fasi:

**1) Mappatura delle aree di rischio:**

In questa fase bisogna procedere con una scrupolosa analisi dei rischi connessi con l'attività svolta cercando, se possibile, di individuare le modalità con le quali possono essere commessi gli illeciti. Pertanto risulta fondamentale procedere prendendo in considerazione per prima cosa le diverse attività a rischio reato, successivamente individuare le possibili modalità con cui lo stesso può essere realizzato ed infine stabilire le misure di prevenzione da adottare.

**2) Valutazione del sistema di controllo interno:**

In questa fase viene analizzato il sistema di controlli interni applicato dalla banca e nello specifico si valuta chi detiene i poteri di firma e i poteri autorizzativi, si analizzano le regole comportamentali vigenti, si esamina il sistema di tracciabilità delle operazioni svolte all'interno della banca ed infine si individuano le varie funzioni aziendali per capire come sono in relazione tra di loro.

**3) Analisi comparativa e piani di miglioramento:**

Si tratta della fase principale in quanto si procede con l'organizzazione del modello, se ne determina il contenuto e si effettuano confronti con i risultati ottenuti nelle prime due fasi. L'obiettivo di questa fase è quello di creare il sistema portante del modello individuando i punti cardine di cui lo stesso si deve comporre.

**4) Redazione:**

Effettuate tutte le valutazioni richieste si procede in questa fase con la stesura del modello. In via del tutto generale il modello è solitamente composto in 3 parti:

- *una parte generale* contenente il codice etico, il regolamento dell'organismo di vigilanza e il sistema disciplinare;

- *una parte speciale* suddivisa solitamente per processi aziendali. In questa parte si individuano le cosiddette “*aree sensibili*” ovvero le aree ritenute a rischio di commissione del reato e si identificano gli “*standard di controllo*” ossia per ciascuna area sensibile si determinano procedure e protocolli di prevenzione;
- *una parte finale* nella quale si possono trovare particolari documenti da allegare al modello.

### 5) Diffusione:

Una volta compilato e approvato dall'organo dirigente il modello deve essere messo a conoscenza e a disposizione di tutti i dipendenti e collaboratori, interni ed esterni, dell'istituto. Si tratta di una fase estremamente importante in quanto l'obiettivo è quello di assicurare che i destinatari del modello siano a conoscenza delle procedure che devono seguire per poter eseguire in maniera corretta le proprie mansioni. Nello specifico la diffusione del modello deve essere tempestiva, accurata, accessibile a tutti e continua.

Riassumendo quanto sopra riportato, un modello di organizzazione si può considerare idoneo se strutturato così come indicato nella figura seguente:

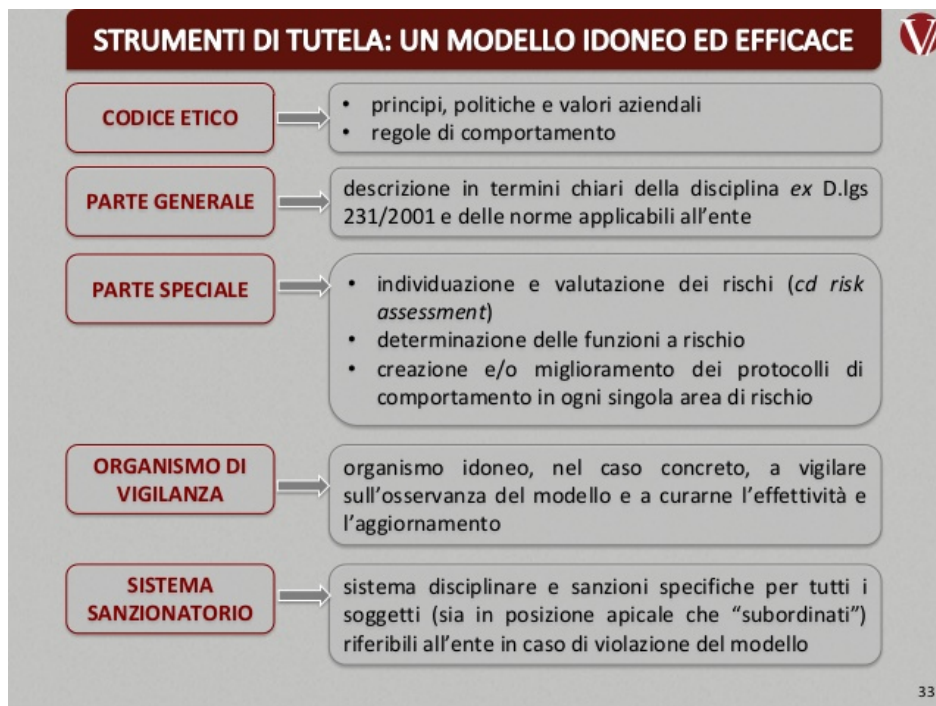


Figura 2.2: L'idoneità del MOG  
(Fonte: Slideshare.net)

Per ciò che concerne **l'attuazione** del modello, l'articolo 6 al comma 1, lettera a, stabilisce che spetta all'organo dirigente adottare in maniera efficace il modello di organizzazione e gestione. Si tratta di un dettato generico poiché il decreto in questione si riferisce ad una pluralità di soggetti: consiglio di amministrazione, amministratore unico, consiglio di gestione, top management (amministratore delegato e alta dirigenza). Si tratta di soggetti che in base al sistema organizzativo dell'ente sono più o meno interessati all'attuazione del modello. In particolare compiti specifici spettano al consiglio di amministrazione e al top management.

**L'organo dirigente** dal canto suo deve svolgere i seguenti compiti<sup>6</sup>:

- Approvare il modello e il codice etico;
- Esaminare le informazioni relative al contenuto del modello;
- Assicurare che siano assegnate risorse finanziarie adeguate per l'efficiente funzionamento del modello;
- Aggiornare, quando necessario, il modello.

Inoltre l'organo dirigente è tenuto come ogni altro soggetto che è coinvolto nell'attività dell'ente, a rispettare i principi e i dettati del modello.

**Il top management**, invece, deve garantire che tutti i poteri e le responsabilità attribuiti ai vari soggetti siano efficacemente comunicati a tutte le strutture interne dell'ente. Inoltre lo stesso deve<sup>7</sup>:

- Dirigere e supportare i dipendenti nel contribuire all'efficacia del modello;
- Promuovere la cultura in materia 231 all'interno dell'ente;
- Assicurarsi che il modello sia adottato e attuato in modo adeguato al fine di prevenire la commissione di reati presupposto;
- Promuovere il miglioramento continuo del modello;
- Incoraggiare l'uso di procedure di segnalazione di carenze e violazione del modello;
- Garantire che nessun soggetto in caso di segnalazioni, eseguite in buona fede e nel rispetto delle modalità stabilite, subisca ritorsioni o azioni discriminatorie;
- Riferire all'organo dirigente relativamente al contenuto del modello e a eventuali segnalazioni di commissione di reati presupposto;

---

<sup>6</sup>ITINERA, guide giuridiche ipsoa, "Responsabilità amministrativa degli enti" a cura di Francesco Sbisà pag. 61.

<sup>7</sup>ITINERA, guide giuridiche ipsoa, "Responsabilità amministrativa degli enti" a cura di Francesco Sbisà pag. 62.

- Riesaminare periodicamente il modello;
- Conservare prova documentale delle revisioni.

Con particolare riferimento al settore bancario per organo dirigente si intende senza ombra di dubbio il consiglio di amministrazione. Infatti è cura del consiglio di amministrazione o di un soggetto formalmente delegato, procedere con l'efficace attuazione del modello attraverso la valutazione e l'approvazione di tutte le misure idonee ad implementarlo ovvero a modificarlo se necessario. In modo particolare il consiglio di amministrazione, tenendo conto del sistema di controlli interni, delega quelle strutture che sono tenute ad attuare il modello e a sottoporlo a continuo aggiornamento a seguito dell'entrata in vigore di nuove normative ovvero dell'introduzione di nuove tipologie di reati presupposto. Il consiglio di amministrazione può stabilire di non dotare la banca di un modello di organizzazione e gestione dandone, in questo caso, specifica motivazione in modo tale da rendere questa scelta sorretta da una tesi plausibile che dimostri i punti di forza ed i benefici che ne derivano da quanto deciso.

Di conseguenza l'adozione del modello, per la banca<sup>8</sup>, è una facoltà e in quanto tale viene attuata con modalità differenti che variano da istituto a istituto. Infatti nel momento in cui si adotta un modello organizzativo, la banca deve tener conto delle proprie dimensioni, del territorio in cui opera, del tipo di clientela nonché del rapporto costi-benefici che il modello da adottare richiede. Inoltre spetta alla banca stessa stabilire con che modalità tecniche e che procedure utilizzare in fase di adozione del modello, con la conseguenza che tutto ciò che viene indicato e proposto dal decreto 231/01 risulta essere un mero suggerimento al quale gli istituti di credito e non solo, sono liberi di ispirarsi in sede di realizzazione del modello stesso.

Ciò nonostante va precisato che scegliere di non dotare l'ente, in questo caso specifico la banca, di un modello organizzativo può rappresentare un rischio per gli amministratori: infatti operando in questa direzione possono violare un dovere particolare legato all'adeguatezza dell'assetto organizzativo, amministrativo e contabile.

Nel caso in cui venga commesso un reato presupposto previsto dal decreto 231/01 la mancata adozione del modello da parte degli amministratori rileva sotto l'aspetto dell'inadempimento del dovere generale di assicurare e valutare l'adeguatezza degli assetti organizzativi di cui all'articolo 2381, commi 3 e 5 del codice civile.

Non adottare un modello potrebbe rappresentare un grosso rischio per gli amministratori in quanto è possibile imputare nei loro confronti una responsabilità per colpa organizzativa.

---

<sup>8</sup>L'adozione del modello non è un obbligo e quindi qualsiasi ente è libero di decidere se attuarlo oppure no.



3

TRIBUNALE MILANO  
SENTENZA 13 FEBBRAIO 2008  
N. 1774

Fattispecie

- ✓ Una società era stata sottoposta a indagini preliminari per mancata predisposizione di un adeguato modello organizzativo e aveva patteggiato e assolto una condanna al pagamento di una pena pecuniaria.
- ✓ L'amministratore delegato era stato processato per corruzione, truffa, turbativa d'asta, patteggiando una condanna a pena detentiva.

➔ Azione di responsabilità in sede civile della società nei confronti del suo amministratore delegato (*ex art. 2392 c.c.*), volta a far valere la responsabilità del medesimo per inadeguata attività amministrativa e la conseguente condanna al risarcimento dei danni subiti dalla società medesima.

MDA  
AVVOCATI ASSOCIATI D'IMPRESA

Figura 2.3: **Sentenza del Tribunale di Milano**  
(Fonte: *Slideplayer.it*)

A tal proposito la dottrina ha evidenziato le implicazioni in tema di corporate governance dell'adozione di modelli organizzativi i quali sono aggiunti alle norme che disciplinano il principio di adeguatezza nella gestione di una società<sup>9</sup>.

In particolare le norme di riferimento sono le seguenti:

- **L' articolo 2381, comma 5, c.c.**, ai sensi del quale gli organi delegati curano che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa e riferiscono al consiglio di amministrazione e al collegio sindacale sul generale andamento della gestione, sulla sua prevedibile evoluzione e sulle operazioni di maggior rilievo. Il consiglio di amministrazione valuta l'adeguatezza del suddetto assetto sulla base delle informazioni ricevute.
- **L' articolo 2403, comma 1, c.c.**, ai sensi del quale il collegio sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e, in particolare, sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento.

<sup>9</sup>D'ARCANGELO F., I canoni di accertamento dell'idoneità nel MOG, in *Rivista* 231, 02-2011.

Sulla base di queste norme, in tema di adeguatezza organizzativa, viene ricostruito il cosiddetto “*dovere esplicito*” di adottare misure idonee a prevenire la commissione di reati presupposto e ad evitare l'insorgere della responsabilità amministrativa dell'ente<sup>10</sup>.

In via del tutto generale e sulla base di quanto stabilito dal decreto, il modello deve essere adottato prima della commissione del reato affinché l'ente possa giovare del beneficio di esonero della responsabilità.

È prevista, tuttavia, un'adozione “*tardiva*” ovvero un'adozione che avvenga dopo che il reato è stato commesso. In questo caso si possono verificare 2 situazioni differenti:

- l'ente adotta il modello prima dell'apertura del dibattimento;
- il modello viene adottato dopo la sentenza di condanna.

Nel primo caso l'ente che si impegna ad adottare tardivamente un modello può ottenere prima di tutto la sospensione della misura cautelare eventualmente disposta dal giudice<sup>11</sup>. In secondo luogo il giudice non potrà applicare sanzioni interdittive se l'ente ha risarcito il danno e restituito l'eventuale profitto; eventuali sanzioni pecuniarie verranno applicate in misura ridotta e non si potrà procedere con la pubblicazione di sentenza di condanna.

Nel secondo caso invece, il giudice può convertire la sanzione interdittiva in sanzione pecuniaria purché il modello venga adottato entro 20 giorni dalla notifica dell'estratto della sentenza e purché sia accertata l'avvenuta esecuzione di quanto previsto dell'articolo 17 che disciplina la riparazione delle conseguenze del reato.

Giova, infine, soffermarsi su un aspetto particolare che il decreto 231/01 non disciplina in modo diretto: il momento in cui risulta necessario procedere con l'adeguamento del modello.

In modo particolare le linee guida di confindustria consigliano l'adeguamento del modello ogniqualvolta si verificano casi di violazione dello stesso, qualora ci fosse una modifica rilevante dell'assetto societario ovvero quando vengono introdotte modifiche normative<sup>12</sup>.

Con specifico riferimento alle violazioni del modello rientrano in questa casistica, ad esempio, tutte quelle condotte in contrasto con le regole e i principi del modello stesso. In situazioni di questo tipo l'ente è tenuto ad operare in modo specifico:

- a) Agire direttamente nei confronti del soggetto autore delle violazioni non solo applicando le eventuali sanzioni previste ma anche agendo a livello formativo con lo scopo che in futuro violazioni simili non si ripetano;

<sup>10</sup>D'ARCANGELO F., I canoni di accertamento dell'idoneità nel MOG, in Rivista 231, 02-2011.

<sup>11</sup>Tale misura sarà altresì revocata qualora l'ente dia effettiva attuazione degli impegni assunti.

<sup>12</sup>In ognuno di questi casi vi è l'obbligo per l'organismo di vigilanza di trasmettere nuove proposte volte a riallineare il modello affinché l'ente possa essere esente dalla responsabilità individuata dal decreto studiato.

b) Modificare le regole e i precetti del modello oggetto di violazione.

Rientrano invece nelle casistiche delle modifiche dell'assetto societario mutamenti significativi delle deleghe o dei poteri, la quotazione in borsa, cambiamenti ai vertici e del business svolto, e così via. Infine, relativamente alle modifiche normative, troviamo tra le altre cose, ad esempio, l'entrata in vigore di una norma che introduca o elimini determinate fattispecie di reati presupposto.



## 2.2 ODV, codice etico e sistema disciplinare

Il decreto legislativo 231/01 amplia gli effetti prodotti dal reato commesso senza rivedere il concetto di responsabilità penale che rimane modellato sulla persona fisica. Il decreto in questione, infatti, presuppone che tra l'ente destinatario e il soggetto autore del reato vi sia una stretta forma di dipendenza da cui ne deriva il carattere subordinato della responsabilità dell'ente. Pertanto, in caso di reato, l'ente risponde in maniera autonoma rispetto alla persona fisica e la sua responsabilità si ha anche quando il soggetto che ha commesso l'illecito non viene identificato oppure non è identificabile. Data tale premessa l'ente si avvale di diversi strumenti e organi interni il cui obiettivo è quello di prevenire l'insorgere di reati presupposto. Con il presente lavoro si va ad esaminare chi vigila all'interno dell'ente e che strumenti utilizza per prevenire i reati.

### 2.2.1 ODV: composizione, funzioni e poteri

Come già illustrato nel capitolo 1, la responsabilità dell'ente non è prevista se, tra le altre cose, il compito di vigilare sul funzionamento e sull'osservanza del modello e di curare il suo aggiornamento è stato affidato *“ad un organo dotato di poteri autonomi e di poteri di iniziativa e controllo”* ovvero **l'organismo di vigilanza (ODV)**.

In merito alla composizione dell'organismo di vigilanza, il decreto 231/01 non contiene previsioni specifiche ma risultano fondamentali, in questo caso, le linee guida proposte dalle varie associazioni; ciò consente all'ente di scegliere tra una composizione monosoggettiva oppure plurisoggettiva. La scelta tra queste due alternative deve assicurare l'effettività dei controlli e di conseguenza la composizione dovrà tener conto delle dimensioni dell'ente, della sua organizzazione e del tipo di attività svolta.

In una nota sentenza relativa al caso Impregilo<sup>13</sup>, i giudici di legittimità hanno affermato che *“non era divisibile che l'ODV della società fosse alle dirette dipendenze del presidente del consiglio di amministrazione, perché tale impostazione sembrerebbe mettere in dubbio l'autonomia dell'ODV ai sensi dell'articolo 6, comma 1, lett. b) del decreto 231/01”*.

Secondo la cassazione, quindi, in una situazione di questo tipo si va a snaturare il principio secondo cui l'organo controllante non può essere subordinato al controllato. Le linee guida di confindustria si sono espresse in tal senso affermando che il modello di organizzazione non deve sovrapporre il soggetto controllore con il soggetto controllato: le due figure devono essere ben distinte. In altre parole, non è possibile che anche un solo membro dell'ODV sia “giudice di se stesso”, in quanto ciò farebbe emergere un chiaro conflitto di interessi<sup>14</sup>.

<sup>13</sup>Cassazione penale sez. V, 18/12/2013, n. 4677.

<sup>14</sup>LEDDA U., Caso ThyssenKrupp. Cassazione settembre 2014. Composizione dell'ODV e idoneità dei modelli organizzativi. Spunti di riflessione, in Rivista 231, 01-2015.

Con particolare riferimento ai soggetti che compongono l'ODV, secondo la giurisprudenza questi devono rispettare determinati requisiti:

### 1 **Autonomia e indipendenza:**

- evitare che all'ODV siano attribuiti compiti operativi;
- eliminare ogni forma di condizionamento, economica o personale, da parte dei vertici dell'ente;
- prevedere nel modello cause effettive di ineleggibilità, decadenza e onorabilità<sup>15</sup>.

### 2 **Professionalità:**

- è necessario nominare soggetti competenti in materia ispettiva e di consulenza, in grado di svolgere attività di analisi e valutazione dei rischi;
- è opportuno che almeno un soggetto abbia competenze in tema giuridico.

### 3 **Continuità di azione:**

E' bene predisporre una struttura dedicata alla vigilanza del modello supportata eventualmente da una segreteria tecnica di coordinamento.

Nel caso in cui venga a mancare uno di questi requisiti, il modello di organizzazione è da considerarsi inidoneo così come stabilito dal Tribunale di Milano il 20/04/2004.

Le funzioni che l'organismo di vigilanza è chiamato a compiere gli vengono direttamente attribuite dal consiglio di amministrazione. In linea generale le funzioni che deve svolgere si possono riassumere così:

- Vigilare sulla coerenza tra comportamenti posti in essere e quanto stabilito dal modello;
- Valutare l'adeguatezza del modello ovvero assicurare la capacità dello stesso di prevenire comportamenti vietati;
- Assicurare il mantenimento nel tempo dei requisiti fondamentali del modello;
- Aggiornare il modello organizzativo;
- Promuovere attività formative in materia 231;
- Esaminare e valutare tutte le segnalazioni in ambito 231;
- Curare i flussi di informazione di competenza con le funzioni aziendali;

---

<sup>15</sup>Le cause di ineleggibilità, decadenza e onorabilità sono quelle previste dal DPR 161/98.

- Approvare il programma di attività di vigilanza;
- Fornire chiarimenti in merito alle disposizioni contenute nel modello;
- Promuovere l'attivazione di eventuali provvedimenti disciplinari;

Tutte le attività poste in essere dall'ODV non possono essere in nessun modo sindacate da altri organismi o strutture aziendali.

Sulla base di quanto detto si può tranquillamente concludere affermando che all'organismo di vigilanza è attribuito un ruolo di assoluto rilievo poiché esso rappresenta il perno del sistema di prevenzione dei reati presupposto. Di conseguenza un modello organizzativo affinché si possa considerare idoneo, deve presentare un'apposita sezione con la quale disciplina tale organo, la sua composizione, i suoi compiti e i suoi poteri<sup>16</sup>.



Figura 2.4: L'organismo di vigilanza  
(Fonte: *Ilgiornaledellepmi.com*)

<sup>16</sup>ABRIANI N. – GIUNTA F., L'organismo di vigilanza previsto dal decreto legislativo 231/2001. Compiti e funzioni. In rivista 231, 03-2012.

Con particolare riferimento all'attività bancaria e nel rispetto delle già citate prerogative di autonomia e indipendenza, l'ODV esercita specifiche attività di controllo avvalendosi di libero accesso a tutta la documentazione aziendale, estraendone, se necessario, copia elettronica o cartacea. L'ODV può, inoltre, effettuare interviste a qualunque dipendente o terze parti interessate, ovvero supportare le varie strutture aziendali coinvolte nelle attività ispettive.

Nello svolgimento delle sue mansioni l'ODV ha come interlocutori e referenti i responsabili delle funzioni di internal auditing, di compliance nonché il dirigente preposto alla redazione dei documenti contabili societari.

Le attività di vigilanza svolte da tale organo possono essere di due tipologie:

- **attività periodiche:** si tratta di svolgere controlli periodici mirati su attività aziendali sensibili ovvero ritenute a rischio reato. In base ai risultati emersi l'ODV procede con le necessarie indagini volte ad accertare le presunte violazioni del MOG e dei soggetti autori di tali violazioni. I risultati devono essere trasmessi al consiglio di amministrazione per gli opportuni provvedimenti.
- **attività discrezionali:** si tratta di svolgere controlli a seguito di segnalazioni effettuate da dipendenti o terze parti relative a comportamenti ritenuti sospetti ovvero non in linea con quanto stabilito dal MOG.

