BANCA
SISTEMA

# BANCA SISTEMA S.p.A.

## MODELLO DI ORGANIZZAZIONE E GESTIONE

**ai sensi dell'art. 6, comma 1, lett. a) del**
**D.Lgs. 8 giugno 2001, n.231 e successive modifiche**

**Versione del 17 marzo 2023**

# INDICE

# PARTE GENERALE

# Quadro normativo

## 1.1 *Introduzione*

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito "D.Lgs. 231/2001" o "Decreto"), recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e di altre strutture associative, anche prive di personalità giuridica (di seguito, "Ente" o "Enti"), a norma dell'art. 11 della Legge 29 settembre 2000, n. 300", ha introdotto per la prima volta in Italia una responsabilità amministrativa da reato a carico delle persone giuridiche (o "Enti"), che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

Si tratta di una nuova e più estesa forma di responsabilità, che colpisce l'Ente per alcuni reati commessi – o anche solo tentati - nel suo interesse o vantaggio, da soggetti ad esso funzionalmente legati (soggetti in posizione apicale e soggetti sottoposti alla direzione e vigilanza di costoro).

Il Decreto prevede che gli Enti possano essere ritenuti responsabili, e conseguentemente sanzionati, in relazione esclusiva al compimento di taluni reati (c.d. "reati presupposto") indicati tassativamente dalla legge, per quanto l'elencazione sia suscettibile di modifiche e integrazioni da parte del legislatore.

Il Decreto ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia aveva già da qualche tempo aderito[1].

Il primo criterio fondamentale d'imputazione consiste quindi nel fatto che il reato sia stato commesso nell'interesse o a vantaggio dell'Ente: ciò significa che la responsabilità dell'Ente sorge qualora il fatto sia stato commesso per favorire l'Ente, senza che sia necessario il conseguimento effettivo e concreto dell'obiettivo.

L'Ente non è responsabile se l'illecito è stato commesso da uno dei soggetti sopra indicati nell'interesse esclusivo proprio o di terzi.

[1] Quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione del 26 maggio 1997, anch'essa firmata a Bruxelles, sulla lotta alla corruzione e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il secondo criterio fondamentale d'imputazione è costituito dal tipo di soggetti autori del reato, dai quali può derivare una responsabilità amministrativa a carico dell'Ente.

Tali soggetti, infatti, possono essere:

- soggetti in posizione apicale (quali, ad esempio, il legale rappresentante, l'amministratore, il direttore generale o le persone che esercitano, anche di fatto, la gestione o il controllo dell'Ente);
- soggetti subalterni, tipicamente lavoratori dipendenti, ma anche soggetti esterni all'Ente, ai quali sia stato affidato un incarico da svolgere sotto la direzione e la sorveglianza dei soggetti apicali.

Se più soggetti concorrono alla commissione del reato (art. 110 c.p.) non è necessario che il soggetto "qualificato" ponga in essere direttamente il fatto, ma è sufficiente che fornisca un consapevole contributo causale alla realizzazione del reato stesso.

La responsabilità prevista dal suddetto Decreto si configura anche sui reati commessi all'estero dall'Ente, alle seguenti condizioni:

- il reato è stato commesso da un soggetto funzionalmente legato all'Ente (apicale o subordinato, come sopra illustrato);
- l'Ente ha la propria sede principale in Italia;
- l'Ente può rispondere solo nei casi e alle condizioni previste dagli articoli 7, 8, 9, 10 c.p. e qualora la legge preveda che la persona fisica colpevole sia punita a richiesta del Ministro della Giustizia, si procede contro l'Ente solo se la richiesta è formulata anche nei confronti dell'Ente stesso;
- l'Ente risponde solo se nei suoi confronti non procede lo Stato del luogo in cui è stato commesso il reato.

La responsabilità amministrativa dell'Ente sorge anche nel caso in cui uno degli illeciti previsti dal Decreto sia commesso anche solo nella forma di tentativo (art. 56 c.p.).

### 1.2 *I reati presupposto*

I reati destinati a comportare il regime di responsabilità amministrativa a carico degli Enti, per i quali si applica la disciplina in esame, sono stati progressivamente ampliati rispetto alla promulgazione dello stesso e, ad oggi, comprendono quelli di seguito elencati:

1. **reati commessi nei rapporti con la Pubblica Amministrazione e contro il Patrimonio** (artt. 24 e 25);
2. **delitti informatici e trattamento illecito di dati** (art. 24-*bis*);
3. **delitti di criminalità organizzata** (art. 24-*ter*);
4. **peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso di ufficio (art. 25);**
5. **falsità in monete, carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (art. 25-*bis*);
6. **delitti contro l'industria e il commercio** (art. 25-*bis*.1);
7. **reati societari** (art. 25-*ter*);
8. **reati con finalità di terrorismo o di eversione dell'ordine democratico** (art. 25-*quater*);
9. **pratiche di mutilazione degli organi genitali femminili** (art. 25-*quater*.1);
10. **delitti contro la personalità individuale** (art. 25-*quinquies*);
11. **abusi di mercato** (art. 25-*sexies*);
12. **reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** (art. 25-*septies*);
13. **reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita** (art. 25-*octies*);
14. **delitti in materia di violazione del diritto d'autore** (art. 25-*novies*);
15. **delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 25-*decies*);
16. **reati ambientali** (art. 25-*undecies*);
17. **impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25-*duodecies*);

18. **razzismo e xenofobia** (art. 25-*terdecies*)**;**
19. **frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** (art. 25-*quaterdecies)*;
20. **reati tributari** (art. 25-*quinquiesdecies)*;
21. **contrabbando** (art. 25-*sexiesdecies)*.
22. **disposizioni in materia di reati contro il patrimonio culturale** (art. 25-*septiesdecies*);
23. **riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** (art. 25-*duodevicies*);
24. **delitti tentati** (art. 26).

I reati e gli illeciti amministrativi sopra richiamati possono comportare la responsabilità amministrativa dell'Ente avente sede principale nel territorio italiano anche se commessi all'estero.

Come meglio specificato nel prosieguo, nella Parte Speciale del presente documento saranno trattati solo i reati presupposto astrattamente ipotizzabili in capo alla Banca.