A conclusione della propria attività, l'organismo di vigilanza verbalizza quanto effettuato, segnala senza indugio al consiglio di amministrazione i casi di violazione intenzionale e fraudolenta delle disposizioni previste dal modello, archivia i verbali e tutta la documentazione prodotta. Infine, con cadenza semestrale, l'ODV procede con la stesura di una relazione di sintesi delle attività ispettive effettuate e sui risultati emersi. Relazione da presentare al consiglio di amministrazione, con la presenza del collegio sindacale, rimanendo a disposizione per ogni richiesta di chiarimento o approfondimento.

Con questa relazione l'ODV stila la lista di tutte quelle attività poste in essere durante le fasi di vigilanza ed indica tutte le considerazioni raccolte nell'ottica di un miglioramento del modello organizzativo. È necessario indicare i destinatari della relazione, le finalità della stessa, il periodo di riferimento e riportare in modo chiaro, accurato e obiettivo, le principali considerazioni e argomentazioni. Si tratta di una serie precisa di elementi ritenuta doverosa affinché la relazione si possa considerare da un lato utile per chi la riceve e dall'altro si possa dimostrare la professionalità dell'organismo che l'ha redatta<sup>17</sup>.

Tutte le notizie relative alla commissione o al sospetto di commissione di illeciti per i quali è applicabile il decreto analizzato nonché le violazioni dei precetti contenuti nel

---

<sup>17</sup>GENNARO V, La documentazione delle attività di pianificazione e di esecuzione delle verifiche da parte dell'organismo di vigilanza. In rivista 231, 03-2008.



modello devono essere segnalati all'ODV. Le segnalazioni possono essere effettuate in forma anonima direttamente all'organismo di vigilanza oppure per il tramite della funzione internal auditing. Inoltre le stesse possono essere eseguite senza anonimato tramite il responsabile della funzione interna auditing ovvero per il tramite del comitato per il controllo della gestione nel caso in cui si ritenesse che la funzione di internal auditing possa potenzialmente essere in posizione di conflitto di interessi. Queste modalità di segnalazione possono essere usate sia da soggetti interni come i dipendenti sia da soggetti esterni alla banca.

Una volta ricevute le segnalazioni l'ODV le valuta e procede con l'applicazione di eventuali provvedimenti tenendo conto di quanto detto e riportato dall'autore della segnalazione e dal responsabile della presunta violazione.

### 2.2.2 Il codice etico

In ambito 231 il codice etico rappresenta *la carta dei principi fondamentali* che rende espliciti i fondamenti e i valori di riferimento su cui poggia la cultura dell'ente. Si tratta di una carta che rende concrete le regole di comportamento che devono essere rispettate da tutti i soggetti: sia interni che esterni all'ente.

Ne deriva che la finalità di tale codice è duplice:

- 1- stabilire qual'è il nocciolo duro dei principi portanti dell'ente;
- 2- promuovere comportamenti in linea con quanto stabilito nel modello organizzativo.

Nel suo insieme il codice stabilisce quali sono i diritti, i doveri e le responsabilità dell'ente nei confronti dei soggetti con cui intrattiene una relazione. Lo scopo principale del codice etico è quello di fornire un sistema di regole comportamentali che siano comuni tra i vari soggetti che fanno capo all'ente in modo tale che ognuno di essi si comporti in maniera moralmente corretta rispettando la normativa interna all'ente stesso. I principi contenuti nel codice vanno ad integrare il comportamento che il personale deve osservare in ambito lavorativo in virtù del contratto di lavoro, delle procedure interne e in base alle normative in essere.

Nello specifico è considerato oggetto del codice etico il rispetto dei seguenti principi<sup>18</sup>:

- Principio di legalità con il quale l'ente garantisce il rispetto delle regole e delle leggi al proprio interno;
- Principio di lealtà, in base al quale l'ente assicura e promuove la lealtà e correttezza nelle relazioni intrattenute con i destinatari, nonché la trasparenza, chiarezza e completezza nelle informazioni;

---

<sup>18</sup>ITINERA, Responsabilità amministrativa degli enti, a cura di Sbisà F.

- Principio di coinvolgimento e consenso, in base al quale l'ente promuove e richiede il rispetto delle leggi, dei regolamenti, delle disposizioni organizzative interne anche da parte dei collaboratori, consulenti e fornitori;
- Principio di liceità, che comporta l'astensione da comportamenti illeciti;
- Principio di tutela delle risorse umane, con cui l'ente si impegna a promuovere il valore delle risorse umane garantendo il rispetto della professionalità e dell'integrità fisica e morale dei propri dipendenti e collaboratori;
- Principio di etica nello svolgimento della propria attività;
- Principio di imparzialità, considerando in modo oggettivo la pluralità di interessi pubblici e privati implicati nella sua valutazione, evitando di discriminare la posizione dei soggetti coinvolti e sottraendosi a pressioni indebite;
- Principio delle correttezza e tutela della concorrenza, che implica il rispetto e l'applicazione di regole antitrust e le disposizioni emanate dalle autorità che regolano il mercato;
- Principio della trasparenza nella sua organizzazione.

**PRINCIPALI  
VALORI DI RIFERIMENTO**  
**(DECRETO LEG. 231/2001)**

- *PRINCIPIO DELLA LEGALITÀ*
- *TRASPARENZA E LEALTA'*
- *ATTENZIONE ALLA PERSONA*
- *SENSO DI APPARTENENZA*
- *ECCELLENZA NEL SERVIZIO*

Figura 2.5: **Il codice etico: principi**  
(Fonte: Slideshare.it)

Inoltre il codice etico deve indicare una serie di principi nei confronti dei dipendenti come ad esempio adottare criteri di merito e competenza ovvero creare un ambiente di lavoro all'interno del quale comportamenti personali non diano luogo a discriminazioni.

Particolare attenzione merita poi il fatto che gli effetti del codice etico si ripercuotono in modo automatico nei confronti del personale dipendente ma non nei confronti di quei soggetti che intrattengo con l'ente un rapporto subordinato.

In quest'ultimo caso, infatti, è necessario stabilire che quanto indicato nel codice produce effetti anche per ciò che riguarda le seguenti tipologie di rapporti:

- Obbligazioni contrattuali dei dipendenti ai sensi e per gli effetti dell'articolo 2104 c.c.;
- Rapporto fiduciario instaurato con organi sociali;
- Obbligazioni contrattuali assunte da fornitori, consulenti, e collaboratori.

Nel caso si verificassero violazioni del modello 231/01, siano esse ascrivibili a dolo, o colpa dell'autore, nel codice etico deve essere chiaramente indicato che ciò comporta la commisurazione di sanzioni. Proprio per questa ragione quanto contenuto nel codice deve essere portato a conoscenza dei dipendenti, in fase di assunzione, ovvero nei confronti di fornitori o altre parti terze.

In modo particolare, in caso di violazioni, si deve tener conto di specifici elementi prima di stabilire l'entità e la tipologia della sanzione. Tra questi elementi troviamo:

- a) Illecito commesso a seguito di omissione o azione;
- b) Comportamento intenzionale, negligente, imprudente o avvenuto a seguito imperizia;
- c) Posizione ricoperta dal soggetto all'interno dell'ente;
- d) Comportamento complessivo tenuto dal dipendente con particolare riguardo al fatto che siano stato commessi o meno illeciti in precedenza;
- e) Mansioni del dipendente;
- f) Posizione funzionale dei soggetti coinvolti nell'illecito;
- g) Distinzione tra violazioni formali e violazioni più gravi che possono portare a pregiudizievoli per l'ente;
- h) Effetto prodotto dall'illecito;

In situazioni di questo tipo la gravità è valutata in base ad elementi soggettivi di chi ha compiuto il reato e dalla frequenza degli episodi, mentre le conseguenze tengono conto della problematica che si è creata a seguito dell'illecito.

Per ciò che concerne il sistema bancario prima di tutto va precisato che la condivisione e il rispetto delle regole indicate nel codice etico rappresentano elementi fondamentali per

il raggiungimento degli obiettivi in esso stabiliti. All'interno di questo lavoro sono stati presi in considerazione ed analizzati codici redatti da diversi istituti di credito. Lo scopo è quello di individuare punti in comune al fine di redigere uno schema generale all'interno del quale riportare principi e valori che a mio avviso devo essere sempre trascritti in fase di redazione del codice etico.

A tal proposito va detto che il codice una volta redatto deve essere portato a conoscenza di tutte le strutture aziendali affinché:

- L'attività economica della banca sia eseguita nel rispetto delle norme di riferimento;
- Sia esclusa qualsiasi forma di opportunismo contrario alle regole di correttezza;
- Sia assicurata la diffusione della cultura della legalità;
- Tutte le attività vengano svolte in modo corretto e leale e con etica professionale;
- Sia evitata la commissione di illeciti stabiliti dal decreto legislativo 231/01;
- Vengano dettati principi e regole a cui ispirarsi;

Il codice etico deve essere consegnato ad ogni nuovo amministratore, sindaco, dipendente o collaboratore esterno in fase di nuova nomina, dell'assunzione o di avvio di un nuovo rapporto collaborativo.

Tutti questi soggetti devono attenersi a quanto stabilito nel codice contribuendo in maniera efficace alla sua osservanza e diffusione. Nello specifico i destinatari del codice etico<sup>19</sup> sono da un lato i soggetti interessati ovvero dipendenti, amministratori e sindaci della banca, e dall'altro i soggetti che instaurano con la banca un rapporto, temporaneo o continuativo, di collaborazione ovvero che operano nell'interesse della stessa.

Tutti i soggetti interessati sono tenuti a rispettare le direttive aziendali: se si verifica una condotta ritenuta illecita deve essere applicata una sanzione disciplinare. Tale sanzione può rivelarsi dannosa per la banca dal punto di vista economico, soprattutto in tema di illeciti derivanti da reati presupposto disciplinati dal decreto 231/01. Per questo motivo è fondamentale che ogni soggetto di ordine e grado operi con il massimo impegno e rigore professionale nel rispetto del principio di onestà, correttezza, trasparenza e integrità.

In merito all'ambiente e al luogo di lavoro, in linea generale, la banca è tenuta a realizzare condizioni di lavoro funzionali alla tutela dell'integrità psicofisica dei soggetti interessati evitando qualsiasi tipo di discriminazione o condizionamento illecito.

---

<sup>19</sup>Soggetti nei confronti dei quali si applicano le norme indicate nel codice senza eccezione alcuna.

Dall'altro canto i soggetti interessati devono operare, ciascuno per propria competenza, in modo tale da mantenere l'ambiente di lavoro il più sano e sicuro possibile osservando e rispettando le norme interne in materia di sicurezza.

I soggetti interessati sono tenuti a salvaguardare il patrimonio della banca: locali, attrezzature e qualsiasi altro bene di proprietà aziendale.

La banca deve mettere a disposizione dei propri dipendenti strumenti informatici necessari per lo svolgimento dell'attività lavorativa: l'uso non appropriato e non autorizzato di detti sistemi, indipendentemente dal fatto che comporti alla banca un vantaggio o uno svantaggio, è da ritenersi un comportamento disciplinare rilevante.

Relativamente ai rapporti con soggetti terzi e con particolare riguardo al rapporto cliente-dipendente, l'accettazione di regali è consentita purché si tratti di regali di modico valore e ascrivibili a normali relazioni di cortesia. Qualora si vada ad oltrepassare tale limite i soggetti interessati devono rifiutare l'offerta ed informare il proprio superiore ovvero l'ODV al fine di restituire quanto ricevuto.



Figura 2.6: L'etica  
(Fonte: *Enricoberardi.it*)

I soggetti interessati devono assolutamente astenersi dal compiere qualsiasi tipo di attività che possa essere potenzialmente in conflitto di interesse con l'istituto di credito. In modo particolare i dipendenti hanno il divieto di compiere affari in concorrenza con il proprio datore di lavoro così come stabilito dall'articolo 2105 del codice civile. Di conseguenza ogni situazione che genera un conflitto di interessi deve essere comunicata dal dipendente al suo responsabile e comporta per il soggetto interessato l'obbligo di astenersi dal compiere ogni atto connesso a tale situazione.

Con riguardo alla prevenzione dei reati va detto che ogni transazione bancaria deve essere tracciata e adeguatamente documentata nel rispetto della normativa tempo per tempo in vigore. La banca ha il compito di formare i soggetti interessati affinché sia garantita la verità, la correttezza e la chiarezza di informazioni, sia interne che esterne, nonché la massima accuratezza nel custodire dati contabili e societari.

Eventuali errori, omissioni o falsificazioni di scritture contabili devono essere segnalate senza indugio agli organi di controllo competenti.

Inoltre la banca si impegna a rifiutare di porre in essere operazioni sospette sotto il profilo della trasparenza e correttezza contabile. Di fatto ogni istituto è tenuto da un lato a verificare in via preventiva le informazioni disponibili sulle controparti e dall'altro ad operare in modo tale da evitare ogni tipo di implicazione in operazioni atte a favorire in modo particolare il riciclaggio di denaro e più in generale ogni operazione potenzialmente idonea a favorire la commissione di reati presupposto.

Infine tutti i soggetti interessati hanno l'obbligo di segnalare ogni violazione o sospetta violazione delle regole aziendali o del codice etico di comportamento agli organi competenti per materia. Con particolare riferimento ai reati individuati dal decreto 231/01, le segnalazioni devono essere effettuate anche all'ODV.

### 2.2.3 Il sistema disciplinare

Come accennato in precedenza l'ODV e il codice etico hanno come obiettivo principale quello di prevenire la commissione di reati. Tuttavia nel caso si verificano commissioni di illeciti è necessario adottare misure idonee a sanzionare il mancato rispetto delle regole riportate nel modello<sup>20</sup>. È necessario che l'ente adotti un modello disciplinare all'interno del quale indicare sanzioni e modalità applicative da intraprendere nei confronti dei soggetti che hanno commesso un illecito. Obiettivo principale del sistema sanzionatorio è quello di assicurare l'efficacia del modello organizzativo.

Il sistema sanzionatorio che ogni ente adotta deve tener conto della normativa vigente che regola i rapporti di lavoro, in modo particolare:

- Il contratto collettivo nazionale di lavoro per i dirigenti;
- Il contratto collettivo nazionale di lavoro per quadri direttivi e aree professionali;
- La legge 300 del 20 maggio 1970, articolo 7 sanzioni disciplinari;
- La legge 604 del 15 luglio 1966<sup>21</sup>;
- Il libro V del codice civile; in modo particolare gli articoli 2104 (diligenza del prestatore di lavoro), 2105 (obbligo di fedeltà), 2106 (sanzioni disciplinari), 2118 e 2119 (licenziamento con e senza preavviso), 2392 (responsabilità verso la società), 2407 (responsabilità dei sindaci), 2409 (denuncia al tribunale), 2409-sexies (responsabilità dei controllori e delle società di revisione).

Per quanto riguarda il personale dirigente, in caso di violazione delle regole e dei principi interni, si provvederà ad applicare nei confronti di tali soggetti provvedimenti particolari

<sup>20</sup>Così come stabilito dall'articolo 6 paragrafo 2 comma e) del decreto 231/01.

<sup>21</sup>Legge che disciplina i licenziamenti individuali.

poiché bisogna tener conto del rapporto fiduciario di collaborazione in essere. Nello specifico il contratto collettivo nazionale che disciplina questa tipologia di rapporti prevede, come strumenti da porre in essere nei casi di massima gravità, il licenziamento con preavviso e il licenziamento per giusta causa

Tuttavia, considerando che l'applicazione di questi provvedimenti porta alla risoluzione del contratto di lavoro, l'ente ha la facoltà di applicare sanzioni meno gravi a seconda di ciò che si è verificato. Tra queste sanzioni troviamo il rimprovero scritto e la sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni.

Per quanto concerne il contratto collettivo di lavoro per i quadri direttivi e le aree professionali l'articolo 44 enuncia le sanzioni applicabili, che sono le seguenti:

- **Rimprovero verbale**, previsto in caso di lieve inosservanza di quanto stabilito dal modello ovvero in caso di violazioni di norme interne o di comportamenti non adeguati;
- **Biasimo scritto**, si applica in caso di inosservanza non grave delle regole contrattuali o delle direttive impartite da organi superiori;
- **Sospensione dal lavoro per un periodo non superiore a 10 giorni**, si applica in caso di inosservanza ripetuta o di una certa gravità delle regole contrattuali o delle direttive impartite da organi superiori;
- **Licenziamento per giustificato motivo**, previsto in caso di notevoli inadempimenti degli obblighi contrattuali del lavoratore;
- **Licenziamento per giusta causa**, previsto per mancanza così grave da far venir meno la fiducia sulla quale si basa il rapporto di lavoro tale da non consentire la prosecuzione dello stesso.

In base alla **legge 300**, invece, va precisato quanto segue

- Il datore di lavoro non può adottare provvedimenti disciplinari senza aver contestato in maniera preventiva l'addebito al lavoratore il quale nei 10 giorni successivi può presentare le sue difese;
- Non possono essere applicate sanzioni disciplinari che portano ad un cambiamento del contratto di lavoro;
- I provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi 5 giorni dalla contestazione per iscritto del fatto che li ha creati.

Dalla **legge 604**, invece, il licenziamento del lavoratore può avvenire esclusivamente per giusta causa o giustificato motivo.

In merito agli articoli del codice civile questi disciplinano quanto segue:

**-articolo 2014:** il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale;

**-articolo 2105:** il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio;

**-articolo 2016:** l'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari secondo la gravità dell'infrazione;

**-articolo 2392:** gli amministratori devono adempiere i doveri ad essi imposti dalla legge e dallo statuto con la diligenza richiesta dalla natura dell'incarico e delle loro specifiche competenze; essi sono solidalmente responsabili verso la società dei danni derivanti dall'inosservanza di tali doveri, a meno che si tratti attribuzioni proprie del comitato esecutivo o di funzioni in concreto attribuite ad uno o più amministratori; in ogni caso gli stessi sono solidalmente responsabili se, essendo a conoscenza di atti pregiudizievoli, non hanno fatto quanto potevano per impedirne il compimento o eliminarne le conseguenze dannose;

**-articolo 2407:** i sindaci devono adempiere i loro doveri con la professionalità e la diligenza richieste dalla natura dell'incarico, sono responsabili della verità delle loro attestazioni e devono conservare il segreto sui fatti e sui documenti di cui hanno conoscenza per ragione del loro ufficio; essi sono responsabili solidalmente con gli amministratori per i fatti o le omissioni di questi quando il danno non si sarebbe prodotto se essi avessero vigilato in conformità degli obblighi della loro carica;

**-articolo 2049:** se vi è fondato sospetto che gli amministratori, in violazione dei loro doveri, abbiano compiuto gravi irregolarità nella gestione che possono arrecare danno alla società o a una o più controllate, i soci che rappresentano il decimo del capitale sociale o, nelle società che fanno ricorso al mercato del capitale del rischio, il ventesimo del capitale sociale, possono denunciare i fatti al tribunale con ricorso notificato anche alla società;

**-articolo 2409-sexies:** i soggetti incaricati del controllo contabile sono sottoposti alle disposizioni dell'articolo 2407 e sono responsabili nei confronti della società, dei soci e dei terzi per i danni derivanti dall'inadempimento ai loro doveri; nel caso di società di revisione i soggetti che hanno effettuato il controllo contabile sono responsabili in solido con la società medesima.



Concludendo l'azienda ha la facoltà di applicare i provvedimenti disciplinari ritenuti più adeguati dopo aver effettuato tutte le valutazioni del caso. Le sanzioni sono applicate nel rispetto del principio di gradualità e proporzionalità delle stesse e tenendo conto della gravità della mancanza. In particolare l'entità di ogni provvedimento disciplinare deve tener conto:

- dell' intenzionalità del comportamento o al grado di negligenza;
- delle mansioni del lavoratore e al concorso di più lavoratori in accordo tra loro;
- alla recidività e alla posizione funzionale;
- al comportamento complessivo del lavoratore con riguardo particolare ai precedenti disciplinari.

Nella tabella sottostante si riporta un elenco di comportamenti sanzionabili e l'entità delle sanzioni. Relativamente alle categorie indicate possiamo individuare le seguenti funzioni aziendali:

- FUNZIONI DI CONTROLLO E RAPPRESENTANZA: Membri del collegio sindacale, Presidente, Membri del consiglio di amministrazione;
- DIRIGENTI: Direttore generale e Dirigenti;
- PERSONALE DIPENDENTE: Quadri direttive e Impiegati;

INFRAZIONI	FUNZIONI DI CONTROLLO E RAPPRESENTANZA	DIRIGENTI	PERSONALE DIPENDENTE
<b>Omessa segnalazione ODV</b>	-	- Richiamo	- Rimprovero verbale - Biasimo scritto
<b>Mancato rispetto procedure aziendali</b>	-	- Richiamo	- Rimprovero verbale - Biasimo scritto - Sospensione
<b>Non osservanza livelli autorizzazione</b>	-	- Richiamo	- Rimprovero verbale - Biasimo scritto - Sospensione
<b>Violazioni codice etico</b>	- Denuncia	- Richiamo - Licenziamento	- Rimprovero verbale - Biasimo scritto - Sospensione - Licenziamento

Tabella 2.1: *Le sanzioni disciplinari*  
(Fonte: Il Mog BCC di Roma)

Come si evince da quanto indicato in tabella, le sanzioni possono coinvolgere, oltre alla persona che ha commesso il reato, anche tutti quei soggetti responsabili di non aver vigilato coerentemente sulla base di quanto stabilito nel Mog. In ogni caso le sanzioni devono rispettare le normative e le legislazioni vigenti.

Infine nella tabella che segue si riportano le sanzioni applicabili, alle varie categorie di soggetti che appartengono ad un istituto di credito, tenendo conto del fatto che non vengono rispettate le norme disciplinate dal decreto 231/01.

INFRAZIONI RELATIVE AL D.LGS 231/01	FUNZIONI DI CONTROLLO E RAPPRESENTANZA	DIRIGENTI	PERSONALE DIPENDENTE
<b>Reati previsti dal d.lgs 231/01</b>	- Denuncia	-Richiamo - Licenziamento	- Sospensione - Licenziamento
<b>Mancata correttezza e trasparenza informativa con le Autorità di vigilanza</b>	- Denuncia	- Richiamo - Licenziamento	- Sospensione - Licenziamento

Tabella 2.2: *Le sanzioni disciplinari in funzione 231/01*  
(Fonte: Il Mog BCC di Roma)

## 2.3 Reati presupposto: la segnalazione

Per quanto riguarda i reati presupposto oltre alle segnalazione previste, da effettuarsi all'organismo di vigilanza così come indicato dal decreto 231/01, si possono verificare situazioni particolari che possono mettere a repentaglio la responsabilità dell'ente. Con particolare riferimento agli istituti di credito non è da escludere la possibilità che siano messe in atto operazioni che minano fortemente la responsabilità della banca.

A tal proposito per prevenire la commissione di reati presupposto nel nostro ordinamento è prevista una stretta collaborazione tra diversi soggetti: gli operatori di sistema, le autorità amministrative, gli organi investigativi e l'autorità giudiziaria.

L'obiettivo è quello di prevenire e individuare tutte quelle operazioni anomale che possono dar vita ad illeciti che rientrano nel ambito del decreto 231/01.

Attraverso questa collaborazione gli istituti di credito, oltre ad avvalersi di un sistema di controlli interni volto a prevenire la commissione di reati presupposto attraverso segnalazioni all'ODV, sono tenuti a segnalare operazioni ritenute sospette ad un organo esterno alla banca stessa: **l' Unità di Informazione Finanziaria**.

In entrambi i casi con la segnalazione si esime l'ente da responsabilità: tuttavia mentre la segnalazione all'ODV ha per oggetto operazioni poste in essere dai componenti dell'ente stesso, la segnalazione fatta all'UIF avviene quanto l'operazione è posta in essere da soggetti esterni come ad esempio i clienti di una banca.

Quest'ultima tipologia di segnalazione non è meno importante della prima in quanto è volta a prevenire situazioni anomale che possono portare alla commissione di illeciti che hanno come responsabile l'ente: potrebbero verificarsi casi in cui i membri dell'ente agiscono di concerto con i clienti.

A tal riguardo gli operatori di mercato sono chiamati ad adempiere ad obblighi specifici ovvero:

- L'adeguata verifica della clientela;
- La conservazione dei documenti e delle informazioni acquisite;
- L'individuazione e la segnalazione delle operazioni sospette all'UIF.

Si tratta di un insieme di obblighi che colpisce una platea assai numerosa di operatori<sup>22</sup>.

---

<sup>22</sup>Tra questi operatori troviamo anche diverse categorie di professionisti (notai, avvocati, ecc.) ed operatori non finanziari come ad esempio case d'asta, società di recupero crediti, operatori professionali in oro, soggetti che esercitano mediazione civile, ecc.

In questo lavoro andremo ad analizzare nel dettaglio ciò che sono tenuti a fare gli intermediari bancari quando si verificano situazioni particolari che vanno ad impattare con quanto disciplinato dal decreto 231/01.

### 2.3.1 Contenuti e modalità di segnalazione

Con la **legge 197/91** è stato introdotto, per la prima volta nel nostro ordinamento, l'obbligo per gli intermediari bancari di effettuare le segnalazioni di operazioni sospette. In particolare gli stessi erano tenuti ad inviare le segnalazioni direttamente al questore competente per territorio; sin da subito si trattava di una procedura che mostrava delle criticità operative soprattutto per ciò che riguardava il rispetto del principio di riservatezza della segnalazione.

Sulla base di questa carenza operativa, a partire dal 1997 il legislatore ha stabilito che tutte le segnalazioni dovevano effettuarsi presso l'**UIC**: anche in questo caso la decisione non fu ottimale e l'ente fu soppresso. Infatti a partire dal 2008 tutte le segnalazioni vanno inoltrate all'**UIF** ovvero l'unità di informazione finanziaria per l'Italia: si tratta di un ente autonomo e operativamente indipendente, istituito presso la Banca d'Italia.

Con questa soluzione il legislatore italiano ha risolto tutte le carenze operative finora riscontrate e ha dato vita a un ente conforme agli standard internazionali: autonomo dal punto di vista operativo, unico a livello nazionale, specializzato nelle funzioni di analisi finanziaria e capace di scambiare informazioni in modo diretto.

Nel caso specifico delle segnalazioni che devono pervenire all'ODV i contenuti e le modalità da seguire sono molto simili alle segnalazioni che l'intermediario deve effettuare nei confronti dell'UIF. Vediamo ora nel dettaglio quali devono essere i contenuti ritenuti essenziali nelle segnalazioni rivolte all'ODV prendendo in considerazione quanto approvato nel modello organizzativo di due importanti istituti di credito del nostro paese: Intesa San Paolo spa e Unicredit spa.

Per ciò che riguarda i flussi informativi questi devono avere ad oggetto informazioni e dati che possono consentire all'ODV di aumentare il livello di conoscenza della banca. Con questi flussi informativi l'ODV deve essere in grado di valutare il rischio insito in tutti i processi aziendali nonché svolgere la propria attività di vigilanza ponendo particolare attenzione al rispetto di quanto riportato nel modello.

In particolare L'ODV deve essere informato in maniera tempestiva su tutti quegli eventi e comportamenti anomali che potrebbero far sorgere la responsabilità della banca.

Infatti è necessario segnalare senza indugio le notizie relative alla commissione di illeciti per i quali è prevista l'applicazione del decreto 231/01, eventuali violazioni delle regole

di comportamento contenute nel modello nonché qualsiasi fatto o situazione critica che potrebbe esporre l'istituto alle sanzioni previste dal decreto 231/01.

All'organismo di vigilanza devono essere obbligatoriamente trasmesse anche tutte le informazioni che hanno i seguenti contenuti:

- Informazioni riguardanti provvedimenti provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, fatti salvi gli obblighi di segreto imposti dalla legge, da cui emerge lo svolgimento di indagini per illeciti previsti dal decreto in questione. Le informazioni devono essere comunicate tramite la funzione di internal auditing purché le indagini coinvolgano la banca stessa, i dipendenti oppure gli organi sociali;
- Informazioni su fatti, eventi e omissioni rispetto all'osservanza delle norme del decreto;
- Informazioni relative ai procedimenti disciplinari applicati nei confronti dei dipendenti in seguito a violazioni di norme disciplinate dal decreto 231/01 o a seguito di violazioni del modello organizzativo. Le informazioni in questo caso saranno trasmesse direttamente dalla funzione risorse umane.



Figura 2.7: **La via della segnalazione**  
(Fonte: *Cplconcordiagroup.com*)

Tutte le segnalazioni effettuate all'ODV devono essere dettagliate e basate su elementi di fatto precisi e ben definiti. Tutti i dipendenti sono tenuti a segnalare eventuali comportamenti anomali e contrari a quanto previsto dal modello nel rispetto del dovere di diligenza e obbligo di fedeltà del prestatore di lavoro.

In nessun caso il corretto adempimento dell'obbligo di segnalazione potrà dar vita all'applicazione di sanzioni disciplinari nei confronti del segnalante a meno che la segnalazione sia stata effettuata con dolo o colpa grave e si riveli del tutto infondata.

Chi effettua la segnalazione è inoltre garantito da qualsiasi forma di ritorsione, discriminazione o penalizzazione ed è assicurata la **massima riservatezza** in merito all'identità del segnalante ad esclusione dei casi previsti dalla legge o per quelle situazioni che tutelano i diritti della banca o delle persone accusate erroneamente o in mala fede.

Le segnalazioni all'ODV possono essere effettuate con diverse modalità:

- Direttamente all'ODV tramite e-mail o lettera scritta;
- Tramite la funzione Internal Auditing la quale poi informa l'ODV e lo rendiconta sui fatti riscontrati;
- Tramite il responsabile della funzione di Internal Auditing, il cosiddetto "*whistleblower*". In questo caso i dipendenti dell'istituto di credito segnalano fatti o comportamenti anomali che possono rappresentare una violazione delle norme che regolamentano l'attività bancaria;
- Tramite il comitato per il controllo sulla gestione nel caso in cui chi effettua la segnalazione ritenga che la funzione di Internal Auditing possa trovarsi in posizione di conflitto di interesse in virtù della natura della segnalazione stessa.

La segnalazione dovrà riportare i dati e le generalità del segnalante, indicare una chiara e completa descrizione dei fatti, dare l'indicazione dei soggetti coinvolti, indicare eventuali parti terze che potrebbero riferire sull'argomento descritto e indicare ogni altro argomento utile in grado di dare rilevanza alla segnalazione. Una volta ricevute le segnalazioni l'ODV può convocare, qualora lo ritenga necessario, il presunto autore dell'illecito espletando tutti gli accertamenti del caso.

### 2.3.2 Il whistleblowing

Con il termine **whistleblowing** si fa riferimento ad una particolare azione: *soffiare il fischiotto*. Nel nostro sistema economico questa azione si può tradurre come una denuncia sul posto di lavoro.

Il termine sembra trarre origine dalla pratica dei poliziotti inglesi di soffiare nel fischiotto qualora notino la commissione di un crimine in modo tale da richiamare l'attenzione di altri poliziotti e della collettività in modo più generale. L'obiettivo pertanto è quello di bloccare un'azione, nel nostro caso la commissione di un illecito, richiamando l'attenzione dei soggetti atti a vigilare.

Il whistleblower pertanto rappresenta quel soggetto che nel corso della propria attività lavorativa, scopre e denuncia fatti che possono causare un danno all'ente in cui lavora o ai soggetti che con questo si relazionano.

---

#### Definizione

Il whistleblowing ("fare una rivelazione nel pubblico interesse") è un istituto di origine anglosassone che disciplina la condotta dei soggetti che segnalano illeciti penali o irregolarità all'interno del proprio ambiente di lavoro, all'interno di procedure che ne garantiscono la protezione.



**LAWORO**  
STUDIO LEGALE

Figura 2.8: Il whistleblowing  
(Fonte: Slideshare.it)

Nel nostro ordinamento il decreto whistleblowing è stato approvato in data 15 novembre 2017 con 357 voti favorevoli, 46 contrari e 15 astenuti. Si tratta di un provvedimento assai

importante poiché rafforza quella che è la disciplina sulla protezioni da discriminazioni o ritorsioni dei lavoratori che vogliono segnalare illeciti.

In **ambito pubblico** il provvedimento in questione va a sostituire l'articolo 54 bis del testo unico del pubblico impiego. Con questa sostituzione il dipendente pubblico che intende segnalare violazioni o comportamenti illeciti, di cui è venuto a conoscenza durante lo svolgimento della propria attività, è fortemente tutelato e protetto in quanto non potrà subire ritorsioni<sup>23</sup> dovute alla segnalazione effettuata.

Particolare importanza assume il fatto che con questo decreto è previsto il divieto di rivelare l'identità del segnalante le cui generalità sono protette:

- In caso di processo penale, sulla base di quanto stabilito dall'articolo 329 del codice di procedura penale;
- In caso di processo contabile, poiché è previsto l'obbligo di non rilevare l'identità del segnalante fino alla fine dell'istruttoria;
- In caso di processo amministrativo, in virtù del fatto che l'identità non può essere resa pubblica senza il consenso del segnalante.

Nel caso in cui venissero applicate ritorsioni o forme di discriminazione di qualsiasi natura nei confronti del segnalante, sono previste delle sanzioni applicate direttamente dell'ANAC. L'importo della sanzione può variare da un minimo di 5.000,00 euro a un massimo di 30.000,00 euro.

Sanzioni più alte sono invece applicate nel caso in cui non sia adottato un sistema interno di segnalazione ovvero nel caso in cui il responsabile di sistema ometta la verifica di quanto ricevuto<sup>24</sup>. Nel caso in cui il segnalante sia stato condannato in sede penale per calunnia, diffamazione o altri reati simili, ovvero venga accertata la sua responsabilità civile per colpa o dolo viene meno l'istituto del whistleblowing.

In **ambito privato** il presente decreto porta modifiche rilevanti in tema di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni introducendo specifiche disposizioni in merito alla violazione del MOG. In particolare il decreto implementa quanto già adottato dal legislatore in seguito al recepimento di determinate normative europee.

Tra queste ricordiamo:

---

<sup>23</sup>Sono da considerarsi escluse, pertanto, l'applicazione di sanzioni, il licenziamento, il demansionamento e il trasferimento presso altri uffici.

<sup>24</sup>In questo caso la sanzione varia tra i 10.000,00 e i 50.000,00 euro.



- Il decreto legislativo 8 maggio 2015 recante il recepimento della direttiva 2013/36 UE del parlamento europeo e del consiglio del 26 giugno 2013: direttiva che introduce modifiche sia al TUB che al TUF prevedendo specifiche disposizioni di segnalazione interna in caso di violazioni da parte del personale delle banche<sup>25</sup>;
- Il decreto legislativo 25 maggio 2017 recante il recepimento della quarta direttiva antiriciclaggio con il quale si evidenzia per la prima volta la previsione di sistemi di whistleblowing<sup>26</sup>;
- Il decreto legislativo 3 agosto 2017 recante il recepimento della direttiva europea 2016/1034 che richiede agli intermediari di cui alla parte II del TUF, ai soggetti di cui alla parte III del TUF e alle imprese di assicurazione di dotarsi di procedure specifiche per la segnalazione di violazioni dell'attività svolta.

Con l'approvazione del decreto di whistleblowing sono aumentati i soggetti che sono obbligati a dotarsi di un sistema di segnalazione interna. Con particolare riferimento al decreto 231/01 il whistleblowing introduce, dopo il comma 2 dell'articolo 6, i commi 2-bis, 2-ter e 2 quater in forza dei quali i vari modelli che saranno adottati dagli enti devono prevedere tra le altre cose le seguenti misure:

- **Comma 2-bis articolo 6 decreto 231/01:** i modelli prevedono uno o più canali che consentono ai soggetti indicati nell'articolo 5 di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
  - i modelli prevedono almeno un canale alternativo di segnalazione idoneo a garantire la riservatezza del segnalante;
  - il divieto di atti di ritorsione, diretti o indiretti, nei confronti del segnalante;
  - nel sistema disciplinare devono essere previste sanzioni nei confronti di chi viola le misure di tutela del segnalante nonché di chi effettua segnalazioni infondate con dolo o colpa grave.
- **Comma 2-ter articolo 6 decreto 231/01:** l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può

<sup>25</sup>Circolare della Banca d'Italia n. 285 del 17 dicembre 2013, che recependo le disposizioni contenute nell'art. 52-bis del TUB, ha disposto l'introduzione obbligatoria di sistemi interni di segnalazione delle violazioni da parte di banche e intermediari finanziari.

<sup>26</sup>Direttiva europea 2015/849.

essere denunciata all'ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione indicata dal medesimo.

- **Comma 2-quater articolo 6 decreto 231/01:** il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2013 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. E' onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Sulla base di ciò i modelli di organizzazione dovranno presentare una descrizione specifica per quel che riguarda i soggetti abilitati ad effettuare segnalazioni, ai contenuti delle stesse, alle funzioni aziendali preposte alla gestione del sistema di whistleblowing e alle forme di tutela riservate alla protezione dell'identità dei soggetti segnalanti e alle relative sanzioni previste nei confronti di chi viola tali misure.

## Capitolo 3

# Attività bancaria e reati connessi con la responsabilità amministrativa dell'ente

Nel presente capitolo viene proposta una visione del decreto 231/01 diversa da quanto finora analizzato.

Il decreto in questione è stato introdotto con l'obiettivo principale di prevenire la commissione di illeciti e rendere l'ente esimente qualora si verificassero reati, salvo il fatto che tutte le misure previste vengano adottate in maniera corretta.

Il sistema 231/01, a mio modo di vedere, va oltre questa finalità: il decreto, infatti, assolve anche una funzione di governance aziendale e di gestione dei processi dell'ente rilevandosi meno statico e più operativo di ciò che appare.

Basta pensare al modello organizzativo che si può definire come uno strumento che integra gli altri processi aziendali contribuendo da un lato a migliorare l'organizzazione dell'ente, la definizione e le scelte strategiche dello stesso, dall'altro a prevenire la commissione di reati.

Con questo lavoro si analizza il contributo fornito dal modello organizzativo al sistema bancario e si affronta la tematica del rischio: come valutare il rischio di commissione dei reati presupposto? Come adottare un sistema di controlli preventivo? Che processi applicare per rendere adeguato questo sistema di controlli?

L'obiettivo è quello di offrire spunti operativi su come impostare un modello di organizzazione centrando l'attenzione su quella che è la valutazione del rischio-reato necessaria per poter definire un sistema di controlli idoneo a prevenire il rischio o quantomeno ridurlo a rischio accettabile, essendo comunque irrealizzabile la sua completa eliminazione.

### 3.1 L'approccio basato sul rischio e i protocolli preventivi

Dal punto di vista legislativo, un'indicazione generale su come strutturare un modello organizzativo è data dall'articolo 6 al comma 2. In base a tale comma il modello deve rispondere alle seguenti esigenze:

- a) Individuare le attività nel cui ambito possono essere commessi reati;
- b) Prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) Individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- d) Prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- e) Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Si tratta di **5 esigenze fondamentali** che un modello deve rispettare per poter essere considerato idoneo all'assolvimento del suo compito. A tal proposito possiamo individuare due gruppi di esigenze che delineano due fasi ben precise in cui articolare la costruzione di un modello organizzativo.

La prima fase la possiamo definire come *valutazione del rischio* e comprende il concetto indicato al punto a) del comma 2 dell'articolo 6 del decreto, mentre la seconda fase, che comprende tutti gli altri punti indicati dalla norma in questione, si sostanzia in un insieme di *protocolli preventivi* da adottare per poter controllare i rischi-reato.

Nella costruzione di un modello organizzativo la valutazione e la misurazione dei vari rischi rappresentano due passaggi fondamentali per poter rispondere nel modo più efficiente possibile al trattamento degli stessi. Senza una corretta valutazione e misurazione del rischio si potrebbe incorrere in un'attuazione errata di misure di prevenzione: si potrebbero infatti attuare misure uguali rispetto a rischi differenti e viceversa, con la conseguenza che si darebbe vita a modelli organizzativi inadeguati, dotati di protocolli inutili rispetto a rischi irrilevanti, ovvero con protocolli poco efficaci e non in grado di far fronte a rischi che meriterebbero una risposta più attenta e dettagliata<sup>1</sup>.

Terminata la fase di valutazione del rischio e individuato il grado di esposizione dell'ente allo stesso, si passa alla definizione dei protocolli necessari a ridurlo. Nello specifico, poiché

---

<sup>1</sup>In questo caso verrebbe meno il requisito di specificità e concretezza richiesto per la costruzione di un modello.

dal punto di vista pratico non è possibile azzerare completamente il rischio, l'obiettivo di questi protocolli non è quello di cancellare l'eventualità che un reato possa essere commesso, ma bensì di ridurre la probabilità di commissione a un livello più basso: il cosiddetto rischio accettabile<sup>2</sup>.

In particolare i protocolli in questione devono svilupparsi sulla base delle seguenti fasi:

- Fase di iniziativa;
- Fase di parere;
- Fase di decisione;
- Fase di esecuzione.

Procedendo con un sistema di creazione di protocolli suddiviso per fasi, le attività in essi regolate sono controllabili. In altre parole le operazioni che vengono compiute dall'operatore saranno sempre tracciabili e di conseguenza ricostruibili in ogni momento successivo nel tempo, rispetto all'attimo in cui le stesse sono state compiute.

Sulla base di queste premesse si conviene che il modello organizzativo disciplinato dal decreto 231/01 diventa uno strumento utile per l'ente in quanto da una parte assicura la legalità nella gestione dell'attività imprenditoriale e dall'altra assicura efficienza nelle strategie di business, rappresentando, in questa maniera, un'opportunità di crescita aziendale oltre che di prevenzione di potenziali illeciti.

---

<sup>2</sup>Anche le linee guida di confindustria affermano che "concetto nodale nella costruzione di un sistema di controllo preventivo è quello di rischio accettabile".

### 3.1.1 L'approccio basato sul rischio

Quando si parla di valutazione del rischio si fa riferimento a quel particolare processo volto ad individuare le cosiddette aree sensibili nel cui ambito possono essere commessi i reati.

La valutazione del rischio rappresenta l'attività centrale all'interno del processo di risk management il cui obiettivo è quello di misurare e valutare i fattori di rischio<sup>3</sup> attribuendo a ciascuno di essi una probabilità di realizzazione. In altre parole l'attività in questione si può definire come il processo che porta alla stima dei fattori di rischio associati a determinate operazioni svolte all'interno dell'istituto bancario.

Il processo di valutazione del rischio qui esposto avviene attraverso un metodo particolare definito come process oriented e risk based come di seguito riportato in figura.

<p><b>Analisi del rischio</b></p>	<ul style="list-style-type: none"> <li>• Mappatura e analisi dei processi con riferimento al contesto interno ed esterno</li> <li>• Individuazione delle aree di rischio</li> <li>• Identificazione dei rischi che caratterizzano le fasi/attività aziendali suddivise per ambiti di controllo</li> <li>• Valutazione del livello di esposizione al rischio</li> </ul>
<p><b>Trattamento del rischio</b></p>	<ul style="list-style-type: none"> <li>• Definizione della priorità di trattamento del rischio</li> <li>• Definizione dell' action plan per ogni area – evento di rischio</li> </ul>

Figura 3.1: **Il process oriented e risk based**  
(Fonte: Infocamere.it)

Nello specifico, è possibile individuare quattro fasi salienti così classificate<sup>4</sup>:

- Identificazione delle attività;
- Individuazione delle minacce e dei fattori di rischio;
- Valutazione e attribuzione del livello di rischio;
- Classificazione delle attività in base al rischio potenziale.

<sup>3</sup> Si precisa che nel presente contesto per rischio si intende un evento che può provocare effetti pregiudizievoli per l'ente e nello specifico il rischio di commissione di reati contemplati dal decreto 231/01.

<sup>4</sup>Come da circolare 83607/2017 della Guardia di Finanza.