### 1.3 *Le sanzioni applicabili*

Le sanzioni previste a carico dell'Ente previste dal Decreto n. 231/2001, in conseguenza della commissione o tentata commissione dei reati presupposto, sono:

- Sanzione pecuniaria: applicabile a tutti gli illeciti, determinata dal Giudice penale attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille, ciascuna di valore tra un minimo di Euro 258,23 ed un massimo di Euro 1.549,37[2]. Il Giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di

[2] Perciò la sanzione oscilla tra un minimo di Euro 25.823 ed un massimo di Euro 1.549.370, eccetto per i reati societari le cui sanzioni pecuniarie sono raddoppiate in base a quanto previsto dalla Legge sul Risparmio 262/2005, art. 39, comma 5.

ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione.

La sanzione pecuniaria è 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 le conseguenze dannose o pericolose del reato, ovvero si è comunque efficacemente adoperato in tal senso;
- ✓è stato adottato o reso operativo un Modello organizzativo idoneo a prevenire reati della specie di quello verificatesi.

Inoltre, è prevista la riduzione della metà della sanzione pecuniaria se:

- ✓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.

Il principio fondamentale che guida l'intera materia della responsabilità dell'Ente stabilisce che soltanto quest'ultimo risponde, con il suo patrimonio o il fondo comune, dell'obbligazione per il pagamento della sanzione pecuniaria inflitta. La norma, dunque, esclude una responsabilità patrimoniale diretta dei soci o degli associati, indipendentemente dalla natura giuridica dell'Ente collettivo.

- Sanzioni interdittive: sono irrogate, congiuntamente a quella pecuniaria, solo se espressamente previste per quella fattispecie di reato, e soltanto quando ricorre almeno una di queste due condizioni:
  1. la società ha già commesso in precedenza un illecito da reato (reiterazione degli illeciti);
  2. la società ha tratto dal reato un profitto di rilevante entità.

Si traducono in:

a) interdizione dall'esercizio dell'attività;

b) sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrattare con la Pubblica Amministrazione;
d) esclusione da agevolazioni, finanziamenti, contributi, sussidi ed eventuale revoca di quelli già concessi;
e) divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l'Ente, prima della dichiarazione di apertura del dibattimento di primo grado, abbia:

a) risarcito il danno o lo abbia riparato;
b) eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
c) messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del reato;
d) eliminato le carenze organizzative che hanno determinato il reato, adottando modelli organizzativi idonei a prevenire la commissione di nuovi reati.

- Confisca: consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato, anche in forma per equivalente (confiscando cioè una somma di denaro, beni o altre utilità di valore corrispondenti al prezzo o profitto del reato); la confisca è sempre disposta con la sentenza di condanna.

- Pubblicazione della sentenza: può essere disposta dal Giudice quando, nei confronti dell'Ente, viene applicata una sanzione interdittiva. È effettuata mediante affissione nel comune ove l'Ente ha la sede principale, nonché mediante la pubblicazione sul sito internet del Ministero della Giustizia.

- Misure cautelari: il Pubblico Ministero può chiedere l'applicazione delle sanzioni interdittive anche in via cautelare, qualora:

a. sussistano gravi indizi della responsabilità dell'Ente;
b. vi siano fondati e specifici elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti dello stesso tipo di quello già commesso.

### 1.4 *Esenzione dalla responsabilità amministrativa*

Il Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede una forma specifica di esonero da detta responsabilità qualora l'Ente dimostri di avere adottato tutte le misure organizzative opportune e necessarie al fine di prevenire la commissione di reati da parte di soggetti che operino per suo conto. La presenza di un'adeguata organizzazione è, dunque, misura e segno della diligenza dell'Ente nello svolgere le proprie attività, con particolare riferimento a quelle in cui si manifesta il rischio di commissione dei reati previsti dal Decreto.
Al Consiglio di Amministrazione compete l'adozione e l'efficace attuazione del Modello di Organizzazione, Gestione e controllo (o "MOG"), ai sensi dell'art. 6, comma 1, lett. a), nonché la nomina dei membri dell'Organismo di Vigilanza, ai sensi della successiva lett. b).
Il Decreto indica quali sono le componenti di un apparato organizzativo efficace ed effettivo la cui corretta predisposizione porta ad escludere la sua responsabilità. In particolare, l'Ente va esente da pena se prova:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei (di seguito il "Modello") a prevenire i reati della specie di quello verificatosi;
- di aver affidato la vigilanza sul funzionamento e l'osservanza del Modello, nonché il compito di curarne l'aggiornamento ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo ("Organismo di Vigilanza");
- che le persone che hanno commesso il reato l'abbiano fatto eludendo fraudolentemente il Modello;

- che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Inoltre, l'art. 6, al secondo comma, indica anche il contenuto del Modello, che dovrà presentare le seguenti caratteristiche:

a) individuare le attività nel cui ambito esiste la possibilità che siano commessi i reati di cui al Decreto;
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 tali reati;
d) prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (denominati anche linee guida) redatti da associazioni rappresentative di categoria.
Le linee guida vengono comunicate al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sulla idoneità a prevenire i reati dei Modelli elaborati in conformità alle linee guida delle associazioni di categoria.

# 2 Adozione del Modello

## 2.1 *Obiettivi perseguiti con l'adozione del Modello*

Banca Sistema S.p.A. (di seguito **"Banca"**), con l'adozione, l'efficace attuazione ed il costante aggiornamento del modello organizzativo *ex* D.Lgs. n. 231/2001, si impegna a operare in condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali.

Banca Sistema è un istituto bancario indipendente, costituita nel giugno 2011 dall'integrazione tra le attività di Banca Sintesi SpA e quelle del gruppo S.F. Trust Ltd., specializzato nell'acquisto e nella gestione di crediti commerciali vantati dalle imprese verso la Pubblica Amministrazione italiana. Da luglio 2015 la Banca è quotata sul Mercato Telematico Azionario (MTA) – Segmento STAR organizzato e gestito da Borsa Italiana SpA.

Dall'inizio della sua attività la Banca ha ampliato le proprie attività e i servizi offerti, sia alla clientela business sia a quella *retail*, affiancando ai prodotti di factoring e recupero crediti, anche la gamma completa dei servizi bancari, aprendo nuove filiali e perfezionando sempre di più la personalizzazione alla propria Clientela, che spazia da grandi multinazionali a piccole e medie imprese, oltre a professionisti e risparmiatori privati.