- ***a) Identificazione delle attività***

Nella valutazione del rischio la prima fase, relativa all'identificazione delle attività e dei processi, rappresenta una sorta di scissione dell'organizzazione aziendale. Questa attività prevede, infatti, un'approfondita analisi dell'ente al fine di individuare tutti quei processi per i quali sussiste il rischio di commissione di reati presupposto contemplati dal decreto 231/01.

In questa fase si esamina la struttura organizzativa della banca, si analizzano le procedure utilizzate, si effettua la mappatura dei processi interni e si controlla tutta la documentazione in grado di fornire informazioni utili ai fini dell'individuazione dell'attività considerata rischiosa.

Inoltre con questa analisi si identificano i soggetti ritenuti responsabili dei processi aziendali e si svolgono delle interviste, attraverso questionari di controllo interno, con lo scopo di delineare con precisione qual è l'organizzazione aziendale.

- ***b) Individuazione delle minacce e dei fattori di rischio***

Con questa fase viene realizzato l'elenco di tutti i potenziali rischi che possono coinvolgere la responsabilità dell'istituto di credito. In particolare ogni rischio viene attribuito alla singola attività o al singolo processo: la finalità è quella di evidenziare le possibili modalità di commissione dei reati presupposto rispetto al contesto aziendale.

Con riferimento al rischio di commissione di illeciti legati alla salute e alla sicurezza sul luogo di lavoro, bisogna considerare quanto stabilito dal decreto 81/2008 ai sensi del quale i rischi lavorativi devono essere comunque integralmente eliminati in relazione alle conoscenze acquisite, in base al progresso tecnico e, ove ciò non sia possibile, ridotti al minimo e, quindi, gestiti.

- ***c) Valutazione e attribuzione del livello di rischio***

La terza fase del processo richiede l'assegnazione di un determinato valore alle diverse categorie di rischio individuate. In modo particolare si procede con l'attribuzione di un peso specifico alle diverse categorie di rischio e alla successiva valutazione dei singoli fattori di pericolo per ogni singola attività individuata.

I criteri di valutazione che vengono utilizzati possono variare da banca a banca e possono portare all'utilizzo di una scala valori composta, ad esempio, dai tre ai cinque elementi quali il rischio trascurabile, il rischio basso, il rischio medio, il rischio effettivo e il rischio alto.

Per quanto riguarda, invece, le componenti principali che vengono utilizzate in questa fase di valutazione, troviamo la probabilità di accadimento dell'evento e la gravità del danno in termini di conseguenze dovute al verificarsi del reato presupposto. Si possono, infatti, individuare danni in termini di immagine alla banca ovvero danni in termini economici. Con particolare riferimento alla probabilità di accadimento del reato, questa dipende fortemente dalla fattispecie di attività a rischio, dalla frequenza di esecuzione e dall'efficacia del sistema di controlli interni dell'istituto di credito.

- ***d) Classificazione delle attività in base al rischio inerente***

Terminata la fase di valutazione del livello del rischio è possibile stabilire quali attività sono potenzialmente più soggette alla commissione di illeciti. In questa fase si può, pertanto, stabilire una sorta di priorità di intervento sulle singole attività il cui obiettivo è quello di verificare che tipi di controllo vengono eseguiti e quali azioni sono intraprese dal top management per la riduzione del rischio.

In conclusione il risultato che si ottiene dal processo di valutazione del rischio è quello di avere una mappatura delle singole attività aziendali classificate in base al livello di rischio che gli viene attribuito. Va precisato che le attività con rischio maggiore richiedono un'attenzione prioritaria e specifici interventi di controllo.

Inoltre il processo sopra descritto deve essere costantemente sottoposto a verifiche continue e metodiche utilizzando personale specializzato e, se possibile, utilizzando tecniche e procedure di auto valutazione assistita.



### 3.1.2 I protocolli preventivi

L'articolo 6, comma 2, lettera b) del decreto 231/01 stabilisce che il modello di organizzazione debba prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire. In base a tale comma il modello deve individuare con precisione tutte quelle attività di verifica che l'ente è tenuto a porre in essere dando vita ad un sistema di controlli interni, i cosiddetti protocolli, il cui obiettivo è quello di impedire la commissione di reati presupposto.

Questa attività dovrà essere svolta su tutti quei processi che sono stati rilevati nella fase precedente ossia durante la fase di risk assessment.

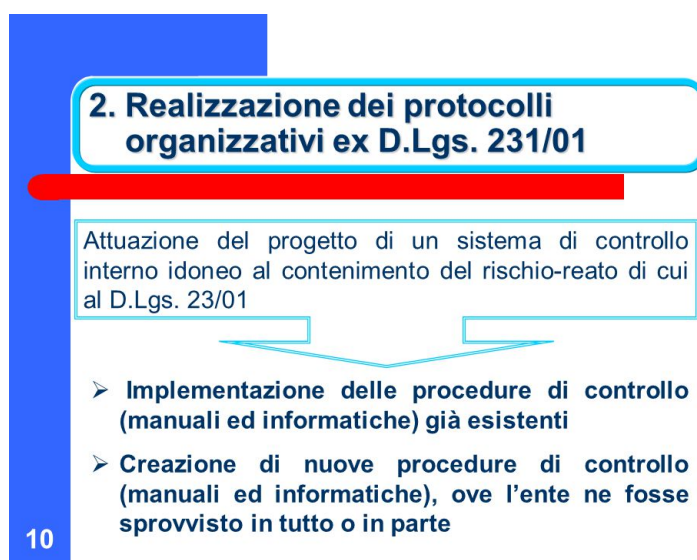


Figura 3.2: **Realizzazione di protocolli**  
(Fonte: Slideplayer.it)

Nello specifico l'attività che porta alla creazione del sistema di controlli interni si articola in quattro fasi<sup>5</sup>:

- Descrizione formalizzata e di dettaglio delle attività a rischio;
- Individuazione e descrizione delle attività di controllo implementate;
- Individuazione e descrizione dei controlli carenti ed inesistenti;
- Verifiche per esaminare la conformità dei comportamenti effettivi confrontandoli con quelli previsti nel modello.

<sup>5</sup>Come da circolare 83607/2017 della Guardia di Finanza.

- *a) Descrizione formalizzata e di dettaglio delle attività a rischio*

Il primo passo da compiere per poter valutare in maniera corretta l'adeguatezza dei protocolli consiste in una rilevazione minuziosa di tutti i processi che sulla carta si possono considerare a rischio di commissione di illecito.

Durante questa fase l'obiettivo è quello di effettuare una ricognizione generale ovvero una raccolta di tutte quelle informazioni utili sui processi da esaminare.

In altri termini ogni singolo processo viene analizzato e studiato nel suo complesso e tutte le informazioni ad esso relative, vengono raccolte in un database e utilizzate nella fase successiva.

La ricognizione, poco fa menzionata, può essere svolta attraverso l'uso di diverse tecniche. Tra queste, quelle maggiormente utilizzate sono le seguenti:

- Interviste ai soggetti coinvolti nel processo;
- Utilizzo di questionari appositi per la raccolta di informazioni relative al processo<sup>6</sup>;
- Osservazioni sul posto;
- Studio e comparazione delle relazioni tra informazioni finanziarie e non;
- Analisi delle procedure;
- Creazione di diagrammi di flusso necessari per una descrizione più schematica dei processi.

L'obiettivo primario in questa attività è quello di formalizzare un quadro dettagliato su come i processi vengono messi in atto, su chi sono i soggetti che vi prendono parte e in quali fasi questi intervengono.

- *b) Individuazione e descrizione delle attività di controllo implementate*

Durante la fase di ricognizione particolare importanza deve essere attribuita all'attività di controllo realizzata dal management. In buona sostanza si devono sottolineare quali strumenti di controllo sono stati introdotti al fine di assicurare il rispetto di quanto stabilito dal decreto 231/01.

I controlli che il management può implementare si contraddistinguono in:

- Controlli preventivi, utilizzati per evitare il verificarsi di eventi negativi;
- Controlli rivelatori, volti a individuare anomalie di processo;

---

<sup>6</sup>I cosiddetti ICQ Internal Control Questionnaires

- Controlli direttivi, volti a indirizzare il processo in una certa direzione;
- Controlli correttivi, diretti a impedire che si verifichino conseguenze negative al verificarsi di un problema;

Classificare i controlli in questo modo permette all'istituto di credito una valutazione degli stessi più omogenea e agevole.

• *c) Individuazione e descrizione dei controlli carenti ed inesistenti*

Una volta individuati e classificati, i controlli devono essere valutati in base alla loro efficacia e adeguatezza. L'obiettivo principale in questa fase è quello di verificare e individuare quali possono essere le parti più carenti del sistema di controlli interno.

Con questa valutazione, prima di tutto si esegue una verifica sull'effettiva applicazione dei controlli per cercare di capire che il controllo sia presente e non venga escluso durante l'attività svolta. In seconda battuta si cerca di individuare quali possono essere considerati controlli carenti o addirittura inesistenti mettendo a confronto processi controllati con situazioni ipotetiche o attese. Lo scopo è quello di migliorare e adeguare il sistema di controlli interni affinché sia il più compatibile con lo svolgimento dell'attività dell'ente.

• *d) Verifiche per esaminare la conformità dei comportamenti effettivi confrontandoli con quelli previsti nel modello*

Una volta terminata la fase precedente, si procede con una verifica volta a esaminare la conformità dei comportamenti adottati con quanto stabilito e previsto dal modello. La verifica in questione viene svolta attraverso l'uso dei seguenti strumenti:

- Interviste di dettaglio;
- Questionari;
- Comparazione di documenti;
- Verifica diretta del patrimonio;
- Osservazioni sul comportamento dei soggetti coinvolti nel processo;
- Verifica delle procedure.

Quest'ultima fase è necessaria in quanto eventuali anomalie emerse durante lo svolgimento dell'attività siano risolte in maniera efficace e tempestiva evitando il protrarsi delle stesse nel tempo con possibili conseguenze negative per l'intera organizzazione aziendale.

### 3.2 Il rischio inerente e il rischio residuo

Il rischio, in via del tutto generale, si definisce come l'eventualità di subire un danno connessa a circostanze più o meno prevedibili. Ciò nonostante, esistono molteplici definizioni di rischio che dipendono dal contesto e dalle applicazioni considerate. In particolare la definizione di rischio dipende dal contesto del danno e dal suo metodo di misura.

In ambito 231/01 siamo interessati all'analisi di un duplice concetto di rischio: il rischio inerente e il rischio residuo.

Il **rischio inerente** è il rischio presente in ogni attività e in ogni processo prima di applicare qualsiasi forma di controllo o altro fattore di mitigazione previsto dal modello di organizzazione. La valutazione del rischio inerente richiede che siano considerati contemporaneamente due fattori tra loro strettamente correlati ovvero la probabilità che un evento negativo, indipendentemente dal sistema di controlli adottato, si verifichi, e l'impatto che questo avrà sull'attività aziendale. Nel primo caso si parla di probabilità di accadimento mentre nel secondo caso ci si riferisce alla gravità del danno.

Il **rischio residuo**, invece, si può definire come il livello di rischio rimanente una volta applicate e introdotte tutte le misure di controllo e mitigazione, previste dal modello, volte a ridurre la probabilità di accadimento e l'impatto di un evento negativo. Si tratta, pertanto, di una tipologia di rischio che ogni istituto di credito è in grado di tollerare e accettare durante lo svolgimento della propria attività. Il livello di rischio residuo dipende fortemente dal sistema di controlli adottato dal management e di conseguenza il suo valore è fortemente legato all'efficacia e dall'efficienza delle misure di controllo e procedure di mitigazione adottate.

I protocolli e le misure di mitigazione del rischio sono rappresentati da presidi, sistemi procedurali, meccanismi di governance, sistemi di deleghe, e flussi informativi.

A titolo esemplificativo i maggiori istituti di credito del nostro paese adottano le seguenti misure di mitigazione:

- Modello di organizzazione;
- Codice etico;
- Organigramma aziendale;
- Sistema dei poteri e delle deleghe;
- Regolamento interno;
- Sistema sanzionatorio;
- Sistema di accesso alle procedure informatiche;

- Utilizzo di sistemi informatici finalizzati alla tracciabilità delle operazioni;
- Procedura per la redazione del bilancio;
- Predisposizione delle comunicazioni sociali, ai soci e ai terzi;
- Regolamento per il funzionamento del servizio cassa;
- Indagini, verifiche e comunicazioni verso la pubblica amministrazione;
- Monitoraggi periodici dell'ODV;
- Flussi informativi all'ODV
- Sistema di segnalazioni all'ODV;
- Piani di formazione periodici;
- Protocollo clausole contrattuali 231/01.

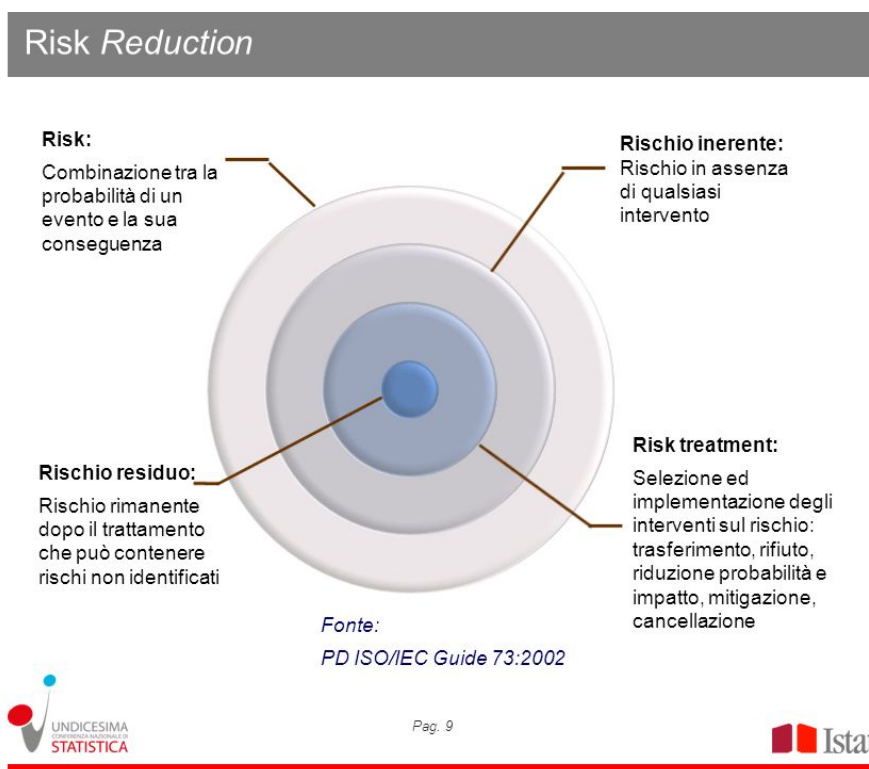


Figura 3.3: **Rischio inerente e rischio residuo**  
(Fonte: Slideplayer.it)

Per gli istituti di credito adottare un sistema interno di controlli efficace è molto importante poiché tale sistema influisce sul valore che viene attribuito al rischio residuo. Infatti, per le banche, ridurre il più possibile il valore di rischio residuo significa ridurre fortemente la probabilità che vengano commessi illeciti previsti dal decreto 231/01 e ciò si traduce in minore responsabilità per l'ente e maggior efficienza organizzativa.

Il valore del rischio residuo dipende quindi dal livello di mitigazione: tanto più basso è il valore di rischio residuo tanto più i protocolli preventivi adottati sono efficaci. In questa situazione la probabilità che l'ente risulti esimente in caso di commissione di reati è elevata poiché quest'ultimi saranno commessi solo in maniera fraudolenta eludendo quanto stabilito dal modello organizzativo.

La scala di valutazione del rischio residuo può articolarsi, ad esempio, su cinque livelli:

1. Rischio residuo **ALTO**;
2. Rischio residuo **MEDIO-ALTO**;
3. Rischio residuo **MEDIO**;
4. Rischio residuo **MEDIO-BASSO**;
5. Rischio residuo **BASSO**.

Nel caso specifico il valore di rischio residuo è determinato come indicato nella tabella che segue.

RISCHIO	DESCRIZIONE
<b>Rischio residuo alto</b>	In passato si sono già verificati eventi negativi e il processo è caratterizzato da elevata esposizione al rischio data la mancanza di idonee misure preventive di controllo
<b>Rischio residuo medio-alto</b>	Il processo è caratterizzato da elevata esposizione al rischio data la mancanza di sufficienti misure preventive di controllo
<b>Rischio residuo medio</b>	Nel processo considerato le misure preventive di controllo sono insufficienti e vi è un rischio medio che si possa commettere un illecito
<b>Rischio residuo medio-basso</b>	L'esposizione al rischio è contenuta data la parziale presenza di misure preventive e protocolli adottati efficaci
<b>Rischio residuo basso</b>	Bassa esposizione al rischio in quanto le misure preventive e i protocolli adottati sono considerati efficaci ed efficienti

Tabella 3.1: *La determinazione del rischio residuo*  
(Fonte: Linee guida confindustria)

In particolare si può notare che nel calcolo, il valore del rischio è fortemente correlato al livello di vulnerabilità. Per *livello di vulnerabilità* si intende l'effettiva presenza e la corretta applicazione di misure preventive di controllo. La vulnerabilità è considerata **alta** se mancano completamente misure preventive di controllo, è **media** se vi è una parziale presenza di misure di controllo o se le misure adottate sono per lo più inefficaci, è **bassa** se le misure preventive di controllo sono presenti e al tempo stesso efficaci.

Per la maggior parte degli istituti di credito solamente un rischio residuo basso è tollerabile e nessun tipo di intervento viene predisposto<sup>7</sup>. Invece qualsiasi processo, a cui viene associato un livello di rischio diverso da quello basso, viene considerato un processo per il quale è bene intervenire e introdurre misure preventive migliorative.

Infine per quanto riguarda la determinazione delle soglie di accettabilità, gli enti prendono in considerazione quanto stabilito dalle linee guida di confindustria. Nello specifico la determinazione di questa soglia viene individuata seguendo il percorso indicato nella figura sottostante:

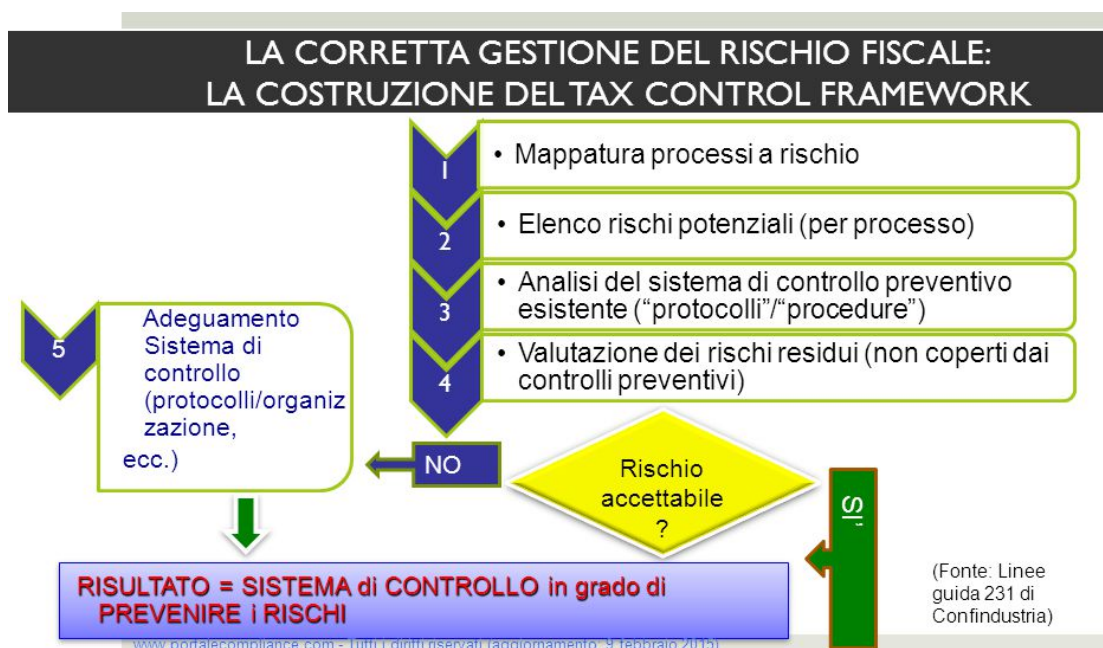


Figura 3.4: **La soglia di accettabilità: determinazione**  
(Fonte: Linee guida confindustria)

<sup>7</sup>A tal proposito i protocolli adottati e le misure preventive risultano idonee e sufficienti a garantire il controllo del processo considerato.

### 3.3 La matrice dei rischi

Uno degli scopi del modello organizzativo è quello di individuare le attività definite sensibili all'interno delle quali possono essere commessi i reati disciplinati dal decreto 231/01. Lo strumento operativo che viene utilizzato per porre in essere questo tipo di attività prende il nome di matrice dei rischi.

Nello specifico l'ente, nel nostro caso un istituto di credito, costruisce la matrice dei rischi procedendo nel modo seguente:

*"Si procede dapprima con la mappatura di tutte le attività aziendali, che vengono suddivise per tipologia, ottenendo le cosiddette aree sensibili; successivamente si individuano tutti i reati che possono essere commessi all'interno di ciascuna area sensibile e si valuta il rischio di commissione degli stessi; poi, per ogni attività individuata, si associa il potenziale reato che può essere commesso; infine si attribuisce per ogni area e attività sensibile una procedura di controllo preventivo."*

Attraverso la matrice dei rischi, sostanzialmente, per ogni attività svolta dalla banca, viene associato il reato che potenzialmente può essere commesso, rendendo più semplice l'attività di controllo dell'ODV. Infatti, lo stesso avrà una visione più specifica e dettagliata delle attività poste in essere dalla banca e in caso di carenze operative che gli vengono segnalate, ha la possibilità di individuare in maniera più rapida ed efficiente dove e come intervenire per colmare questo gap e apportare le migliori del caso.