Uno degli obiettivi primari perseguiti da Banca Sistema non è solo quello di soddisfare la domanda finanziaria delle imprese, facendo da *trait d'union* tra settore pubblico e privato e favorendone l'efficienza e un corretto bilanciamento della domanda finanziaria, ma di garantire alle aziende e alle persone un accesso al mondo bancario evoluto, semplificato, disponibile e attento alle esigenze di un Paese e di imprenditori che crescono.

La Banca è in grado di offrire un'ampia gamma di servizi di factoring pro-soluto, pro solvendo (anche tra privati), reverse/maturity factoring, rimborso crediti IVA, certificazione dei crediti vantati nei confronti della PA. La Banca è inoltre attiva nel comparto dell'acquisto e della gestione di crediti finanziari e commerciali in sofferenza, oltre alla gestione e al recupero crediti tra privati.

Un'altra linea di business della Banca è la concessione del credito derivante da finanziamenti contro cessione del quinto dello stipendio/pensione (CQS e CQP), sia in forma diretta con il prodotto denominato "QuintoPuoi" promosso mediante una rete commerciale di agenti monomandatari diffusa su tutto il territorio nazionale, sia mediante accordi di cessione pro-soluto di crediti con società cedenti.

Per quanto riguarda i prodotti "bancari" dedicati alla clientela retail sottoscrivibili on-line o presso le filiali, ci sono i conti correnti e i conti deposito vincolati, con una durata fino a 10 anni, oltre ai servizi di deposito titoli.

Banca Sistema – sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri dipendenti – ha ritenuto conforme alle proprie politiche aziendali procedere all'attuazione del Modello previsto dal Decreto Legislativo n. 231/2001.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello – al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio – possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto della Banca affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

Il suddetto Modello è stato predisposto tenendo presenti, oltre alle prescrizioni del Decreto, le linee guida elaborate in materia da associazioni di categoria (es. Confindustria e Assiosim).

Sempre in attuazione di quanto previsto dal Decreto, il Consiglio di Amministrazione, nell'adottare il suddetto Modello, ha affidato ad un Organismo di Vigilanza (di seguito anche **"OdV"**) l'incarico di assumere le funzioni di organo di controllo con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

## 2.2 *Modello di corporate governance*

Il modello di *corporate governance* della Banca è strutturato in modo tale da assicurare e garantire la massima efficienza ed efficacia operativa, mediante l'adozione del sistema di amministrazione e controllo c.d. "tradizionale". Secondo tale modello, la gestione spetta esclusivamente al Consiglio di Amministrazione, la funzione di vigilanza al Collegio Sindacale e quella di revisione legale ad una società di revisione iscritta nell'albo speciale tenuto da Consob.

L'Assemblea degli Azionisti è l'organo che rappresenta l'universalità degli azionisti e a cui compete deliberare (i) in sede ordinaria, in merito all'approvazione del bilancio annuale, alla nomina e alla revoca dei componenti il Consiglio di

Amministrazione, alla nomina dei componenti il Collegio Sindacale e del loro Presidente, alla determinazione dei compensi di Amministratori e Sindaci, al conferimento dell'incarico di revisione legale, alla responsabilità degli Amministratori e dei Sindaci ed alle ulteriori materie attribuite alla sua competenza; (ii) in sede straordinaria, in merito alle modificazioni dello Statuto ed alle operazioni di carattere straordinario quali gli aumenti di capitale, le fusioni e le scissioni, salvo per quanto statutariamente delegato al Consiglio ai sensi di legge.

Il Consiglio di Amministrazione è l'organo investito dei più ampi poteri di ordinaria e straordinaria amministrazione e svolge tutti i compiti previsti dalla legge e dal Codice di Autodisciplina.

Il Collegio Sindacale è l'organo deputato a vigilare sull'osservanza della legge e dello Statuto, sul rispetto dei principi di corretta amministrazione sull'adeguatezza del sistema di controllo interno nonché dell'assetto organizzativo, amministrativo, contabile e sulla sua affidabilità. È, inoltre, chiamato a vigilare sulla concreta attuazione delle regole di governo societario adottate dalla Società e a vigilare sull'indipendenza della società di revisione. A seguito dell'entrata in vigore del Testo Unico della Revisione Legale, il Collegio Sindacale svolge ulteriori e/o rafforzati compiti di vigilanza in qualità di "Comitato per il controllo interno e la revisione contabile".

Il Collegio si compone di tre membri effettivi e due supplenti che durano in carica per tre esercizi; i Sindaci non possono assumere cariche in organi diversi da quelli di controllo presso altre società appartenenti al Gruppo o al conglomerato finanziario, nonché presso società nelle quali la Banca detenga, anche indirettamente, una partecipazione strategica.

Inoltre, in conformità alle raccomandazioni del Codice di Autodisciplina delle società quotate cui la Banca ha aderito e ai principi di corporate governance osservati a livello internazionale e suggeriti in ambito comunitario, il Consiglio ha costituito al suo interno i seguenti Comitati:

- Comitati endoconsiliari, tra i quali sono ricompresi i seguenti:
  - Comitato Esecutivo (se costituito).

- Comitato per il Controllo Interno e Gestione dei Rischi.
- Comitato per le Nomine.
- Comitato per la Remunerazione.
- Comitato Etico.

- Comitati esoconsiliari:
  - Comitato Gruppo.
  - Comitato Gestione Rischi.
  - Comitato Tecnico Organizzativo.
  - Comitato Crisi.

La revisione legale dei conti è svolta da una società di revisione iscritta nell'albo speciale tenuto dalla Consob. La nomina della società spetta all'Assemblea, su proposta motivata del Collegio Sindacale, ai sensi dell'art. 2409 *bis* e seguenti c.c. e del D.Lgs. 27 gennaio 2010, n. 39.

### 2.3 *Il sistema di deleghe e procure*

La politica della Banca prevede che solo i soggetti muniti di formali e specifici poteri scritti possano assumere impegni verso terzi in nome e per conto della Banca stessa. Pertanto, quest'ultima ha adottato un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate implicanti effettive necessità di rappresentanza e con la previsione, quando opportuno, di una puntuale indicazione di soglie quantitative di spesa stabilite da provvedimenti interni all'azienda.

Per deleghe societarie si intendono normalmente due concetti distinti:

1. Deleghe agli Amministratori

Il Consiglio di Amministrazione può distribuire i propri poteri ad uno o a più amministratori (che, in seguito al conferimento di deleghe, diventano Amministratori Delegati o con delega). Le deleghe sono approvate dal Consiglio di Amministrazione e il relativo verbale viene depositato in Camera di Commercio per rendere noti ai terzi i contenuti delle deleghe.