Per facilitare la costruzione della matrice dei rischi, i reati che generalmente possono essere commessi all'interno di un istituto di credito vengono suddivisi in due grandi tipologie:

- I reati e gli illeciti che possono essere rilevabili nelle attività di gestione e nelle scritture contabili<sup>8</sup>;
- I reati che nulla hanno a che fare con scritture contabili e le operazioni di gestione.

Nel primo caso l'ODV, di comune accordo con l'Internal Auditing, individua le procedure di controllo da porre in essere all'interno di ogni attività di gestione ed effettua verifiche periodiche per individuare eventuali falle dovute ad aggiornamenti normativi e procedurali che le varie attività subiscono. Nel caso sia necessario vengono apportate le migliori al sistema di controllo preventivo procedendo alla sistemazione delle carenze riscontrate.

<sup>8</sup>Rientrano in questa tipologia, ad esempio, fatti di gestione occultati, la produzione di falsa documentazione, alterazione di scritture contabili.



Completamente diversa, invece, è la metodologia che l'ODV deve utilizzare per il secondo gruppo di reati. Infatti, mentre nel caso precedente è richiesta esclusivamente la conoscenza delle procedure e dei sistemi aziendali da parte dell'ODV, ora ciò non è più sufficiente. Infatti è previsto l'intervento di professionalità esterne ben qualificate in grado di offrire assistenza all'ODV in fase di prevenzione dei reati. Basti pensare, per esempio, al tema di sicurezza sul luogo di lavoro. Pertanto è richiesta una collaborazione tra ODV e organi esterni alla banca: collaborazione che deve portare alla definizione di sistemi di controllo preventivi efficaci ed efficienti e che rispettino le normative tempo per tempo vigenti. Collaborazione non sempre facile da realizzare.

Gli istituti di credito ricorrono alla matrice dei rischi per poter valutare con esattezza la pericolosità di un evento negativo e indesiderato al fine di stabilire la priorità o l'urgenza delle misure necessarie per poterlo controllare.

La matrice dei rischi è uno strumento operativo che non deve essere confuso con la raccolta di informazioni, dati di processi aziendali e con la semplice descrizione del reato, ma è uno strumento che utilizza le informazioni raccolte con l'obiettivo di individuare i rischi e schematizzare i potenziali reati che possono essere commessi. Nello specifico la matrice dei rischi individua quali sono i potenziali pericoli attraverso l'analisi delle aree sensibili, stima i potenziali rischi valutando la probabilità di accadimento e la gravità che il danno può causare e infine determina le classi di rischio che vengono associate ad ogni attività.

In questo caso, quando si parla di matrice dei rischi, è bene fornire la definizione di alcuni concetti<sup>9</sup>:

- Il rischio rappresenta il risultato dell'interpretazione della matrice. In modo particolare il rischio (R) rappresenta la pericolosità di un evento e non è altro che il risultato del prodotto tra la probabilità di accadimento (P) e la gravità del danno (G):  $R = P \times G$ .
- La probabilità rappresenta la possibilità che l'evento negativo, in questo caso il reato, si verifichi tenendo conto di tutte le misure di controllo preventivo già poste in essere.
- La gravità del danno, detta anche magnitudo, invece è da intendersi come la gravità delle conseguenze causate dall'evento negativo (reato).

Nella figura sotto riportata si individua la diversa tipologia di rischio che verrà attribuito ad ogni area sensibile individuata. Alla magnitudo viene attribuita una scala di valori crescente che va da bassa ad alta sulla base della minore o maggiore sensibilità del

---

<sup>9</sup>Come da circolare 83607/2017 della Guardia di Finanza.

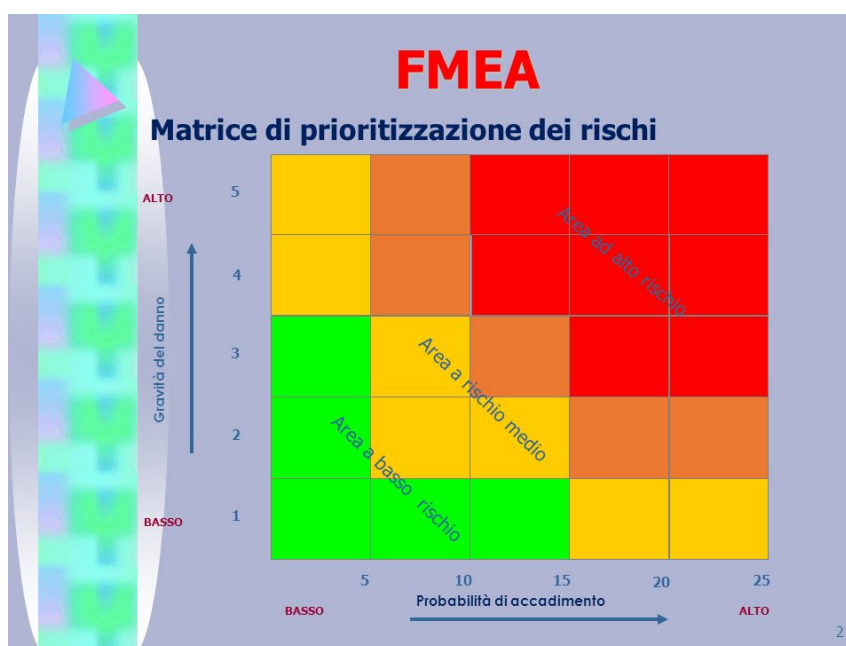


Figura 3.5: La matrice dei rischi  
 (Fonte: Zerounoweb.it)

processo, alla frequenza di esecuzione e alle considerazioni emerse. Sono state, inoltre, prese in considerazione valutazioni circa la tipologia e la gravità di sanzioni che la banca può subire a seguito della commissione di un illecito.

Alla probabilità è stata assegnata la stessa classe di valori prendendo in considerazione i documenti di principio, le procedure utilizzate, i controlli svolti e tutti quei processi volti a mitigare i rischi connessi con la concreta realizzazione dei reati. Il risultato che deriva moltiplicando la probabilità con la magnitudo ci permette di classificare il rischio. Avremmo, pertanto, una scala di rischio che va da un potenziale rischio limitato, dove ad entrambi i fattori è attribuito un valore basso, ad un rischio potenziale estremo, dove ad entrambi i fattori viene attribuito un valore alto.

Una classificazione del rischio per fasce di gravità consente alla banca di individuare le priorità di attuazione e le aree sensibili nelle quali intervenire per mitigare il rischio di commissione di un illecito. Con una classificazione di questo tipo l'istituto di credito può valutare persino azioni di miglioramento in caso di rischi considerati limitati, portando, di conseguenza, un miglioramento all'intero sistema di controlli interni.

## 3.4 Reati presupposto e processi bancari sensibili

In questo passo conclusivo dell'elaborato andrò ad analizzare e sviluppare nel dettaglio quanto stabilito dall'articolo 6 del decreto 231/01. Nello specifico al comma 2 di tale articolo, lettera a), è stabilito che l'ente, e in questo caso la banca, individui le attività nel cui ambito possono essere commessi i reati presupposto.

Con il presente lavoro, partendo dalle aree sensibili, analizzate nel Capitolo 1, procederò ad elencare una serie di reati che possono essere potenzialmente commessi durante lo svolgimento dell'attività bancaria, individuerò i processi aziendali considerati sensibili, ed infine incrocerò ogni reato con i relativi processi aziendali sensibili in modo tale che l'ODV, in caso di illecito, sia in grado di intervenire tempestivamente e possa ricercare e ottenere tutte le spiegazioni e i chiarimenti del caso.

In questo modo l'ODV avrà a disposizione un utile strumento che gli consentirà di rendere più efficace il sistema di controllo interno della banca e, al tempo stesso, di intervenire in maniera più efficiente in caso di commissione di illeciti.

Nel presente lavoro saranno analizzate tutte le aree sensibili per le quali ritengo possano sussistere rischi di commissione di reati, relativamente all'esercizio dell'attività bancaria, già viste nel capitolo primo.

### 3.4.1 Area sensibile 1: reati commessi contro la pubblica amministrazione

Gli articoli 24 e 24-bis del decreto 231/01 esaminano una serie di reati che rientrano nella categoria dei cosiddetti reati "*propri di impresa*", ovvero comportamenti illeciti che si individuano nello svolgimento di un'attività imprenditoriale<sup>10</sup>.

I reati qui analizzati sono i seguenti:

- **Malversazione ai danni dello Stato:** il reato si configura nel momento in cui chi riceve, in maniera lecita, finanziamenti, sovvenzioni o contributi da parte dello Stato o della Comunità Europea per la realizzazione di opere o attività di pubblico interesse, non utilizza le somme per le finalità stabilite. Per quanto riguarda l'attività bancaria, il reato in questione può verificarsi nel caso in cui i contributi siano erogati a favore della banca perché ne fruisca direttamente ovvero nel caso in cui la banca stessa intervenga nel processo di erogazione a favore di soggetti privati.
- **Indebita percezione di erogazioni:** il reato si configura quando, attraverso l'uso o la presentazioni di documenti falsi, si ottengono, senza averne diritto, contributi, finanziamenti, mutui o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato

<sup>10</sup>Garuti G. Contestazione dell'illecito amministrativo e udienza preliminare.

o dalla Comunità Europea. Per questa fattispecie di reato non assume importanza l'uso che viene fatto delle somme percepite poiché il reato stesso si perfeziona nel momento in cui si ottiene il finanziamento. Dal punto di vista bancario il reato può verificarsi quando la banca beneficia delle erogazioni, senza averne diritto, ovvero quando la stessa interviene nel processo di erogazione di finanziamenti a favore di soggetti privati autori di false dichiarazioni e in concorso con gli stessi.

- **Truffa ai danni dello Stato:** il reato si configura nel momento in cui si ottiene un profitto ingiusto attraverso raggiri che inducono in errore e provocano un danno allo Stato. Il reato può configurarsi, ad esempio, quando durante la partecipazione a bandi pubblici, si forniscono informazioni false, allo scopo di aggiudicarsi il bando medesimo.
- **Truffa aggravata per il conseguimento di erogazioni pubbliche:** il reato si configura quando la truffa è finalizzata al conseguimento indebito di erogazioni da parte dello Stato o della Comunità Europea. Il reato in questione si differenzia sia dalla truffa generica, in quanto ha per oggetto l'ottenimento di pubbliche erogazioni, sia dall'indebita percezione di erogazioni, in quanto è previsto il compimento di raggiri atti a indurre in errore l'ente che procede con l'erogazione dei finanziamenti.
- **Frode informatica:** in questo caso il reato consente di ottenere un profitto ingiusto attraverso l'alterazione di un sistema informatico intervenendo sui dati e sui contenuti senza averne diritto. Ai fini del decreto 231/01, il reato assume importanza se e solo se è stato commesso ai danni dello Stato o della Comunità Europea. Dal punto di vista bancario questa ipotesi di reato si configura quando, una volta ottenuto un finanziamento, si viola il sistema informatico della banca al fine di inserire un importo maggiore rispetto a quello ottenuto in modo legittimo.

L'articolo 25 del decreto 231/01 disciplina diverse tipologie di reato che possono essere suddivise in tre sottocategorie secondo un ordine crescente di gravità. Queste sottocategorie sono le seguenti:

- **Concussione:** il reato si manifesta quando un pubblico ufficiale o un incaricato di pubblico servizio, abusando dei suoi poteri, costringe un qualsiasi soggetto a dare o a promettere, a lui o ad un terzo, denaro o altre utilità che non gli spettano<sup>11</sup>. Per la banca, e gli enti in generale, il reato sussiste<sup>12</sup> quando lo stesso è commesso da un soggetto apicale o da un subordinato purché la condotta estorsiva venga eseguita

<sup>11</sup>In questo caso l'abuso di poteri avviene mediante violenza o minaccia di un danno ingiusto, con modalità che non lasciano nessuna alternativa di scelta al soggetto che le subisce. In questo caso tale soggetto viene considerato vittima del reato e pertanto esente da qualsiasi pena.

<sup>12</sup>In questo caso, dalla commissione del reato, deve emergere un interesse ovvero un vantaggio per l'ente.

in concorso con un pubblico ufficiale o un incaricato di pubblico servizio ovvero la condotta venga eseguita nell'esercizio di attività di pubblica rilevanza.

- **Induzione indebita a dare o promettere utilità:** in questa fattispecie di reato il pubblico ufficiale o l'incaricato di pubblico servizio abusano dei loro poteri cercando di condizionare la volontà della controparte, senza esercitare la violenza morale tipica della concussione.
- **Corruzione:** l'elemento rilevante in questa tipologia di reato è dato dal fatto che deve crearsi un accordo tra un pubblico ufficiale o un incaricato di pubblico servizio e un soggetto privato. Questo accordo prevede che i vari soggetti agiscano in posizione paritaria fra di loro e nulla rileva da chi l'iniziativa è partita.
- **Corruzione per l'esercizio della funzione:** il reato si configura nel momento in cui un pubblico ufficiale o un incaricato di pubblico servizio riceve denaro o altra utilità, per se o per altri, in cambio dell'esercizio delle sue funzioni o dei suoi poteri.
- **Corruzione per atto contrario ai doveri d'ufficio:** il reato in questione, detto anche "corruzione propria" consiste in un accordo per la promessa di un compenso indebito riferito ad un atto da eseguirsi o già eseguito, che va contro ai doveri di agente pubblico (ad esempio pagamento di una somma di denaro per assicurarsi l'aggiudicazione di un bando pubblico).
- **Corruzione in atti giudiziari:** in questo caso il fine specifico è quello di favorire o danneggiare una parte in un processo civile, penale o amministrativo.
- **Istigazione alla corruzione:** il reato si configura quando l'offerta di denaro o altra utilità proveniente dal soggetto privato e diretta al pubblico ufficiale o all'incaricato di pubblico servizio non viene accettata.

Dati i reati sopra elencati, le possibili attività bancarie, per le quali sussiste un elevato rischio che siano posti in essere comportamenti illeciti nei rapporti con la pubblica amministrazione, possono essere le seguenti:

- **Stipula dei rapporti contrattuali con la pubblica amministrazione:** a titolo esemplificativo rientrano la stipula di contratti di tesoreria, i finanziamenti diretti ad enti pubblici, stipula di contratti di locazione con enti pubblici, convenzioni per l'erogazione di finanziamenti agevolati.
- **Gestione dei rapporti contrattuali con la pubblica amministrazione:** a titolo esemplificativo rientrano la gestione di convenzioni con enti pubblici per l'offerta di prodotti e servizi bancari rivolta a dipendenti pubblici, gestione di contratti di

tesoreria e servizi di incasso e pagamento, gestione delle imposte in qualità di sostituto d'imposta, gestione di operazioni finanziarie con controparte la Banca d'Italia o il Tesoro, gestione amministrativa delle obbligazioni emesse da enti locali o dallo Stato, pagamento delle pensioni in convenzione.

- **Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la pubblica amministrazione:** a titolo esemplificativo rientrano la gestione dei rapporti con gli enti assistenziali e previdenziali, gestione di rapporti con camera di commercio, amministrazioni statali, regionali, comunali o enti locali, gestione degli accertamenti bancari, gestione dei rapporti con la prefettura, la procura della repubblica, il ministero dello sviluppo economico.
- **Gestione e utilizzo di sistemi informatici:** in questo caso sono coinvolte tutte le strutture della banca che utilizzano sistemi informatici che si interconnettono con software della pubblica amministrazione ovvero con le autorità di vigilanza. Sono, inoltre, interessate le strutture che progettano, realizzano e gestiscono strumenti informatici, tecnologici e di telecomunicazione, ovvero tutte le figure professionali coinvolte nei processi aziendali operanti a qualsiasi titolo<sup>13</sup>.
- **Gestione degli interventi agevolativi:** a titolo esemplificativo rientrano in questa fattispecie di processo i finanziamenti garantiti dal fondo centrale di garanzia istituito presso il Medio Credito Centrale spa, i finanziamenti agevolati e contributi in conto capitale concessi dai ministeri per agevolazioni a progetti di ricerca e sviluppo, i finanziamenti con contributi in conto interessi.
- **Gestione della formazione finanziata:** in questo caso la banca ricorre a finanziamenti e sovvenzioni, concesse da soggetti pubblici, per favorire la formazione del proprio personale. Tra queste tipologie di finanziamento rientrano, ad esempio, quelli concessi dal fondo sociale europeo, dal fondo banche e assicurazioni, dal fondo paritetico interprofessionale nazionale per la formazione dei dirigenti del terziario, dal fondo di solidarietà per il sostegno del reddito e dell'occupazione.
- **Gestione dei contenziosi e degli accordi transattivi:** sono coinvolti, in questo processo, tutte le strutture della banca e tutti quei soggetti che gestiscono contenzioni giudiziali e stragiudiziali ovvero che gestiscono accordi transattivi con enti pubblici o con soggetti privati.
- **Gestione dei rapporti con le autorità di vigilanza:** in questa tipologia di gestione rientrano tutte quelle attività poste in essere durante la fase di segnalazione, comunicazione e richiesta di chiarimenti, rivolte agli organi di controllo e vigilanza esterni alla banca.

<sup>13</sup>In questo caso ci si riferisce sia a dipendenti della banca, sia a qualsiasi altro soggetto che collabora con la banca stessa e utilizza i sistemi informatici trattando dati e patrimonio informativo bancario.

- **Gestione di omaggi, spese di rappresentanza, beneficenze:** in questo caso per *omaggi* si intendono tutte le offerte ricevute che hanno ad oggetto beni di modico valore e che vanno a promuovere l'immagine della banca. Per quanto riguarda le *spese di rappresentanza* si intendono tutte quelle spese sopportate dalla banca durante lo svolgimento di relazioni commerciali destinate a promuovere e migliorare l'immagine della banca stessa. Infine per *beneficienza* si intende qualsiasi erogazione di denaro fatta dalla banca e destinata esclusivamente ad enti senza scopo di lucro.
- **Gestione del processo di selezione e assunzione del personale:** il processo in questo caso si svolge per fasi:
  - analisi delle richieste di assunzione;
  - stesura del profilo del candidato;
  - reclutamento dei candidati;
  - esecuzione del processo selettivo;
  - individuazione dei candidati;
  - formalizzazione dell'assunzione.
- **Gestione del patrimonio immobiliare e dei beni mobili di valore artistico:** in quest'ultimo caso rientrano tutte le attività svolte dalla banca che hanno come obiettivo da un lato, quello di valorizzare il patrimonio immobiliare di proprietà o in locazione, dall'altro quello di valorizzare i beni mobili aventi valore artistico.

Definiti i reati ed elencati i processi bancari sensibili, procedo ora a creare due tabelle che presentano le seguenti caratteristiche:

- Per ogni tabella, nella prima colonna sono riportati i processi bancari per i quali sussiste la possibilità che vengano commessi illeciti;
- Nella prima riga della tabella 3.2 vengono riportati i reati disciplinati dall'articolo 24 e 24-bis del decreto 231/01;
- Nella prima riga della tabella 3.3 sono riportati i reati disciplinati dall'articolo 25 <sup>14</sup> del decreto studiato;

Dalle tabelle sotto riportate si evince quali sono i possibili reati associabili ai diversi processi bancari sensibili. In questo modo l'ODV ha una visione più esaustiva in quanto da un lato è in grado di individuare quali reati possono essere commessi all'interno di ogni

---

<sup>14</sup> Le diverse tipologie di corruzione sono state raggruppate sotto un'unica voce, in quanto il metodo con il quale il reato viene commesso è lo stesso per tutti i tipi di corruzione individuati. A cambiare è il fine del reato, ma ciò non rileva per lo scopo del presente lavoro.

singolo processo, e dall'altro è in grado di intervenire in maniera più efficace utilizzando gli strumenti più adatti per far fronte ad eventuali situazioni di disagio.

In altri termini, l'ODV, qualora volesse apportare delle migliorie al sistema di controlli interni ovvero sanare situazioni negative generate dalla commissione di reati, sarebbe in grado di intervenire con estrema rapidità utilizzando strumenti i più consoni possibile.

Relativamente alla tabella 3.2, va detto che la tipologia di reato concernente la truffa ai danni dello Stato, comprende anche un particolare tipo di illecito: l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mandaci all'autorità giudiziaria.

Tale reato, punito dall' **art. 377-bis c.p.**, costituisce reato presupposto della responsabilità degli enti ai sensi dell'art. 25-novies del Decreto.

Inoltre, ai sensi dell' **art. 10 della L. n.146/2006** può dar luogo alla medesima responsabilità anche se commesso in forma transnazionale<sup>15</sup>.

	Malversazione ai danni dello stato	Indebita percezione di erogazioni	Truffa ai danni dello stato	Truffa aggravata	Frode del sistema informatico
Stipula di contratti con la P.A.			✓		
Gestione di contratti con la P.A.			✓		
Gestione di adempimenti verso la P.A.			✓		
Utilizzo di sistemi informatici		✓	✓	✓	✓
Interventi agevolativi	✓	✓	✓	✓	
Formazione finanziata	✓	✓		✓	
Gestione di contenziosi			✓	✓	

Tabella 3.2: *Processi associati ai reati previsti dall'articolo 24 e 24-bis*

Relativamente alla tabella 3.3, va ricordato che, ai sensi dell'art. **322-bis c.p.**, la condotta del corruttore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i pubblici ufficiali e gli incaricati di pubblico servizio

<sup>15</sup>Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché sia commesso in più di uno Stato; ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; ovvero sia commesso in uno Stato, ma abbia effetti sostanziali in un altro Stato".



nell'ambito della pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda:

- Soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli enti costituiti sulla base dei trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'unione europea;
- Soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore o il soggetto indotto persegua un indebito fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica.).

	Concessione	Induzione indebita	Corruzione	Istigazione alla corruzione
Stipula di contratti con la P.A.		✓	✓	
Gestione di contratti con la P.A.	✓	✓	✓	
Gestione di adempimenti verso la P.A.		✓	✓	
Utilizzo di sistemi informatici		✓	✓	
Interventi agevolativi	✓	✓	✓	
Formazione finanziata		✓	✓	
Gestione di contenziosi		✓	✓	✓
Gestione di rapporti con A.V.		✓	✓	✓
Gestione di omaggi, spese rappresentanza e beneficenza		✓	✓	✓
Gestione del personale		✓	✓	✓
Gestione immobiliare		✓	✓	✓

Tabella 3.3: *Processi associati ai reati previsti dall'articolo 25*

Infine, va specificato che alcuni processi bancari presenti in tabella 3.3 sono stati volutamente esclusi in tabella 3.2. I reati disciplinati dall'articolo 24 del decreto 231/01

hanno possibilità davvero remote di essere commessi durante i processi che riguardano la gestione dei rapporti con le autorità di vigilanza, la gestione di omaggi, spese di rappresentanza e beneficenza, la gestione del personale e la gestione del patrimonio immobiliare. Infatti queste tipologie di processi richiedono la collaborazione tra banca e soggetti privati escludendo quasi del tutto la partecipazione di enti o soggetti pubblici.

### 3.4.2 Area sensibile 2: reati di falsità in moneta, riciclaggio e autoriciclaggio

L'articolo 25-bis del decreto 231/01 disciplina tipologie di reato che al tempo stesso sono contemplate dal codice penale a tutela della fede pubblica.

In particolare i reati puniti hanno ad oggetto l'alterazione di monete, l'alterazione di banconote e carte emesse dai governi autorizzati, l'alterazione di valori di bollo, carte filigranate e strumenti o segni di riconoscimento riservati al falso nummario<sup>16</sup>.

I reati qui analizzati sono i seguenti:

- **Falsificazione, alterazione, spendita e introduzione nello Stato di monete e banconote:** il reato di falsificazione si configura quando, uno o più soggetti, fabbricano ex novo monete o banconote false. L'alterazione, invece, si manifesta quando alle monete e banconote vere, si attribuisce un valore superiore a quello reale. In entrambi i casi vengono puniti sia coloro che hanno contraffatto o alterato le monete e le banconote, sia coloro che procedono all'introduzione delle stesse nel territorio dello Stato ovvero le mettono in circolazione in qualsiasi modo. È, altresì, punito colui che si procura monete o banconote, contraffatte o alterate, con il fine unico di metterle in circolazione.

Relativamente all'attività bancaria appare difficile che soggetti interni ad una banca diano vita ad attività di contraffazione o alterazione di monete o banconote con l'obiettivo di portare un interesse alla banca stessa. Rischi maggiori di commissione di illeciti si possono riscontrare, sempre con riferimento all'attività bancaria, per quanto riguarda l'ipotesi di messa in circolazione di banconote o monete falsificate. Soggetti interni alla banca possono agire in maniera autonoma o di concerto con terzi con l'obiettivo di mettere in circolazione banconote o monete falsificate per l'ottenimento di un interesse o vantaggio personale.

- **Introduzione nello Stato di monete e banconote falsificate e spendita delle stesse ricevute in buona fede:** l'introduzione di monete o banconote falsificate nel territorio dello Stato richiede la consapevolezza o il sospetto di non autenticità

<sup>16</sup>La legge 99/2009 ha modificato l'art. 25-bis, aggiungendo ai reati in tema di falso nummario i reati in tema di contraffazione di marchi, segni distintivi, brevetti e modelli (articoli. 473 e 474 c.p.).

nella persona fisica che attua questa condotta, pur in mancanza di qualsiasi tipo di accordo con il soggetto che ha provveduto alla falsificazione. Nel caso in cui un soggetto riceve, in buona fede, monete o banconote falsificate, il reato si manifesta nel momento in cui le stesse vengono messe in circolazione e contestualmente viene a mancare la buona fede.

In quest'ultima tipologia rientra, ad esempio, l'operatore bancario di sportello che, pur ricevendo in buona fede banconote o monete falsificate, con l'obiettivo di evitare pregiudizi o semplici fastidi operativi derivanti dall'obbligo di denunciare la falsità, le mette in circolazione.

- **Falsificazione di valori di bollo:** si tratta di una fattispecie di reato che avviene molto raramente dato il venir meno l'utilizzo di questi valori.

L'articolo 25-octies, a seguito dell'introduzione del decreto antiriciclaggio<sup>17</sup>, ha esteso la responsabilità dell'ente, soprattutto per quel che concerne l'attività di banca, ai reati di ricettazione, riciclaggio, impiego illecito di denaro nonché autoriciclaggio<sup>18</sup>.

Per quanto riguarda i reati contemplati da tale articolo, fornisco di seguito una breve descrizione:

- **Ricettazione:** il reato si configura quando un soggetto, allo scopo di procurare per se stesso o terze parti un profitto, acquista, riceve od occulta denaro o cose provenienti da un generico delitto, alla cui commissione non ha partecipato. Per questa tipologia di reato è richiesto da un lato il dolo specifico da parte di chi agisce ossia la coscienza e la volontà di ottenere un profitto e dall'altro è richiesta la conoscenza della provenienza delittuosa del denaro o del bene acquistato o ricevuto.
- **Riciclaggio:** in questo caso il reato si configura quando il soggetto agente, che non ha partecipato alla commissione dell'illecito sottostante, sostituisca o trasferisca denaro, beni o altre utilità provenienti da un delitto non colposo, ovvero compia operazioni in grado di ostacolare la loro provenienza delittuosa. In questo caso è punito colui il quale, consapevole della provenienza illecita del denaro o altri beni, cerca di compiere atti tali da rendere difficile la scoperta dell'origine delittuosa dei beni stessi.

Per quanto riguarda l'operatività bancaria, la semplice accettazione di un deposito bancario potrebbe, per esempio, rappresentare una tipica operazione di sostituzione del denaro contante con moneta scritturale, contemplata dal riciclaggio.

<sup>17</sup>Il decreto legislativo 231 del 21 novembre 2007, e il decreto legislativo 109 del 22 giugno 2007, a seguito delle disposizioni comunitarie, hanno rafforzato la normativa in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio di proventi provenienti da attività criminali.

<sup>18</sup>Il nuovo reato di autoriciclaggio è stato inserito nel codice penale e aggiunto ai reati presupposto del decreto 231/01 dalla legge 186/2014, entrata in vigore il 1.1.2015.

- **Impiego di denaro, beni o utilità di provenienza illecita:** il reato si manifesta quando durante una qualsiasi attività economica viene impiegato denaro, beni o altre utilità provenienti da un delitto qualsiasi al di fuori dei casi di concorso nel reato di origine e dei reati di ricettazione e riciclaggio.
- **Autoriciclaggio:** per tale reato risponde chi, avendo compiuto o partecipato di concerto alla commissione di un qualsiasi delitto non colposo, dal quale provengono denaro, beni o altre utilità, su questi proventi compie operazioni di impiego, sostituzione o trasferimento in altre attività economiche, finanziarie o imprenditoriali. Per questa tipologia di reato è altresì richiesta la volontà del soggetto agente di voler ostacolare ad ogni costo l'identificazione delle provenienze delittuose dei beni oggetto di reato.

Per quanto riguarda l'operatività bancaria, se viene commesso questo tipo di reato da un operatore di banca, è prevista un aggravante di pena.

Relativamente ai reati disciplinati dall'articolo 25-octies si devono fare alcune precisazioni. Si tratta, in tutti i casi, di reati che hanno come oggetto di scambio un bene materiale che può essere costituito da denaro, titoli di credito, oggetti preziosi e altri beni in genere. L'oggetto dello scambio deve essere proveniente da un delitto ossia deve rappresentare il profitto o il prezzo atto a istigare il reato. Da aggiungere anche il fatto che alcuni reati attribuibili alla materia fiscale possono essere oggetto di riciclaggio o autoriciclaggio non solo in caso di frodi ma anche nel caso in cui il vantaggio economico derivante da reato sia rappresentato da un risparmio in termini di imposta per mancato esborso di denaro proveniente da attività lecite (per esempio l'omesso o infedele dichiarazione dei redditi). Infine i reati in esame devono essere caratterizzati dalla consapevolezza della provenienza illecita del bene.

Con particolare riguardo all'attività di banca va detto che la stessa, in certe situazioni, e tenendo conto degli indici di anomalia descritti nei provvedimenti della Banca d'Italia, potrebbe essere ritenuta come una circostanza oggettiva grave ed univoca atta a far sorgere il dubbio dell'illecita provenienza del bene.

Dati i reati sopra elencati, le possibili attività bancarie, per le quali sussiste un elevato rischio che siano posti in essere comportamenti illeciti, possono essere le seguenti:

- **Gestione di valori:** tale gestione riguarda tutte le attività che hanno per oggetto la trattazione di valori di qualsiasi natura con particolare riferimento alle banconote, alle monete ed ai valori di bollo aventi corso legale nello Stato e all'estero. Rientrano in questa gestione la movimentazione di valori derivante da operazioni di sportello, cassa continua, gestione del bancomat, la richiesta di nuovi valori, la gestione di banconote e monete sospette di falsità e così via.

- **Gestione di omaggi, spese di rappresentanza, beneficenze:** la definizione di questa tipologia di attività è già stata data nel paragrafo precedente. Ritengo che tale gestione possa essere considerata attività per la quale è possibile venga commesso un reato sopra indicato dato l'oggetto della stessa. È probabile, dunque, che i beni ricevuti siano di provenienza illecita. Anche se le possibilità che ciò accada sono remote, il rischio esiste e non è da sottovalutare.
- **Gestione del patrimonio immobiliare e dei beni mobili di valore artistico:** anche in questo caso la definizione di tale tipologia di gestione è già stata fornita nel paragrafo precedente. Va detto che in fase di gestione del patrimonio immobiliare e non la banca deve effettuare un'attenta valutazione delle controparti contrattuali in genere tenendo conto della possibilità che vengano commessi i reati sopra illustrati.
- **Gestione dei rapporti con la clientela:** il rischio che si verifichino reati individuati nei punti precedenti risulta assai marcato quando si gestiscono i rapporti con la clientela. In particolare possono verificarsi situazioni per le quali la clientela stessa è coinvolta oppure agisce di concerto in attività criminose. Pertanto è bene monitorare con attenzione operazioni di sportello, tutti quei rapporti in essere con la clientela che si possono definire continuativi e tutte quelle operazioni che danno vita a trasferimento di fondi.

Definiti i reati ed elencati i processi bancari sensibili, procedo ora a creare la seguente tabella che nella prima colonna riporta i processi bancari per i quali sussiste la possibilità che vengano commessi illeciti mentre nella prima riga indica i reati disciplinati dagli articoli 25-bis e 25-octies del decreto 231/01.

Per quanto riguarda la gestione di banconote, monete e valori di bollo specifico che per l'operatore di banca è vietato dar vita a comportamenti che possono rientrare nelle fattispecie di reato previste dal decreto analizzato. In particolare è vietato mettere in circolazione valori falsi di qualsiasi tipo ovvero restituire alla clientela valori per i quali sussistono dubbi sulla loro generalità e legittimità.

Per quanto riguarda le altre tipologie di reato va detto che l'operatore di banca è tenuto a non eseguire operazioni, di qualsiasi tipo, quando le stesse si possono considerare sospette e soprattutto se il cliente si rifiuta a fornire le informazioni richieste. Inoltre è vietato trasferire denaro, beni o altre utilità provenienti da illeciti ovvero partecipare o istigare la commissione di illeciti con il fine unico di ottenere un profitto ingiusto.

Infine nel caso in cui operazioni compiute per conto della clientela si possono qualificare come sospette è fatto obbligo per l'operatore di banca procedere senza indugio alla segnalazione dell'operazione alle autorità competenti.

Si tratta di una serie di obblighi che il dipendente di banca è tenuto a rispettare in quanto se si va contro questi adempimenti, avendo piena consapevolezza della provenienza illecita dei beni oggetto delle operazioni, si può essere chiamati a rispondere per i suddetti reati, e potrebbe conseguirne anche la responsabilità amministrativa della banca ai sensi del decreto legislativo 231/01.

	Falsità in valori	Spendita di valori contraffatti	Ricettazione	Riciclaggio e uso illecito di valori	Autoriciclaggio
Gestione di banconote	✓	✓		✓	✓
Gestione di monete	✓	✓		✓	✓
Gestione di valori di bollo	✓	✓		✓	✓
Gestione di omaggi, spese di rappresentanza e beneficenza		✓	✓	✓	✓
Gestione immobiliare			✓	✓	✓
Gestione di rapporti continuativi				✓	✓
Trasferimento di fondi			✓	✓	✓
Operazioni di sportello	✓	✓	✓	✓	✓

Tabella 3.4: *Processi associati ai reati previsti dagli articoli 25-bis e 25-octies*

#### 3.4.3 Area sensibile 3: reati societari e abusi di mercato

L'articolo 25-ter è stato introdotto nel decreto 231/01 nel 2002 attraverso il decreto legislativo 61. Nel corso del tempo tale articolo ha subito numerose modifiche dapprima con la legge 262/05 e poi con la legge 190/2012, fino alla formulazione attuale introdotta dalla legge 69 del 2015. L'articolo considerato disciplina la responsabilità dell'ente per quanto riguarda la commissione di reati societari previsti dal codice civile, libro V, titolo IX. Si tratta di una serie di reati generali che non si possono riferire in maniera specifica all'attività bancaria. I reati che vengono considerati con il presente lavoro hanno per oggetto ambiti diversi e tra questi assumono importanza particolare la formazione del bilancio, le comunicazioni esterne, determinate operazioni sul capitale, l'impedito controllo e l'ostacolo alle funzioni di vigilanza<sup>19</sup>.

<sup>19</sup>Si tratta di una serie di reati che vanno a minare la tutela della trasparenza nella predisposizione di documenti contabili e nella gestione della società in generale.

Relativamente ai controlli posti in essere dalle autorità di vigilanza si rammenta che la banca si pone in una posizione privilegiata per ciò che riguarda l'attuazione dei precetti normativi. In particolare gli istituti di credito sono destinatari di una disciplina speciale che impone loro l'assolvimento di una serie di obblighi e adempimenti in relazione ai rapporti con le autorità di vigilanza.

I reati qui considerati sono i seguenti:

- **False comunicazioni sociali:** il reato è disciplinato dagli articoli 2621 e 2622 del codice civile. Prendendo in considerazione la situazione economica, patrimoniale e finanziaria, il reato in questione si realizza attraverso condotte illecite consapevoli. In particolar modo tali condotte hanno per oggetto:
  - Esposizione di fatti materiali non rispondenti al vero nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico;
  - Omissione di fatti materiali rilevanti la cui comunicazione è richiesta dalla legge;

Si tratta di condotte illecite che possono essere commesse sia da società quotate che da società non quotate. In quest'ultimo caso, tuttavia, si applicano pene attenuate<sup>20</sup> e l'esposizione di fatti materiali falsi rappresenta reato soltanto se contenuta nelle comunicazioni sociali previste dalla legge e i fatti sono considerati rilevanti.

- **Falso in prospetto:** l'articolo 173-bis del decreto legislativo 58 del 1998 punisce la condotta di chi pubblica false informazioni ovvero occulta dati e notizie nei prospetti da esporre ai fini della sollecitazione al pubblico risparmio o dell'ammissione a quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio.

Affinché il reato si concretizzi è necessario che il soggetto che commette la condotta illecita agisca con l'intenzione di ingannare i destinatari dei prospetti, con lo scopo di conseguire un profitto ingiusto per se o per terze persone.

Infine, è indispensabile che le false o le omesse informazioni inducano in errore i loro destinatari. Il reato in questione è disciplinato dall'articolo 2623 del codice civile.

- **Falsità nelle relazioni o nelle comunicazioni delle società di revisione:** il reato, regolamentato dall'articolo 2624 del codice civile, ha per oggetto false relazioni ovvero occultamento di informazioni, da parte dei responsabili della società di revisione, per quanto riguarda la situazione economica, patrimoniale o finanziaria della società sottoposta a revisione. In questo caso chi pone in essere la condotta illecita,

---

<sup>20</sup>È altresì prevista la causa di esclusione della punibilità per ipotesi di particolare tenuità del fatto. In questo caso particolare il giudice valuta in modo prevalente l'entità del danno eventuale cagionato alla società, ai soci o ai creditori.

in maniera consapevole, ha per obiettivo quello di conseguire per sé o per altri un profitto ingiusto.

- **Impedito controllo:** il reato in questione, disciplinato dall'articolo 2625, comma 2 del codice civile, si manifesta quando gli amministratori impediscono ovvero ostacolano, attraverso occultamento di documenti, lo svolgimento dell'azione di controllo attribuita ai soci o ad altri organi societari, procurando danni ai soci. In questo caso l'illecito è punito a querela della persona offesa e la pena può essere aggravata se è stato commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante<sup>21</sup>.
- **Indebita restituzione di conferimenti:** il reato si configura quando la restituzione, anche attraverso operazioni simulate, dei conferimenti dei soci o la liberazione degli stessi dall'obbligo di eseguirli avviene al di fuori dei casi di legittima riduzione del capitale sociale. La normativa disciplina questa condotta all'articolo 2626 del codice civile.
- **Illegale ripartizione degli utili e delle riserve:** reato contemplato dall'articolo 2627 del codice civile. La condotta illecita si ha quando si ripartiscono utili o acconti su utili non effettivamente conseguiti ovvero destinati a riserva. La stessa condotta illecita si manifesta quando si ripartiscono riserve che per legge non possono essere distribuite<sup>22</sup>.
- **Illecite operazioni su azioni o quote sociali o della società controllante:** il reato si configura quando vengono acquistate o sottoscritte, al di fuori dei casi stabiliti dalla legge, azioni o quote sociali proprie e della società controllante, che creano un danno all'integrità del capitale sociale o delle riserve non distribuibili per legge. Il reato in questione è disciplinato dall'articolo 2628 del codice civile.
- **Omessa comunicazione del conflitto di interessi:** reato disciplinato dall'articolo 2629-bis del codice civile che si manifesta quando l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in un mercato regolamentato o diffusi in misura rilevante tra il pubblico, ovvero soggetta a vigilanza ai sensi del TUB o del TUF, non comunica, nelle forme e nei termini previsti dall'articolo 2391

<sup>21</sup>L'art. 2625 c.c. contemplava anche il reato di impedito controllo degli amministratori nei confronti della società di revisione. Con la riforma della disciplina della revisione legale dei conti il reato è stato espunto dall'art. 2625 c.c. e riformulato dall'art. 29 del D.Lgs. n. 39/10 e poi depenalizzato dal D.Lgs. n. 8/16; poiché l'art. 25-ter del D.Lgs. n. 231/01 non è stato conseguentemente modificato con l'inserimento di un richiamo anche al citato art. 29, sembra potersi affermare che l'illecito di impedito controllo nei confronti della società di revisione non rientri più nella disciplina della responsabilità amministrativa degli enti.

<sup>22</sup>Va ricordato che la restituzione degli utili o la ricostituzione delle riserve entro il termine previsto per l'approvazione del bilancio estingue il reato.



del codice civile, l'interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società in questione.

- **Corruzione e istigazione alla corruzione:** soggetti, quali amministratori, direttori generali, dirigenti, sindaci, liquidatori e qualsiasi altra persona fisica investita di funzioni direttive, sollecitano o ricevono denaro o altra utilità non dovuta o ne accettano promessa, al fine di compiere un atto contrario agli obblighi inerenti al loro ufficio o agli obblighi di fedeltà nei confronti della società di appartenenza.
- **Aggiotaggio:** il reato è disciplinato dall'articolo 2637 del codice civile e si perfeziona quando sono diffuse notizie false ovvero poste in essere operazioni simulate il cui obiettivo è quello di cagionare una sensibile alterazione di prezzo di strumenti finanziari non quotati o per i quali è stata presentata una richiesta di ammissione a negoziazione in un mercato regolamentato.
- **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza:** il reato si configura quando si espongono alle autorità di vigilanza comunicazioni e fatti materiali non rispondenti al vero oppure quando si occultano totalmente o parzialmente fatti circa la situazione economica, patrimoniale o finanziarie dell'ente, che dovevano essere comunicati per legge.

Il reato, disciplinato dall'articolo 2638 del codice civile, si manifesta anche mediante qualsiasi condotta attiva che porta a generare un ostacolo allo svolgimento delle funzioni che spettano alle autorità di vigilanza.

L'articolo 25-sexies del decreto 231/01 disciplina i reati riconducibili agli abusi di mercato. In particolare la legge 62 del 2005, ha introdotto agli articoli 184 e 185 del decreto legislativo 58/1998, i reati di abuso di informazioni privilegiate e di manipolazione di mercato.

I reati in questione sono puniti anche se commessi all'estero nel caso in cui abbiano per oggetto strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano.

Per quanto riguarda l'esercizio dell'attività bancaria i maggiori rischi di commissione di reati concernenti abusi di mercato si possono ipotizzare nei seguenti casi:

- Operazioni simulate;
- Abuso di informazioni privilegiate per conto della banca o a favore di clienti della stessa;
- Diffusione di notizie false o fuorvianti legate ad operazioni eseguite sul mercato.

Esiste, inoltre, un obbligo di segnalazione in capo all'intermediario qualora si venisse a conoscenza di operazioni richieste da clienti che facciano sospettare la commissione di una condotta illecita relativa ad abuso di informazioni privilegiate ovvero di manipolazione di mercato.

Pertanto, i reati che vado ad analizzare sono due:

- **Abuso di informazioni privilegiate:** il reato si configura quando un soggetto acquista, vende o compie altre operazioni per conto proprio o di terzi su strumenti finanziari usando informazioni privilegiate di cui è venuto in possesso in qualità di membro degli organi di amministrazione, direzione o controllo, ovvero come membro partecipante al capitale emittente ovvero come partecipante di un'attività lavorativa o professionale della società. La fattispecie di reato si manifesta anche quando i soggetti sopra elencati comunicano informazioni privilegiate al di fuori dell'esercizio del proprio lavoro ovvero quando inducono altri soggetti, sulla base delle informazioni privilegiate di cui dispongono, a compiere determinate operazioni con l'obiettivo di ottenere un profitto ingiusto.