2. Deleghe funzionali interne alla Banca

Le deleghe funzionali costituiscono articolazioni di poteri interni alla Banca, nate soprattutto nella dottrina aziendalistica e riprese dalla giurisprudenza soprattutto penalistica (cfr. D.Lgs. n. 81/2008 e norme sull'ambiente). Con le deleghe funzionali, i poteri organizzativi interni vengono distribuiti dal Consiglio di Amministrazione e/o dall'Amministratore/i Delegato/i all'alta dirigenza e in tutta la struttura aziendale. Le deleghe funzionali non comportano alcuna "spendita del nome della Banca".

3. Procure

Quando il compimento di un atto comporta una "spendita del nome" della Banca (ossia l'atto si riverbera sull'esterno), il potere relativo, se non è in capo ad un amministratore, deve essere conferito con procura. La procura è dunque lo strumento in base al quale i poteri di compiere atti verso l'esterno sono conferiti a dipendenti o a terzi, non amministratori. Perché i poteri conferiti siano opponibili ai terzi, la procura deve essere "notarile" e va depositata presso la Camera di Commercio, in mancanza, la Banca non può opporre al terzo alcuna limitazione dei poteri: il procuratore può in tal caso impegnare la Banca senza limiti.

Tutto ciò premesso, in termini generali, il sistema delle deleghe funzionali e delle procure adottato dalla Banca assicura che:

- l'esercizio dei poteri nell'ambito di un processo decisionale sia svolto da posizioni di responsabilità congruenti con l'importanza e/o la criticità di determinate operazioni economiche;
- al processo decisionale partecipino i soggetti che svolgono le attività oggetto dell'esercizio dei poteri;
- i poteri e le responsabilità siano chiaramente definiti, coerenti tra loro e conosciuti all'interno della organizzazione societaria;
- la Banca sia validamente impegnata nei confronti di terzi (es. clienti, fornitori, banche, amministrazioni pubbliche, ecc.) da un numero determinato e limitato di soggetti muniti di deleghe formalizzate e opportunamente comunicate verso l'esterno, ove siano specificamente indicati i relativi poteri;

- sia costantemente aggiornata la mappatura dei soggetti (anche dei non dipendenti) cui sia stato conferito il potere di impegnare la Banca verso i terzi.

Le unità aziendali interessate, con il supporto dell'Organismo di Vigilanza, verificano periodicamente il sistema delle deleghe e procure in vigore, anche attraverso l'esame della documentazione attestante l'attività concretamente effettuata dai soggetti che operano per conto della Banca, suggerendo le necessarie modifiche nel caso in cui le funzioni di gestione e/o qualifica non corrispondano ai poteri di rappresentanza conferiti.

# 3 Funzione del Modello

## 3.1 *Il Modello di Banca Sistema*

Lo scopo principale del Modello è la costruzione di un sistema strutturato e organico di procedure nonché di attività di controllo, volto a prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto.

I principi e le disposizioni contenute del presente Modello devono essere rispettati dai componenti del Consiglio di Amministrazione, del Collegio Sindacale, dai dipendenti della Banca, dai consulenti, dai collaboratori e in generale da tutti coloro che operano in Italia e all'estero per conto o a favore della Banca nelle aree a rischio reato "231", come di volta in volta individuati.

In particolare, mediante l'individuazione delle aree di attività a rischio e la conseguente modalità di svolgimento delle predette attività, il Modello si propone come finalità quelle di:

- determinare, in tutti coloro che operano in nome e per conto della Banca nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni da parte dell'azienda così come previsto al Capitolo 6;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da Banca Sistema in quanto contrarie oltre che alle disposizioni

di legge, anche ai principi etico-sociali cui la Banca intende attenersi nell'espletamento della propria attività aziendale;

- consentire alla Banca, grazie ad un'azione di monitoraggio sulle "aree di attività a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Punti cardine del Modello sono, oltre ai principi già indicati:

- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la "mappa delle aree di attività a rischio" della Banca, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- l'attribuzione all'OdV di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- la verifica e documentazione delle operazioni a rischio;
- il rispetto del principio della separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico.

### 3.2 *Attività preparatoria del Modello*

Il Modello di Banca Sistema è stato predisposto seguendo la metodologia suggerita dalle linee guida delle principali associazioni di categoria, ovvero attraverso la suddivisione dell'attività in tre fasi:

Fase 1 - Analisi dei rischi

Analisi delle aree a rischio che possono causare eventi pregiudizievoli ai sensi del Decreto.

In particolare, l'analisi dei rischi viene condotta attraverso il seguente approccio metodologico:

- analisi della struttura societaria ed organizzativa della Banca, attraverso lo studio della principale documentazione sociale, finalizzata a pervenire ad una conoscenza generale della Banca;
- comprensione del modello di business della Banca;

- analisi storica relativa ad eventuali casi già emersi nel passato con riferimento a precedenti penali, civili od amministrativi nei confronti della Banca o suoi dipendenti che abbiano punti di contatto con la normativa rilevante;
- analisi dei rischi specifici che possono causare eventi pregiudizievoli per gli obiettivi indicati nel Decreto;
- analisi e rilevazione dei sistemi normativo–regolamentari e dei sistemi di controllo adottati dalla Banca nelle aree considerate potenzialmente a rischio.

Lo svolgimento della fase in oggetto si è concretizzata anche attraverso l'attuazione di interviste ai "soggetti chiave" del sistema decisionale e di controllo, ed è stata integrata alla luce della quotazione della Banca sul mercato azionario.

Fase 2 – La *gap analysis*

Con tale attività sono stati confrontati i sistemi di controllo esistenti nella Banca a presidio delle aree a rischio individuate nella Fase 1 con i requisiti organizzativi richiesti dal Decreto al fine di individuare le modifiche necessarie per la preparazione del modello volto a prevenire i "reati presupposto".

Fase 3 – Definizione della Parte Generale del Modello

La Parte Generale contiene una panoramica sui contenuti normativi del Decreto e sulle funzioni del Modello, l'individuazione dell'Organismo di Vigilanza della Banca (delle sue caratteristiche, delle funzioni, dei poteri e del sistema di *reporting*) e dell'impianto sanzionatorio predisposto dalla Banca per la violazione delle regole di condotta previste dallo stesso Modello.