In base a quanto stabilito dall'articolo 181 del TUF, al comma 1, per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

In ambito bancario sono state individuate numerose fattispecie di operazioni nelle quali si possono manifestare elementi di rischio e che possono comportare al tempo stesso la responsabilità della banca nel caso in cui il reato sia commesso nell'interesse della stessa. Basti pensare, ad esempio, all'attività di proprietary trading in base alla quale chi dispone o esegue l'operazione può abusare di un'informazione privilegiata riguardante un determinato emittente cui ha accesso la banca nello svolgimento della propria attività.

- **Manipolazione di mercato:** il reato si configura quando un soggetto diffonde notizie false o pone in essere operazioni simulate idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari disciplinati dall'articolo 182 del TUF.

Dati i reati sopra elencati, le possibili attività bancarie, per le quali sussiste un elevato rischio che siano posti in essere comportamenti illeciti possono essere le seguenti:

- **Gestione dei rapporti con il comitato per il controllo sulla gestione e con la società di revisione:** questa tipologia di gestione vede coinvolti i membri del consiglio di amministrazione e tutti gli organi e le strutture della banca coinvolte

nella gestione dei rapporti con il comitato per il controllo sulla gestione e con la società di revisione in virtù di verifiche e controlli svolti sulla base di quanto stabilito dalla normativa in vigore. In particolare la gestione considerata si articola in diverse attività quali:

- comunicazione delle informazioni periodiche previste per legge;
- comunicazione di informazioni e dati societari e messa a disposizione della documentazione richiesta;

Le varie modalità operative di queste gestione sono indicate nella normativa interna di ogni singolo istituto di credito, sviluppata e aggiornata dalle strutture competenti in materia.

- **Gestione dell’informativa periodica:** questa tipologia di attività spetta a tutte le strutture atte alla predisposizione di documenti che contengono comunicazioni sociali o che sono rivolte al mercato ed hanno per oggetto informazioni inerenti la situazione economica, patrimoniale e finanziaria della banca. La predisposizione dell’informativa periodica avviene sulla base di quanto stabilito dalla legge 262/2005 ed in modo particolare dall’articolo 154-bis del TUF. In base a ciò è prevista la figura del “dirigente preposto alla redazione dei documenti contabili societari” responsabile di fornire una rappresentazione veritiera e corretta della situazione economica, patrimoniale e finanziaria della banca e dell’eventuale gruppo bancario. All’interno di questa gestione particolare interesse assume l’attività volta a produrre il bilancio d’esercizio, il bilancio consolidato, la stesura di prospetti riguardanti la situazione infrannuale dell’istituto, la determinazione degli oneri fiscali e lo svolgimento degli adempimenti relativi alle imposte dirette ed indirette. In altri termini le attività in questione riguardano il processo di gestione della contabilità e delle segnalazioni di vigilanza, il processo di gestione del bilancio d’impresa e del bilancio consolidato e il processo di gestione di adempimenti fiscali.
- **Predisposizione dei prospetti informativi:** per questa tipologia di gestione sono coinvolte strutture bancarie il cui compito è quello di predisporre prospetti informativi richiesti dalla legge ai fini della sollecitazione al pubblico risparmio e per l’ammissione a quotazione nei mercati regolamentati<sup>23</sup>. Nello specifico i prospetti informativi devono contenere informazioni che in base alle caratteristiche dei prodotti finanziari e degli emittenti, sono considerate necessarie affinché gli investitori

---

<sup>23</sup> Ai sensi delle disposizioni previste dal decreto legislativo 58 del 24/02/1998 e successive modifiche (tra cui la Legge 262 del 28/12/2005) e dalla Direttiva 2003/71/CE del 04/11/2003 come recepita nel Regolamento (CE) 809/2004 della Commissione del 29 aprile 2004. Sono considerati sia i prospetti informativi relativi alle emissioni sul mercato domestico, sia quelli relativi alle emissioni di titoli sui mercati internazionali.

possano giungere ad un fondato giudizio sulla situazione economica, patrimoniale e finanziaria del soggetto emittente.

In base alla normativa vigente la predisposizione dei prospetti si articola in quattro fasi:

- Raccolta delle informazioni necessarie alla predisposizione;
- Predisposizione e sottoscrizione dei prospetti informativi;
- Attestazione da parte del dirigente preposto in base all'articolo 154-bis del TUF;
- Inoltro dei prospetti e gestione dei rapporti con le autorità competenti.

Anche in questo caso spetta alle strutture interne competenti stabilire le modalità operative più adatte alla gestione.

- **Acquisto, gestione e cessione di partecipazioni:** le strutture coinvolte in questa gestione svolgono operazioni di acquisto, gestione e cessione di partecipazioni di capitale di altre società ovvero hanno per oggetto altre forme di investimento molto simili all'assunzione di partecipazione<sup>24</sup>. In questo caso il processo prevede per prima cosa un esame di fattibilità dell'operazione e l'individuazione delle opportunità di investimento. Successivamente vengono gestiti i rapporti precontrattuali e il compimento di tutte le attività propedeutiche alla stipulazione del contratto. Si procede poi con la predisposizione e il perfezionamento del contratto ed infine vengono eseguiti tutti gli adempimenti richiesti per legge connessi con l'acquisto, la gestione e la cessione di partecipazioni.
- **Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato:** sono coinvolti in questa gestione gli organi sociali e tutti i dipendenti della banca che hanno accesso ad informazioni privilegiate ovvero che gestiscono le comunicazioni della banca al mercato ed in linea generale all'esterno. Rientra in questa fattispecie anche la diffusione di notizie, dati e informazioni nell'ambito di rapporti di business, di attività di marketing, e tutte le comunicazioni a carattere obbligatorio.

Per quel che riguarda l'attività bancaria le informazioni privilegiate possono avere per oggetto:

- La banca stessa, le sue controllate e gli strumenti finanziari emessi;
- Le società clienti e gli strumenti finanziari da queste emesse;

<sup>24</sup>Rientrano in quest'ultima tipologia, ad esempio, la sottoscrizione di prestiti obbligazionari convertibili o di strumenti finanziari partecipativi.

- Le informazioni trasmesse da un cliente;
- Le informazioni relative agli ordini trasmessi da un cliente.

L'informazione privilegiata può nascere da una decisione che la banca prende internamente ovvero nascere dall'accertamento di eventi o circostanze aventi un riflesso sull'attività bancaria e sul corso degli strumenti finanziari emessi. Può, infine, derivare da attività svolte in nome e per conto di società terze e dallo svolgimento di attività eseguite per conto proprio o di terzi sui mercati finanziari.

- **Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato:** questa gestione coinvolge tutte le strutture e tutto il personale che svolge operazioni di mercato su strumenti finanziari.

Nello specifico il processo in questione riguarda attività di trading che la banca svolge per conto proprio o per conto di terzi e che hanno per oggetto strumenti finanziari indicati dall'articolo 182 del TUF.

Per quanto riguarda il trading eseguito per conto proprio le attività coinvolte sono le seguenti:

- Definizione delle linee guida per la gestione del portafoglio;
- Elaborazione di strategie di investimento;
- Gestione del portafoglio;
- Supporto all'intermediazione in titoli;
- Supporto tecnico per la gestione dei profili finanziari delle partecipazioni azionarie quotate della banca;
- Gestione di operazioni sui mercati di azioni proprie;
- Esecuzione sui mercati di operazioni di negoziazione per la gestione dei portafogli titoli della banca;
- Svolgimento di adempimenti di carattere amministrativo e normativo connessi all'esecuzione di operazioni di negoziazione.

Per quanto riguarda, invece, il trading svolto dalla banca per conto di terzi, come ad esempio l'esecuzione di ordini per conto di clienti, sono previsti controlli in merito alle operazioni richieste al fine di individuare eventuali operazioni sospette strumentali al compimento di un reato o di un illecito amministrativo.

Definiti i reati ed elencati i processi bancari sensibili, procedo ora a creare tre tabelle che presentano le seguenti caratteristiche:

### 3. Attività bancaria e reati connessi con la responsabilità amministrativa dell'ente

- Nella prima riga della tabella 3.5 vengono riportati i reati disciplinati dall'articolo 25-ter del decreto 231/01<sup>25</sup>;
- Nella prima riga della tabella 3.6 vengono riportati i reati disciplinati dall'articolo 25-ter del decreto 231/01;
- Nella prima riga della tabella 3.7 vengono riportati i reati disciplinati dall'articolo 25-ter e 25-sexies del decreto 231/01;
- Per ogni tabella, nella prima colonna sono riportati i processi bancari per i quali sussiste la possibilità che vengano commessi illeciti con riferimento ai reati presi in considerazione<sup>26</sup>;

	False comunicazioni sociali	Falso in prospetto	False comunicazioni alla S.R.	Impedito controllo
Gestione di rapporti con il C.C.	✓		✓	✓
Gestione di rapporti con la S.R.	✓		✓	✓
Gestione di informativa periodica	✓		✓	
Predisposizione di prospetti informativi	✓	✓		
Gestione di partecipazioni		✓		

Tabella 3.5: *Processi associati ai reati previsti dall'articolo 25-ter*

Nella tabella sopra riportata alcune attività bancarie non sono state inserite volutamente. Nello specifico è stata omessa l'attività di gestione di informazioni privilegiate e l'attività di gestione delle operazioni di mercato.

Si tratta di particolari tipologie di gestione per le quali, a mio avviso, è difficile che si possano commettere i reati presupposto indicati in tabella e contemplati dall'articolo 25-ter, avente per oggetto illeciti societari.

Nella tabella che segue, invece, è stata aggiunta una voce tra le attività per le quali sussiste la possibilità che vengano commessi illeciti: si tratta della gestione di operazioni di

<sup>25</sup>In questa riga S.R. sta per Società di Revisione

<sup>26</sup>In tutte e tre le colonne C.C. e S.R. significano rispettivamente Comitato di Controllo e Società di Revisione

mercato. Secondo il mio punto di vista si tratta di una gestione particolare e per la quale l'ODV deve fare molta attenzione. Infatti si tratta di una gestione che interessa ambiti bancari molteplici e di conseguenza la probabilità che venga commesso un illecito aumenta. Compiere operazioni di mercato implica che esistono potenzialmente numerose occasioni per la commissione di reati basti pensare ad esempio l'esecuzione di ordini di compravendita che forniscono indicazioni false in merito all'offerta, alla domanda o al prezzo di strumenti finanziari, ovvero impartizione di ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno, e così via.

	<b>Indebita restituzione di conferimenti</b>	<b>Illegale ripartizione degli utili</b>	<b>Illecite operazioni su azioni o quote sociali</b>	<b>Omessa comunicazione del conflitto di interesse</b>
<b>Gestione di rapporti con il C.C.</b>				✓
<b>Gestione di rapporti con la S.R.</b>				✓
<b>Predisposizione di prospetti informativi</b>		✓	✓	✓
<b>Gestione di partecipazioni</b>	✓	✓	✓	✓
<b>Gestione di informazioni privilegiate</b>				✓
<b>Gestione di operazioni di mercato</b>	✓	✓		✓

Tabella 3.6: *Processi associati ai reati previsti dall'articolo 25-ter*

Nella tabella 3.7, che segue, sono state aggiunte, rispetto a quanto riportato nelle precedenti, entrambe le tipologie di reato disciplinate dall'articolo 25-sexies del decreto 231/01. Questa aggiunta è dovuta al fatto che le gestioni introdotte rappresentano potenziali occasioni da sfruttare per poter commettere i reati indicati. Corruzione, agiottaggio, abuso di informazioni privilegiate e manipolazione di mercato sono reati che possono essere commessi durante l'esercizio di queste attività e pertanto l'ODV, quale organo di vigilanza, deve creare un sistema di controlli adeguato al fine di limitare il più possibile il rischio di commissione di condotte criminose. Infatti, proprio per la particolare natura di queste attività, all'interno di alcuni tra i maggiori istituti di credito del nostro paese, per le operazioni di trading ed altre attività di negoziazione, concluse dal cliente per conto proprio, è presente una procedura a sostegno dell'ODV: si tratta di un procedimento automatico di controllo che va a selezionare operazioni poste in essere dal cliente e che si possono definire sospette.

In questo modo si rafforzano i controlli e si limita ulteriormente il rischio di commissioni di illeciti.

	Corruzione	Agiotaggio	Ostacolo alle autorità di vigilanza	Abuso di informazioni privilegiate e manipolazione di mercato
Gestione di rapporti con il C.C.			✓	
Gestione di rapporti con la S.R.			✓	
Gestione di informativa periodica	✓	✓	✓	✓
Predisposizione di prospetti informativi		✓		✓
Gestione di partecipazioni	✓	✓		✓
Gestione di informazioni privilegiate	✓	✓		✓
Gestione di operazioni di mercato	✓	✓		✓

Tabella 3.7: *Processi associati ai reati previsti dall'articolo 25-ter e 25 sexies*

#### 3.4.4 Area sensibile 4: reati informatici, contro l'industria e contro il commercio

Con riferimento al decreto 231/01 la criminalità informatica è disciplinata dall'articolo 24-bis. Si tratta di un articolo introdotto dalla legge 48 del 18 marzo 2008 e che elenca una serie di reati informatici che possono dar luogo alla responsabilità amministrativa degli enti e della banca nel caso studiato.

Tale legge ha, inoltre, modificato parte del codice di procedura penale con lo scopo di agevolare le indagini e le operazioni di sequestro dei dati informatici, imponendo alle autorità preposte di adottare misure tecniche volte a garantire la conservazione dei dati originali ed ad impedirne, al tempo stesso, l'alterazione.

Si illustrano di seguito i reati disciplinati dall'articolo 24-bis:

- **Accesso abusivo ad un sistema telematico o informatico:** il reato in questione, contemplato dall'articolo 615-ter del codice penale, si configura quando si accede



abusivamente ad un sistema informatico o telematico protetto anche senza scopo di lucro o danneggiamento del sistema.

In un contesto bancario il reato può essere commesso anche da un dipendente o da un collaboratore esterno alla banca che, pur essendo in possesso di credenziali di accesso, acceda a parti precluse ovvero vi acceda senza esserne legittimato.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche:** l'articolo che disciplina questa condotta è il numero 617-quater del codice penale. Il reato si manifesta quando si intercettano in modo fraudolento comunicazioni relative ad un sistema informatico o telematico ovvero si impediscono o interrompono le comunicazioni stesse.
- **Danneggiamento di informazioni, dati e programmi informatici:** l'articolo 635-bis del codice penale punisce chiunque distrugge, deteriora, cancella, altera o sopprime, informazioni, dati o programmi informatici di altri.
- **Danneggiamento di sistemi informatici o telematici:** il reato, disciplinato dall'articolo 635-quater si configura quando un soggetto, attraverso condotte illecite descritte dall'articolo 635-bis, distrugge, danneggia o rende inservibili sistemi informatici o telematici altrui.
- **Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici:** la fattispecie di reato è normata dall'articolo 615-quater che punisce chiunque si procura in modo abusivo, riproduce, diffonde o consegna codici idonei all'accesso di un sistema protetto da misure di sicurezza. In questo caso chi commette il reato lo fa per ottenere un profitto, per se o per altri, ovvero per commettere un danno ad altri soggetti.
- **Falsità nei documenti informatici:** il reato è disciplinato dall'articolo 491-bis del codice penale ed ha per oggetto la falsità materiale o ideologica commessa da un pubblico ufficiale o da un privato, la falsità in registri e notificazioni, la falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità. In base all'attuale normativa il documento informatico risulta svincolato dal relativo supporto materiale che lo contiene, poiché l'elemento penale determinante consiste nell'attribuire allo stesso un'efficacia probatoria secondo le norme civilistiche. Nello specifico il falso materiale potrebbe compiersi attraverso l'uso di firme elettroniche altrui.
- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica:** il reato si configura dal soggetto che presta servizi di certificazione di firma elettronica. Questo agisce con lo scopo di procurare per se o altri un profitto

ingiusto violando gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Per quanto riguarda l'operatività bancaria si ricorda che la banca riveste la qualifica di "certificatore qualificato"<sup>27</sup>.

Tra le diverse fattispecie di reati informatici elencati va detto che molti potrebbero non presentare il requisito della commissione nell'interesse o a vantaggio della banca, indispensabile affinché possa conseguire la responsabilità amministrativa della stessa. Tuttavia si ricorda che qualora fossero integrati tutti gli elementi previsti dal decreto legislativo 231/2001 la responsabilità della banca potrebbe sorgere, secondo la previsione contenuta nell'articolo 8 del decreto, anche quando l'autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt'altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati che rendono assai difficile anche l'individuazione del luogo dove il reato stesso possa ritenersi consumato.

Per quanto riguarda i reati contro l'industria e contro il commercio, la legge 99 del 23 luglio 2009 ha introdotto nel decreto studiato due articoli fondamentali: l'articolo 25-bis-1 e l'articolo 25-novies. I reati disciplinati da questi articoli sono molteplici, tuttavia ai fini di questo lavoro verranno approfonditi solo i seguenti:

- **Turbata libertà dell'industria e del commercio:** si tratta di un reato contemplato dall'articolo 513 del codice penale e che consiste nel compiere azioni violente su cose e oggetti ovvero nell'utilizzo fraudolento degli stessi al fine di ostacolare il regolare svolgimento di un'attività commerciale. Ad esempio rientra in questa categoria di reato l'inserimento del codice sorgente nel proprio sito internet in modo tale da essere più visibili nei motori di ricerca.
- **Illecita concorrenza con minaccia o violenza:** commette questo reato chi compie atti di concorrenza facendo ricorso a violenza o minacce. Tale norma trova applicazione anche nei confronti di quei reati che vanno al di fuori della criminalità mafiosa. Nello specifico si intende contrastare atti diretti a impedire o limitare l'intervento sul mercato di soggetti concorrenti. L'illecito si configura anche quando le violenze o le minacce sono poste in essere da terzi per conto del titolare d'azienda oppure quando non sono rivolte al concorrente ma ai suoi potenziali clienti. In ambito bancario il reato in questione potrebbe configurarsi quando si minaccia un cliente affermando di applicare condizioni economiche peggiorative ovvero di revocare i crediti concessi.

<sup>27</sup>Per certificatore qualificato si intende, ai sensi dell'art. 1 lettere e) ed f) del decreto legislativo 82 del 2005, l'attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare le firme elettroniche, che sia conforme ai requisiti stabiliti dall'allegato I della direttiva 1999/93/CE, rilasciato da certificatori ossia soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi con quest'ultime e che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

Dati i reati sopra elencati, le possibili attività bancarie, per le quali sussiste un elevato rischio che siano posti in essere comportamenti illeciti possono essere le seguenti:

- **Gestione ed utilizzo dei sistemi informatici:** questa attività coinvolge le strutture atte alla gestione e l'utilizzo di sistemi informativi che interconnettono software della pubblica amministrazione ovvero delle autorità di vigilanza, le strutture deputate alla progettazione di strumenti informatici e le strutture che hanno responsabilità di realizzare interventi organizzativi, normativi e tecnologici.

Nello specifico e ai sensi del decreto 231/01 sono vietate, a titolo esemplificativo e per tutti i dipendenti di banca e collaboratori esterni, le seguenti attività:

- introdursi abusivamente nel sistema informatico bancario;
  - accedere al sistema informatico e alla banca dati della banca senza possedere le credenziali di accesso;
  - intercettare in modo fraudolento comunicazioni relative al sistema bancario informatico;
  - utilizzare dispositivi tecnici o software non autorizzati;
  - cancellare o distruggere informazioni e dati informatici altrui;
  - detenere o riprodurre abusivamente codici di accesso;
  - alterare documenti informatici;
- Con riferimento ai reati contro l'industria e il commercio, per ciò che concerne l'attività bancaria i rischi di commissione di illeciti possono presentarsi nei **rappor- ti con la clientela**, con particolare riferimento alla concessione di finanziamenti a favore di soggetti coinvolti in attività illecite, nella **partecipazione a gare pubbliche**, con riguardo a comportamenti illeciti nei confronti di partecipanti e nell'**approvvigionamento o nell'utilizzo di prodotti, software e banche dati** strumentali all'attività bancaria o destinati ad omaggi per la clientela.
  - **Gestione delle procedure acquisitive dei beni e dei servizi:** il processo in questione coinvolge tutte le strutture della banca che si occupano di gestire l'acquisto di beni e servizi necessari per lo svolgimento dell'attività bancaria. Tra i beni sono comprese le opere d'ingegno aventi carattere creativo mentre tra le prestazioni di servizi sono compresi incarichi professionali ovvero incarichi di consulenza.

L'attività considerata si articola in quattro sotto processi:

- definizione e gestione del budget;
- gestione degli approvvigionamenti;
- gestione del ciclo passivo;

– gestione dei fornitori.

Viene ora presentata la tabella 3.8 che mette in relazione i reati disciplinati dal decreto 231/01 per ciò che riguarda illeciti informatici, contro l'industria e contro il commercio, con le possibili attività e processi ritenuti a rischio di commissione di condotte criminose.

Nella prima riga sono riportate le possibili attività a rischio di commissione di illeciti mentre nella prima colonna vengono esposti i reati citati in precedenza.

In questa tabella sono state aggiunte, altresì, attività già analizzate in precedenza, ma che per loro natura si possono considerare sensibili per quel che riguarda il tema trattato in questo paragrafo.

	Gestione di omaggi	Rapporti con la clientela	Acquisto di beni e servizi	Stipula di contratti con la P.A.	Gestione del sistema informatico
Accesso abusivo al sistema informatico	✓		✓		✓
Interruzione illecita di comunicazioni		✓			✓
Lesione del sistema informatico					✓
Diffusione di codici d'accesso			✓		✓
Falsità di documenti informatici	✓	✓	✓	✓	✓
Frode informatica	✓				✓
Illecita concorrenza	✓	✓	✓	✓	
Turbata libertà nel commercio	✓		✓	✓	✓

Tabella 3.8: *Processi associati ai reati previsti dagli articoli 24-bis, 25-bis-1 e 25-novies*

### 3.4.5 Area sensibile 5: reati con finalità di terrorismo e criminalità organizzata

Nel sistema di responsabilità amministrativa degli enti, numerose norme nel corso degli anni hanno introdotto diverse categorie di illeciti con l'obiettivo di contrastare fenomeni

che destano particolare allarmismo a livello internazionale, soprattutto in relazione a reati di natura politico-terroristica.