Il Consiglio di Amministrazione è responsabile dell'aggiornamento del modello e del suo adeguamento in relazione alle variazioni degli assetti organizzativi, dei processi operativi, alle risultanze dei controlli, e alle modifiche/integrazioni legislative introdotte dal legislatore per le fattispecie previste.

Fase 4 – Predisposizione delle Parti Speciali del Modello

Questa parte è finalizzata a definire i principi procedurali generali e specifici diretti a prevenire la commissione dei reati presupposto.

Le Parti Speciali di cui al presente Modello riguardano:

- i reati contro la Pubblica Amministrazione (artt. 24-25);

- i reati societari (art. 25-*ter*);
- i reati di abuso di mercato (art. 25-*sexies*);
- i reati di riciclaggio e terrorismo (art. 25-*octies*);
- i reati informatici e trattamento illecito dei dati (art. 24-*bis*).
- i reati di omicidio colposo e lesioni gravi o gravissime commessi in violazione delle norme in materia di igiene e sicurezza negli ambienti di lavoro (art. 25-*septies*).

Si sottolinea inoltre che l'introduzione di alcuni reati ha carattere meramente prudenziale in quanto, pur non sussistendo elementi specifici da cui dedurre l'esistenza di attuali rischi, si tratta di reati sui quali la Banca intende comunque mantenere un alto livello di attenzione.

### 3.3 *Adozione, diffusione e aggiornamento del Modello*

È stato demandato al Consiglio di Amministrazione, sulla base anche di criteri e direttive emanati in tal senso, di provvedere mediante apposita delibera all'adozione di un proprio Modello, in funzione dei profili di rischio configurabili nelle attività svolte dalla Banca.

Nell'adottare il Modello, il Consiglio di Amministrazione ha proceduto contestualmente anche alla nomina dell'Organismo di Vigilanza, incaricato di svolgere i compiti di controllo sullo svolgimento delle suddette attività e sull'applicazione del Modello medesimo.

È rimesso alla Banca di predisporre, adottare e aggiornare il Modello in relazione alle esigenze di adeguamento che per esso si verranno nel tempo a determinare. In particolare, è demandato al Consiglio di Amministrazione, anche su proposta dell'OdV, di integrare il presente Modello, ove necessario, mediante apposita delibera, aggiornando i reati presupposto così come previsti dalle normative di tempo in tempo vigenti.

È rimessa alla responsabilità della Banca l'applicazione del Modello in relazione all'attività dalla stessa in concreto posta in essere. A tal fine è attribuito all'OdV il compito primario di esercitare i controlli sull'attuazione del Modello stesso secondo le procedure in esso descritte.

# 4 L'Organismo di Vigilanza

## 4.1 *Requisiti*

In attuazione di quanto previsto dal Decreto – il quale pone come condizione, per la concessione dell'esimente dalla responsabilità amministrativa, che il compito di vigilare sul funzionamento e l'osservanza del modello sia affidato ad un organismo dell'Ente – è stato individuato, nell'ambito di Banca Sistema, un Organismo di Vigilanza (o **"OdV"**) collegiale, composto da tre membri tutti dotati della competenza e professionalità adeguate a ricoprire tale ruolo. L'OdV è composto dai seguenti soggetti:

(i) Dal Presidente del Collegio Sindacale o da un soggetto terzo con una consolidata esperienza in materia 231 nominato dal Consiglio di Amministrazione; tale soggetto assume di diritto anche la presidenza dell'OdV.

(ii) Da un amministratore nominato dal Consiglio di Amministrazione.

(iii) Dal responsabile della Direzione Internal Audit, per garantire un corretto coordinamento delle attività di verifica, evitando duplicazioni e sfruttando possibili sinergie dei controlli interni.

L'OdV è dotato di autonomi poteri di iniziativa e controllo, volti ad assicurare un'effettiva ed efficace attuazione del Modello, e deve presentare i seguenti requisiti:

1. Autonomia: deve avere un'autonomia decisionale, qualificabile come imprescindibile libertà di autodeterminazione e d'azione, con totale esercizio della discrezionalità tecnica nell'espletamento delle proprie funzioni. L'autonomia sarà in primo luogo nei confronti degli altri organi societari, ai vertici e al management, in modo tale che l'OdV possa agire libero da condizionamenti o pressioni. L'OdV dovrà inoltre godere di autonomia di spesa.
2. Indipendenza: deve essere scevro da condizionamenti dipendenti da legami di sudditanza rispetto al vertice di controllo della Banca e deve essere un

organo terzo, collocato in posizione di indipendenza anche gerarchica, capace di adottare provvedimenti ed iniziative autonome.

3. Professionalità: deve essere professionalmente capace ed affidabile, sia per quanto riguarda i singoli membri che lo compongono, sia nella sua globalità; deve disporre, come organo, delle cognizioni tecniche e delle professionalità necessarie al fine di espletare al meglio le funzioni affidategli. A tal fine, potrà avvalersi delle specifiche competenze dei singoli membri oppure di altri organi e/o funzioni aziendali (es. Rischio e Compliance/Antiriciclaggio), nonché di consulenti esterni.
4. Continuità di azione: deve svolgere le funzioni assegnategli in via continuativa, seppure non in modo esclusivo, avvalendosi del supporto di altre funzioni di controllo (es. Compliance/Antiriciclaggio e Internal Audit).
5. Onorabilità ed assenza di conflitti di interesse: non può essere nominato membro dell'OdV e, se del caso, decade dalla carica, il soggetto che:
   - sia interdetto, inabilitato o fallito o che sia comunque stato condannato per uno dei reati previsti dal Decreto o, comunque, ad una delle pene che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;
   - abbia rapporti d'affari (intesi, ad esempio, quali rapporti di *partnership*, contratti di associazione in partecipazione, *joint venture*, ecc.) con la Banca o le società controllate o che la controllano e/o qualsiasi altro rapporto tale da comprometterne l'indipendenza.

Qualora un membro dell'OdV abbia un interesse per conto proprio o di terzi in una delibera, dovrà darne comunicazione agli altri membri dell'Organismo, specificandone la natura, i termini, l'origine e la portata. Gli altri membri decideranno se il soggetto interessato dovrà astenersi dalla delibera.

Il Consiglio di Amministrazione nomina i membri dell'OdV, che restano in carica per tre anni, ma sono in qualunque tempo revocabili per giusta causa dal CdA.