Da sempre il settore bancario dedica molta attenzione ed impegno nel cercare di prevenire fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo con lo scopo di garantire una sana e prudente gestione dei comportamenti e del buon finanziamento del sistema economico nel suo insieme. Infatti, risulta evidente il rischio di finanziare clientela appartenente a malavita o a forme di delinquenza organizzate e mettere a loro disposizione risorse economiche strumentali per l'esercizio di attività illecite.

I reati che rientrano in quest'ambito si possono raggruppare in quattro grandi macro categorie, le seguenti:

- **Delitti con finalità di terrorismo o di eversione dell'ordine democratico:** l'articolo 25-quater del decreto 231/01 prevede la responsabilità dell'ente nel caso in cui siano commessi reati aventi finalità di terrorismo o eversione dell'ordine democratico purché lo stesso ne abbia tratto un vantaggio o abbia agito per proprio interesse<sup>28</sup>.
- **Delitti di criminalità organizzata:** rientrano in questa fattispecie di delitti tutti quei reati legati alle varie forme di associazioni criminose quali le associazioni per delinquere generiche, le associazioni di stampo mafioso, e le associazioni a delinquere con finalità di traffico illecito di sostanze stupefacenti e commissione di delitti in tema di schiavitù.

Per ciò che concerne la responsabilità amministrativa dell'ente è sufficiente che la sola consapevolezza di partecipazione ad una forma di associazione sopra menzionata da parte di un dipendente o di un esponente dell'ente, come per esempio una banca, può determinare una responsabilità per l'ente stesso. È tuttavia necessario che la partecipazione all'associazione crei un vantaggio o rappresenti un interesse per l'ente altrimenti la responsabilità dello stesso viene meno.

- **Delitti transnazionali:** la legge 146 del 2006 è stata introdotta con l'obiettivo di contrastare le organizzazioni criminali che agiscono a livello internazionale. In base a tale legge un reato è da considerarsi transnazionale se si verificano le seguenti caratteristiche:

---

<sup>28</sup>L'art. 270-sexies del codice penale considera connotate da finalità di terrorismo le condotte che possono arrecare grave danno ad un paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto, o di destabilizzare le strutture politiche fondamentali, costituzionali, economiche e sociali, nonché le altre condotte previste da convenzioni o da norme internazionali. Secondo la giurisprudenza (Cassazione. penale. n. 39504/2008) l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

- è commesso in più Stati;
- è commesso in uno Stato ma la sua preparazione è avvenuta in un altro territorio;
- è commesso in uno Stato ma da un gruppo criminale impegnato in attività illecite in altri Stati;
- è commesso in uno Stato ma gli effetti si manifestano in altre parti del mondo.

Tra i reati che rientrano in questa categoria e che possono dar luogo a responsabilità dell'ente, prevista dal decreto 231/01, si ricordano le associazioni per delinquere previste dagli artt. 416 e 416-bis codice penale, le associazioni finalizzate al contrabbando di tabacchi lavorati esteri o al traffico di stupefacenti, i reati in tema di immigrazioni clandestine, l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria e il favoreggiamento personale.

- **Delitti contro la persona:** l'articolo 25-quinquies fornisce un elenco di reati, previsti anche dal codice penale, con lo scopo di contrastare fortemente il fenomeno delle cosiddette "nuove schiavitù". Nello specifico l'articolo in questione ha come obiettivo principale quello di limitare fenomeni quali prostituzione, sfruttamento di minori, accattonaggio, tratta di persone, acquisto e alienazione di schiavi.

Relativamente all'esercizio dell'attività bancaria, il rischio che vengano commessi reati che rientrano in questo ambito si può considerare rilevante solo in riferimento al caso in cui un dipendente o un esponente della banca agisca di concerto con l'autore effettivo del reato. Nello specifico il reato può concretamente realizzarsi in caso di finanziamento da parte della banca a favore di soggetti o di organizzazioni che successivamente commettono reati sopra citati.

Nell'ambito dell'attività bancaria il rischio che possano essere commessi reati con finalità di terrorismo e di eversione dell'ordine pubblico, reati di criminalità organizzata, reati transnazionale e reati contro la persona, riguarda in maniera principale le attività di instaurazione di rapporti con la clientela, il trasferimento di fondi, l'operatività di sportello e nello specifico il processo di erogazione del credito. Si tratta di una serie di attività che si basano su un principio fondamentale: l'adeguata conoscenza della clientela che rappresenta un pilastro del decreto legislativo 231/2007 che ha tra i vari obiettivi anche la prevenzione dell'utilizzo del sistema bancario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Per le attività qui individuate il rischio che venga commesso anche il reato di riciclaggio, in ogni sua forma, è elevato. Inoltre per quanto riguarda l'induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria, si può individuare quale attività bancaria sensibile quella relativa alla gestione di contenziosi e di accordi transattivi.

Vi sono poi due fattispecie di reato che rientrano nell'area dei delitti contro la persona, quali l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare e l'intermediazione illecita e sfruttamento del lavoro, che possono essere commessi durante l'esercizio dell'attività di banca. In particolare il primo reato può essere commesso durante la gestione del processo di selezione e assunzione del personale mentre entrambi i reati possono essere commessi in fase di gestione di procedure di acquisto di beni e servizi.

Nella tabella che segue si riassume quanto finora descritto

	Delitti con finalità di terrorismo	Delitti di criminalità organizzata	Delitti transnazionali	Delitti contro la persona
Rapporti con la clientela	✓	✓	✓	✓
Trasferimento di fondi	✓	✓	✓	✓
Operazioni di sportello	✓	✓	✓	
Erogazione del credito	✓	✓	✓	✓
Riciclaggio	✓	✓	✓	✓
Gestione di contenziosi			✓	
Gestione di accordi transattivi			✓	
Acquisto di beni e servizi		✓	✓	✓
Gestione del personale			✓	✓

Tabella 3.9: *Processi associati ai reati previsti dagli articoli 24-ter, 25-quater e 25-quinquies*





# Conclusione

Lo scopo principale di questa tesi è stato quello di analizzare la correlazione esistente tra il decreto legislativo 231/01 e l'attività bancaria. Nello specifico per prima cosa ho suddiviso i reati contemplati dal decreto in questione in cinque grandi tipologie, successivamente ho individuato e analizzato quali possono essere le diverse attività bancarie potenzialmente sensibili e fortemente soggette alla commissione di illeciti previsti dal decreto 231/01 ed infine ho attribuito per ogni attività bancaria uno o più illeciti che effettivamente possono essere commessi da soggetti che operano o collaborano con la banca.

Nel primo capitolo viene illustrato il decreto 231/01 partendo dai soggetti a cui lo stesso si rivolge. Nel nostro ordinamento giuridico la responsabilità amministrativa degli enti non era disciplinata da nessun tipo di norma fino all'entrata in vigore della legge delega 300 del 2000. Questa legge ha stravolto completamente quanto previsto finora nel nostro ordinamento: infatti, l'ostacolo posto dall'articolo 27 della costituzione in base al quale la responsabilità penale è personale, risultava difficile da superare. Con l'entrata in vigore del decreto 231/01 tutto questo viene rivisto: il concetto di ente cambia e lo stesso non è più considerato come un mero nucleo giuridico ma se ne prende in considerazione l'intero operato evitando quindi di agire solo nei confronti delle persone fisiche responsabili e correlate allo stesso.

Pertanto i destinatari di questo decreto sono tutti gli enti forniti di personalità giuridica nonché le società e le associazioni anche prive di personalità giuridica che possono assumere il ruolo di indagati, imputati o condannati nel procedimento penale in conseguenza della commissione di un reato da parte di uno o più soggetti che operano nell'interesse o a vantaggio dell'ente stesso. Qualora si sviluppasse un procedimento penale le diverse tipologie di sanzioni eventualmente applicabili ai destinatari del decreto si possono suddividere in quattro macro categorie: le sanzioni di base, meramente pecuniarie, le sanzioni interdittive, la confisca e la pubblicazione di condanna. Infatti, in base alla tipologia di reato commesso, alla gravità e alle conseguenze che lo stesso produce possono essere applicate sanzioni differenti.

Infine, nell'ultima parte del capitolo sono stati elencati i reati presupposto disciplinati dal decreto studiato. I reati previsti sono numerosi, oltre 130, tuttavia qui sono stati presi in considerazione solamente quelli ritenuti fortemente connessi con l'esercizio dell'attività bancaria e sulla base di ciò, sono stati suddivisi e raggruppati in cinque tipologie differenti denominate "aree sensibili".

Nel secondo capitolo sono stati presi in esame gli strumenti che ogni ente deve utilizzare per poter mettere in pratica quanto stabilito dal decreto 231/01: vale a dire il *modello di organizzazione e l'organismo di vigilanza*.

In particolare gli istituti di credito devono comportarsi nel rispetto di quanto stabilito da decreto studiato. Infatti, relativamente all'attività bancaria, l'autorità di vigilanza preposta, ha posto in essere un sistema di controlli che influenza e coinvolge una serie di soggetti diversi: sindaci, società di revisione, ufficio controlli, internal auditing devono sempre più interagire fra di loro, con l'obiettivo di dotare la banca di procedure e strutture atte a garantire il principio della sana gestione che rappresenta il cuore di quanto normato dal decreto 231/01.

Per raggiungere questo obiettivo gli istituti di credito devono operare in modo tale da garantire la separatezza tra mansioni operative e mansioni di controllo, misurare ed identificare tutti i rischi che si possono assumere, adottare sistemi di informazione sicuri e in grado di riferire qualsiasi anomalia riscontrata nello svolgimento dell'attività bancaria nonché attuare controlli su ogni livello operativo. Per dar vita a questo complesso sistema di controlli, in grado di prevenire la commissione di illeciti e in grado di monitorare l'operatività bancaria in ogni settore e livello operativo, le banche adottano uno o più modelli di organizzazione e danno vita al cosiddetto organismo di vigilanza.

**Il modello** rappresenta un vademecum ovvero un insieme di norme, regole comportamentali, strutture organizzative e procedure operative, finalizzato a garantire lo svolgimento delle attività della società nel rispetto della legge, individuando ed eliminando in maniera tempestiva le situazioni di rischio. **L'organismo di vigilanza**, invece, è un organo che ha il compito di vigilare sul funzionamento e sull'osservanza del modello e di curarne il suo aggiornamento nonché di effettuare segnalazioni qualora venissero commessi degli illeciti.

Infine, il terzo capitolo dimostra che parte dei reati disciplinati dal decreto 231/01 sono fortemente connessi con lo svolgimento dell'attività bancaria. Attraverso il raggruppamento dei reati in aree sensibili è stato possibile fornire un utile strumento all'organismo di vigilanza volto a migliorare il sistema di controlli interni di un istituto di credito. Infatti, associare ad ogni attività bancaria uno o più reati che possono essere potenzialmente commessi da soggetti interni o che collaborano con la banca, consente all'organismo di vigilanza di avere a disposizione uno strumento in grado di facilitare la sua attività di

controllo. Nello specifico l'ODV potrà avere una visione dettagliata di quali sono le aree e le attività considerate più rischiose e quindi potrà porre in essere tutte le misure ritenute adeguate con l'obiettivo di ridurre il più possibile il rischio di commissione di illeciti.

Tra i vari compiti che spettano all'ODV vi è anche quello di trasformare il rischio inerente in rischio residuo e rendere il livello di quest'ultimo il più basso possibile. Per fare questo da un lato è bene conoscere in maniera approfondita le varie attività che vengono svolte all'interno della banca e dall'altro quali sono le possibili condotte negative che possono essere commesse all'interno di quelle attività. Avere uno strumento che ordina e collega i vari reati ai processi bancari renderà, senz'ombra di dubbio, il compito dell'ODV molto più semplice.

Pertanto, l'ODV avrà a disposizione un utile strumento che gli consentirà di rendere più efficace il sistema di controllo interno della banca e, al tempo stesso, di intervenire in maniera più efficiente e tempestiva in caso di commissione di illeciti.



# Bibliografia

- [1] Abriani N., 2012, *L'organismo di vigilanza previsto dal decreto legislativo 231/2001. Compiti e funzioni.*
- [2] Agrusti, *Le vicende modificative dell'ente*, Padova, 2009.
- [3] Allesandri A., *Diritto penale e attività economiche*, Bologna, 2010.
- [4] Amati E., *Abusi di mercato e sistema penale*, Giappichelli, 2012.
- [5] Amarelli G., *L'indebita inclusione delle imprese individuali nel novero dei soggetti attivi del d.lgs. 231/01*, Diritto penale e contemporaneo, 2011.
- [6] Arena M., *La responsabilità da reato degli enti collettivi*, Milano, 2007.
- [7] Baldi F., *Ius resistentiae: la linea di demarcazione tra i doveri di diligenza e obbedienza contrattuale*, in *Il giuslavorista.it*, fasc., 9 settembre 2016.
- [8] Balducci P., *L'ente imputato. Profili di efficienza e di garanzia nel processo de societate*, Torino, 2013.
- [9] Bartolomucci S., *Corporate governance e responsabilità delle persone giuridiche*, Milano, 2004.
- [10] Bassi A., *Enti e responsabilità da reato. Accertamento, sanzioni e misure cautelari*, Giuffrè, 2006.
- [11] Buonocore V., *La responsabilità da inadeguatezza organizzativa*, Torino, 2015.
- [12] Bussoletti, 2003, *Procedimento sanzionatorio e vicende modificative dell'ente nella legge sulla responsabilità amministrativa degli enti collettivi.*
- [13] Costi R., *L'ordinamento bancario*, Bologna, 2012.
- [14] D'arcangelo F., 2011, *I canoni di accertamento dell'idoneità nel MOG.*
- [15] Di Pinto, *La responsabilità amministrativa da reato degli enti*, Torino, 2003.

- [16] Enria A., *Il sistema bancario italiano nella prospettiva della vigilanza europea*, Roma, 2015.
- [17] Fiorella A., *Principi generali e criteri d'imputazione all'ente della responsabilità amministrativa*, Torino, 2003.
- [18] Frattini M., *Il testo unico della finanza*, Milano, 2012.
- [19] Galanti E., *Diritto delle banche e degli intermediari finanziari*, Padova, 2008.
- [20] Garuti G., *Contestazione dell'illecito amministrativo e udienza preliminare*, in rivista 231.
- [21] Gazzoni F., *Manuale di diritto privato*, Napoli, 2013.
- [22] Gennai, *La responsabilità degli enti*, Milano, 2001.
- [23] Gennaro V., 2013, *La documentazione delle attività di pianificazione e di esecuzione delle verifiche da parte dell'organismo di vigilanza*.
- [24] Giovagnoli R., *Le sanzioni amministrative*, Milano, 2009.
- [25] Irrera M., *Assetti adeguati e modelli organizzativi nella corporate governance delle società di capitali*, Bologna, 2016.
- [26] Itinera , *Guide giuridiche ipsoa*, 2017, *Responsabilità amministrativa degli enti* a cura di Francesco Sbisà.
- [27] Lattanzi G., *Reati e responsabilità degli enti: guida al decreto legislativo 8 giugno 2001, n. 231*, Milano, 2005.
- [28] Lecis U., 2006, *L'organismo di vigilanza e l'aggiornamento del modello organizzativo*.
- [29] Ledda F., 2015, *Caso ThyssenKrupp. Cassazione settembre 2014. Composizione dell'ODV e idoneità dei modelli organizzativi. Spunti di riflessione*.
- [30] Levis M., *La responsabilità amministrativa delle società e degli enti. Commentario*, Bologna, 2014.
- [31] Magris P., 2016, *Modelli di organizzazione ed esenzione di responsabilità: aspetti pratici ed operativi*.
- [32] Montalenti P., *Società per azioni, corporate governance e mercati finanziari*, Milano 2011.
- [33] Mucciarelli F., *Le sanzioni interdittive temporanee nel d.lgs 231/01*, Milano, 2006.

- [34] Paolozzi G., *Vademecum per gli enti sotto processo. Addebiti amministrativi da reato.*, Torino, 2007.
- [35] Pecorella C., *Principi generali e criteri di attribuzione della responsabilità*, Milano 2002.
- [36] Piergallini C., *L'apparato sanzionatorio*, Milano 2010.
- [37] Previtali P., 2007, *Il reato di frode informatica ai sensi del d.lgs 231/2001: standard di controllo e procedure per la compliance del modello organizzativo.*
- [38] Rezzani A., *Big data, Architetture, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Rimini, 2013.
- [39] Roncaglia P., 2010, *La responsabilità amministrativa degli enti con riferimento ai delitti contro l'industria e il commercio e in materia di contraffazione.*
- [40] Santi, *Responsabilità da reato degli enti e modelli di esonero*, Milano, 2016.
- [41] Spagnolo G., *La responsabilità da reato*, Milano, 2007.
- [42] Spangher G., *Le impugnazioni*, Padova, 2002.
- [43] Spataro A., *Sicurezza e politiche antiterrorismo in Europa*, in G. Cocco, I diversi volti della sicurezza, Milano 2012.
- [44] Tirelli M., *I procedimenti speciali*, Padova, 2002.
- [45] Varraso G., *Le misure cautelari*, Padova, 2002.
- [46] Vizzardi M., *La responsabilità degli enti. Commenti articolo per articolo al D. Legisl. 8 giugno 2001, n. 231*, Milano, 2008.

## Siti web utilizzati:

- [47] Abi - Decreto legislativo 231/01  
*<http://www.abi.it>*
- [48] Ambiente diritto - Decreto legislativo 231/01  
*<http://www.ambientediritto.it>*
- [49] Anticorruzione - Decreto legislativo 231/01  
*<http://www.anticorruzione.it>*
- [50] Banca d'Italia - Decreto legislativo 231/01  
*<http://www.bancaitalia.it>*
- [51] Bcc Roma - Decreto legislativo 231/01  
*<http://www.bccroma.it>*
- [52] Borsa Italiana - Decreto legislativo 231/01  
*<http://www.borsaitaliana.it>*
- [53] Camera - Decreto legislativo 231/01  
*<http://www.camera.it>*
- [54] Cdp - Decreto legislativo 231/01  
*<http://www.cdp.it>*
- [55] Confindustria - Decreto legislativo 231/01  
*<http://www.confindustria.it>*
- [56] CONSOB - Commissione Nazionale per le Società e la Borsa - Decreto legislativo 231/01  
*<http://www.consob.it>*
- [57] Cpl concordia group - Decreto legislativo 231/01  
*<http://www.cplconcordiagroup.com>*
- [58] Dlgs 231- Decreto legislativo 231/01  
*<http://www.dlgs231.eu>*
- [59] Diritto - Decreto legislativo 231/01  
*<http://www.diritto.it>*
- [60] Diritto bancario - Decreto legislativo 231/01  
*<http://www.dirittobancario.it>*



- 
- [61] Enrico Berardi - Decreto legislativo 231/01  
*<http://www.enricoberardi.it>*
- [62] Gazzetta Ufficiale della Repubblica Italiana - Decreto legislativo 231/01  
*<http://www.gazzettaufficiale.it>*
- [63] Generali - Decreto legislativo 231/01  
*<http://www.generali.it>*
- [64] Gdf - Decreto legislativo 231/01  
*<http://www.gdf.gov.it>*
- [65] Federcasa- Decreto legislativo 231/01  
*<http://www.federcasa.it>*
- [66] Ferrara Italia - Decreto legislativo 231/01  
*<http://www.ferraraitalia.it>*
- [67] Il giornale dell pmi - Decreto legislativo 231/01  
*<http://www.giornaledellepmi.it>*
- [68] Il sole 24 ore - Decreto legislativo 231/01  
*<http://www.ilsole24ore.com>*
- [69] Informa impresa - Decreto legislativo 231/01  
*<http://www.informaimpresa.it>*
- [70] Intesa san paolo - Decreto legislativo 231/01  
*<http://www.intesasanpaolo.com>*
- [71] Lente Pubblica - Decreto legislativo 231/01  
*<http://www.lenteubblica.it>*
- [72] Milano finanza- Decreto legislativo 231/01  
*<http://www.milanofinanza.it>*
- [73] Portale 231 - Decreto legislativo 231/01  
*<http://www.portale231.com>*
- [74] Puntosicuro - Decreto legislativo 231/01  
*<http://www.puntosicuro.it>*
- [75] Riskcompliance - Decreto legislativo 231/01  
*<http://www.riskcompliance.it>*
- [76] Rivista 231 - Decreto legislativo 231/01  
*<http://www.rivista231.it>*

- [77] Slideplayer - Decreto legislativo 231/01  
*<http://www.slideplayer.it>*
- [78] Slideshare - Decreto legislativo 231/01  
*<http://www.slideshare.net>*
- [79] Studio cataldi - Decreto legislativo 231/01  
*<http://www.studiocataldi.it>*
- [80] Studio tidona - Decreto legislativo 231/01  
*<http://www.studiotidona.com>*
- [81] Uif - Decreto legislativo 231/01  
*<http://www.uif.bancaditalia.it>*
- [82] Unicredit - Decreto legislativo 231/01  
*<http://www.unicredit.it>*
- [83] Wikipedia- Decreto legislativo 231/01  
*<http://www.wikipedia.org>*

# Ringraziamenti

Giunto alla fine del mio percorso universitario, vorrei ringraziare il professore Simone Mazzonetto, relatore di questa tesi di laurea, per avermi dato l'opportunità di approfondire i miei studi con l'assegnazione di questo argomento e per avermi dimostrato grande disponibilità durante lo svolgimento di questo lavoro.

Ringrazio particolarmente il mio amico Giovanni che mi ha sempre incoraggiato e con il quale ho condiviso l'intero percorso di studi. Incredibile ma vero, ce l'abbiamo fatta!

Un grande ringraziamento va fatto alla mia famiglia che instancabilmente mi ha sempre sostenuto e aiutato, sia moralmente che economicamente, e mi ha permesso di arrivare fin qui, contribuendo alla mia formazione personale.

Infine un ringraziamento speciale va a mia moglie Chiara, compagna di vita che mi ha sempre appoggiato e mi è sempre stata vicina in ogni traguardo della mia vita: "*Grazie di tutto*".