È facoltà dell'OdV farsi coadiuvare, nelle sue funzioni di controllo, da soggetti esterni che svolgano professionalmente le attività di verifica.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza di un membro dell'OdV, il CdA provvederà alla sua sostituzione alla prima seduta utile. In ogni caso, il componente uscente resta in carica fino all'avvenuta nomina da parte del CdA del nuovo membro. Il Presidente coordina i lavori dell'Organismo e provvede affinché adeguate informazioni sulle materie iscritte all'ordine del giorno siano fornite a tutti i membri.

L'OdV ha adottato un proprio regolamento che disciplina il proprio funzionamento.

### 4.2 *Modalità di convocazione e tenuta delle riunioni dell'OdV*

L'OdV si raduna tutte le volte che il Presidente o uno dei membri lo ritenga opportuno, oppure quando ne sia fatta richiesta dal Consiglio di Amministrazione o dal Collegio Sindacale, e comunque almeno ogni sei mesi.

Le sedute dell'OdV saranno tenute nel luogo designato nell'avviso di convocazione, contenente l'indicazione del giorno, dell'ora e del luogo dell'adunanza e l'elenco delle materie da trattare. L'avviso di convocazione, da comunicare a ciascun membro dell'Organismo (per mezzo di posta elettronica, fax, a mano), dovrà essere inviato almeno tre giorni prima di quello fissato per la seduta stessa ovvero, in caso di urgenza, almeno un giorno prima.

Le adunanze dell'OdV potranno essere tenute anche per audio e/o videoconferenza, a condizione che tutti i partecipanti possano essere identificati e sia loro consentito seguire la discussione e intervenire alla trattazione degli argomenti e alla votazione.

Le decisioni dell'OdV sugli argomenti in esame possono essere adottate mediante consultazione scritta ovvero mediante consenso espresso per iscritto.

Tali delibere, così come i rapporti relativi alle verifiche compiute dall'Organismo stesso direttamente o tramite collaboratori esterni, saranno trascritte sul Libro delle Adunanze dell'Organismo, depositato presso gli uffici della Banca.

### 4.3 *Funzioni e poteri dell'OdV*

L'OdV di Banca Sistema è organo autonomo rispetto agli organi societari ed esente da vincoli di subordinazione gerarchica.

Ha come referenti aziendali, su base continuativa, l'Amministratore Delegato e i responsabili delle funzioni di controllo della Banca e, su base periodica, il Consiglio di Amministrazione e/o il Collegio Sindacale.

L'OdV della Banca potrà essere chiamato in qualsiasi momento dai suddetti organi - o potrà a sua volta presentare richiesta in tal senso - per riferire in merito al funzionamento del Modello od a situazioni specifiche.

Con cadenza almeno annuale, inoltre, l'OdV trasmette al Consiglio di Amministrazione e al Collegio Sindacale un rapporto scritto sulle attività svolte e sull'attuazione del Modello.

Per l'espletamento dei compiti dell'Organismo di Vigilanza è attribuita allo stesso piena autonomia economico/gestionale, non condizionata da limiti di spesa. L'Organismo informa tempestivamente il CdA della Banca nel caso impegni risorse rilevanti per fronteggiare situazioni eccezionali e urgenti.

All'Organismo di Vigilanza di Banca Sistema è affidato il compito di vigilare:

- sul funzionamento e sull'osservanza delle prescrizioni del Modello da parte dei destinatari, appositamente individuati nelle singole Parti Speciali in relazione alle diverse tipologie di reati contemplate dal Decreto;
- sulla reale efficacia ed effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei reati di cui al Decreto;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali.

Sul piano operativo è affidato all'OdV il compito di:

- attivare le procedure di controllo, tenendo presente che la responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al management operativo e forma parte integrante del processo aziendale, il che conferma l'importanza di un processo formativo del personale;

- condurre ricognizioni dell'attività aziendale ai fini della mappatura aggiornata delle aree di attività a rischio nell'ambito del contesto aziendale;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di attività a rischio come definite nelle singole Parti Speciali del Modello;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso, contenente le istruzioni, chiarimenti o aggiornamenti;
- raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo 4.5) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere allo stesso OdV obbligatoriamente trasmesse o tenute a sua disposizione;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree a rischio. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle suddette aree a rischio e ha libero accesso a tutta la documentazione aziendale rilevante. All'OdV devono essere inoltre segnalate da parte del management eventuali situazioni dell'attività aziendale che possano esporre la Banca al rischio di commissione di un reato;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di reati. In particolare, all'OdV devono essere segnalate le attività più significative o le operazioni contemplate dalle Parti Speciali, devono essere messi a sua disposizione i dati di aggiornamento della documentazione, al fine di consentire l'effettuazione dei controlli;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di reati (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di

osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a un aggiornamento degli elementi stessi;

- mantenere un collegamento costante con gli altri organi di controllo (Collegio Sindacale e Comitato di Controllo Interno)), la Società di revisione e le funzioni di controllo interno;
- coordinarsi con i responsabili delle altre funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello (definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, ecc.).

### 4.4 *Flussi informativi verso l'Organismo di Vigilanza*

Ai sensi dell'art. 6, comma 2, lettera d) del Decreto, l'OdV deve essere tempestivamente informato da tutti i soggetti destinatari del Modello in merito a qualsiasi notizia relativa all'esistenza di possibili violazioni del Modello stesso. In particolare, devono segnalare le notizie relative alla commissione o alla possibile commissione dei reati o di deviazioni comportamentali rispetto ai principi contenuti nel Modello.

In ogni caso, devono essere comunicate all'OdV le informazioni:

a) che possono avere attinenza con potenziali violazioni del Modello quali, a titolo meramente esemplificativo:
   - eventuali offerte o richieste di denaro di doni (eccedenti il valore modico) o di altre utilità provenienti da o destinate a pubblici ufficiali o incaricati di pubblico servizio;
   - provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini per i reati, anche nei confronti di ignoti qualora tali indagini coinvolgano la Banca e/o suoi esponenti aziendali e/o dipendenti;
   - le richieste di assistenza legale inoltrate dagli esponenti aziendali in caso di avvio di procedimento giudiziario per i reati;
   - le notizie relative ai procedimenti sanzionatori effettuati dalle Pubbliche Autorità e alle eventuali misure irrogate (ivi compresi i provvedimenti verso gli esponenti aziendali) ovvero dei provvedimenti di archiviazione di tali

procedimenti con le relative motivazioni, qualora essi siano legati a commissione di reati o violazione delle regole di comportamento o procedurali del Modello;

- anomalie di spese emerse dalle richieste di autorizzazione;
- eventuali omissioni o trascuratezze nella tenuta della contabilità su cui si fondano le registrazioni contabili;
- eventuali segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti sia carenze o inadeguatezze dei luoghi o delle attrezzature di lavoro o dei dispositivi di protezione messi a disposizione della Banca, sia ogni altra situazione di pericolo connessa alla sicurezza sul lavoro.

b) Le informazioni attinenti i compiti dell'OdV e che possono assumere rilevanza per l'espletamento delle sue funzioni, quali, ad esempio:

- le notizie relative ai cambiamenti organizzativi della Banca;
- i rapporti preparati dalle varie funzioni in merito a quelle attività che sono ritenute o che possono ritenersi attinenti ad aree a rischio della Banca;
- il bilancio annuale, corredato dalla nota integrativa e la situazione patrimoniale;
- le comunicazioni, da parte del Collegio Sindacale e della Società di revisione relative a criticità emerse, anche se risolte.

L'Organismo di Vigilanza assicura la massima riservatezza in ordine a qualsiasi notizia, informazione, segnalazione, a pena revoca del mandato e delle misure disciplinari definite nel presente documento, fatte salve le esigenze inerenti lo svolgimento delle indagini nell'ipotesi in cui sia necessario il supporto di consulenti esterni o di altre strutture societarie.

I soggetti apicali e sottoposti ai sensi dell'art. 5 lett. a) e b) del Decreto possono presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di cui siano venuti a conoscenza in ragione delle funzioni svolte relative a:

a) condotte illecite rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti;

b) violazioni del MOG.

Tali segnalazioni devono essere inviate con le seguenti modalità alternative:

a) all'apposita casella di posta elettronica odv@bancasistema.it;

b) mediante l'apposito canale informatico *"whistleblowing"* [3] disponibile sulla Intranet aziendale.

Il processo di gestione delle segnalazioni è disciplinato dal Regolamento dei sistemi interni di segnalazione delle violazioni (*whistleblowing*) adottato dalla Banca; entrambi i canali sopramenzionati garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione.

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute e intraprende le conseguenti iniziative a sua ragionevole discrezione e responsabilità nell'ambito delle proprie competenze, sentendo eventualmente l'autore della segnalazione ed il responsabile della presunta violazione. Ogni conseguente decisione sarà motivata e gli eventuali provvedimenti conseguenti saranno applicati in conformità a quanto previsto al capitolo 6 sul "Sistema Disciplinare".

In conformità alle disposizioni previste dalla Legge n. 179/2017, la Banca garantisce gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti della Banca o delle persone accusate erroneamente o in mala fede.

Si evidenzia che l'art. 6 del Decreto[4], comma 2-*ter*, prevede che l'adozione di misure discriminatorie nei confronti di soggetti che effettuano le segnalazioni di cui al comma 2-*bis* può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza. Inoltre, prevede che il licenziamento ritorsivo o discriminatorio del soggetto segnalante, così come il mutamento di mansioni, sono da considerarsi nulli (comma 2-*quater*). Spetta al datore di lavoro l'onere di dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

[3] Il Consiglio di Amministrazione ha nominato il responsabile della funzione di revisione interna della Banca come responsabile delle segnalazioni *whistleblowing*.
[4] La Legge 30 novembre 2017, n. 179 ha introdotto nel D.Lgs. n. 231/2001 il c.d. «whistleblowing», vale a dire la segnalazione di attività illecite o violazioni relative al modello organizzativo e gestione da parte del dipendente o collaboratore che ne sia venuto a conoscenza per ragioni di lavoro.

Ogni informazione e segnalazione di cui al presente Modello è conservata dall'Organismo di Vigilanza in un apposito archivio informatico e cartaceo, in conformità alle disposizioni contenute nel Decreto Legislativo 30 giugno 2003, n. 196 (Codice Privacy).

### 4.5 *Flussi informativi dell'Organismo di Vigilanza verso gli organi societari*

Il Presidente dell'OdV, o uno degli altri membri designato dallo stesso Organismo, informa il Consiglio di Amministrazione sull'applicazione e sull'attuazione del Modello, nonché sull'emersione di eventuali aspetti critici, sulla necessità di interventi modificativi, in caso di segnalazioni ricevute o altre fattispecie che rivestono carattere d'urgenza.

Entro 90 giorni dalla chiusura dell'esercizio sociale l'OdV predispone una relazione riepilogativa dell'attività svolta nel corso dell'anno trascorso ed un piano delle attività previste per l'anno in corso, da presentare al Consiglio di Amministrazione.

### 4.6 *Modalità di funzionamento dell'OdV*

L'OdV programma le attività di controllo periodico in funzione dello stato delle attività aziendali e delle informazioni in suo possesso.

Il programma annuale delle attività viene approvato dall'OdV all'inizio di ciascun esercizio, indicando quali aree e funzioni si intendono verificare e rispetto a quali criteri. Le verifiche potranno essere condotte dagli stessi membri dell'OdV, oppure affidate alla Direzione Internal Audit o a consulenti esterni.

Al termine di ogni verifica deve essere predisposto un rapporto che illustri l'attività svolta e le risultanze della stessa. Tra le risultanze devono essere indicate:

- le aree aziendali verificate ed ogni informazione utile ulteriore;
- il livello di conformità ovvero le criticità rilevate rispetto ai criteri dell'*audit*;
- il richiamo ai documenti di controllo;
- le eventuali raccomandazioni;
- ogni altra informazione ritenuta opportuna per la migliore valutazione dell'attività sottoposta a verifica.

In occasione della successiva riunione dell'OdV verranno esaminate le risultanze delle attività. L'OdV, ove lo ritenga opportuno, potrà effettuare delle ulteriori verifiche di approfondimento, anche con il supporto di consulenti esterni, ovvero richiedere all'organo di gestione della Banca di intervenire per riportare il livello di rischio a livelli ritenuti accettabili.

Le raccomandazioni dell'OdV devono trovare tempestivo accoglimento da parte delle funzioni interessate ed è compito del Consiglio di Amministrazione verificarne la efficace applicazione.

L'OdV solleciterà riunioni periodiche con il Collegio Sindacale e con le funzioni di controllo interno per la condivisione delle strategie per l'attuazione del sistema dei controlli interni, evitando sovrapposizioni e sfruttando sinergie.

# 5 Piano di comunicazione

## 5.1 *Introduzione*

La Banca, al fine di dare efficace attuazione del presente Modello, intende assicurare una corretta divulgazione dei contenuti e dei principi dello stesso all'interno ed all'esterno della propria struttura.

A questo proposito, obiettivo della Banca è di estendere la comunicazione dei contenuti e dei principi del Modello non solo ai propri dipendenti, ma anche ai soggetti che operano anche solo occasionalmente per il conseguimento degli obiettivi della Banca in forza di contratti e sui quali la Banca sia in grado di esercitare direzione o vigilanza (es. collectors).

Sebbene tale attività di comunicazione sia diversamente caratterizzata a seconda dei destinatari cui essa si rivolge, l'informazione concernente i contenuti e i principi del Modello sarà, comunque, improntata a completezza, tempestività, accuratezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare.

In particolare, l'OdV promuove idonee iniziative per la diffusione della conoscenza e della comprensione del Modello ai soggetti interessati.

## 5.2 *Diffusione e formazione*

I contenuti ed i principi del Modello saranno portati a conoscenza di tutti i dipendenti e gli altri soggetti che intrattengano con la Banca rapporti di collaborazione contrattualmente regolati.

Ogni dipendente è tenuto a:

i) acquisire consapevolezza dei contenuti del Modello;

ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività;

iii) contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

Al fine di garantire un'efficace e razionale attività di comunicazione, la Banca promuove e agevola la conoscenza dei contenuti del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda del grado di coinvolgimento nelle attività individuate come sensibili ai sensi del Decreto.

È garantita ai dipendenti la possibilità di accedere e consultare il Modello, il Codice Etico, nonché la normativa interna aziendale (procedure, regolamenti, policy, ecc.).

Inoltre, al fine di agevolare la comprensione del Modello, i dipendenti, con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del Decreto, sono tenuti a partecipare alle attività formative a carattere obbligatorio.

Ai nuovi dipendenti viene consegnata, all'atto dell'assunzione, una chiavetta USB contenente copia della normativa interna vigente e fatta sottoscrivere dichiarazione di osservanza dei contenuti del Modello.

Ai componenti degli organi sociali di Banca Sistema saranno applicate le medesime modalità di diffusione del Modello previste per i dipendenti.

Idonei strumenti di comunicazione saranno adottati per aggiornare i dipendenti circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

L'attività di comunicazione dei contenuti del Modello e del Codice Etico è indirizzata anche nei confronti di quei soggetti terzi che intrattengano con la Banca rapporti di collaborazione contrattualmente regolati o che rappresentano la Banca senza vincoli di dipendenza (ad esempio: partner commerciali, *introducer,* agenti in attività finanziaria, mediatori creditizi, promotori finanziari, consulenti, procacciatori d'affari ed altri collaboratori autonomi).

A tal fine, negli accordi con i soggetti terzi più significativi Banca Sistema farà sottoscrivere una dichiarazione che attesti la loro conoscenza del Modello e del Codice Etico, con l'impegno all'osservanza dei contenuti ivi descritti. Il MOG e il Codice Etico sono disponibili sul sito internet aziendale www.bancasistema.it nella sezione "Link Utili".

La conoscenza da parte di tutti i dipendenti di Banca Sistema dei principi e delle disposizioni contenuti nel Modello rappresenta elemento di primaria importanza per l'efficace attuazione dello stesso.

L'OdV si impegna ad organizzare specifici interventi formativi rivolti a tutti i dipendenti, al fine di assicurare un'adeguata conoscenza, comprensione e diffusione dei contenuti del Modello e di diffondere, altresì, una cultura aziendale orientata verso il perseguimento di una sempre maggiore trasparenza ed eticità.

I contenuti degli interventi formativi vengono costantemente aggiornati in relazione alle novità normative in materia 231 e alle integrazioni del Modello.

La partecipazione agli interventi formativi è obbligatoria e devono essere raccolte e archiviate a cura dell'OdV le evidenze/attestazioni relative all'effettiva partecipazione a detti interventi formativi.

# 6 Sistema disciplinare

## 6.1 *Principi generali*

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso e per rendere efficiente l'azione dell'OdV.

Al riguardo, infatti, l'art. 6, comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione devono "*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello*".

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dalla Banca in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

L'accertamento delle infrazioni può essere avviato anche d'impulso dell'OdV che abbia, nel corso della sua attività di controllo e vigilanza, rilevato una possibile infrazione del Modello.

L'irrogazione delle sanzioni nei confronti di dirigenti, quadri e impiegati sono di competenza dell'Amministratore Delegato o, a seconda dei casi, dalla Direzione Risorse Umane.

L'OdV può, inoltre, essere chiamato a svolgere una funzione consultiva nel corso dell'intero procedimento disciplinare al fine di acquisire eventuali elementi utili in vista del costante aggiornamento del Modello. L'accertamento delle eventuali responsabilità derivanti dalla violazione del Modello e l'attribuzione della conseguente sanzione devono essere comunque condotti nel rispetto della vigente normativa, della tutela della privacy, della dignità e della reputazione dei soggetti coinvolti.

Il sistema disciplinare viene costantemente monitorato dall'Organismo di Vigilanza e dalla Direzione Risorse Umane.

### 6.2 *Misure nei confronti degli Amministratori*

La Banca valuta con estremo rigore le infrazioni al presente Modello poste in essere da coloro che rappresentano il vertice della Banca e ne manifestano dunque l'immagine verso i dipendenti, gli azionisti, i creditori ed il pubblico.

La formazione e il consolidamento di un'etica aziendale sensibile ai valori della correttezza e della trasparenza presuppongono, innanzitutto, che tali valori siano acquisiti e rispettati da coloro che guidano le scelte aziendali, in modo da costituire esempio e stimolo per tutti coloro che, a qualsiasi livello, operano per la Banca.
In caso di violazione da parte degli Amministratori delle procedure interne e dei principi di comportamento previsti dal presente Modello e/o di adozione, nell'esercizio delle proprie attribuzioni, di provvedimenti che contrastino con le disposizioni o i principi del Modello, l'OdV informa tempestivamente tutti i membri del Consiglio di Amministrazione e tutti i componenti del Collegio Sindacale, i quali, a seconda delle rispettive competenze, provvederanno ad assumere le iniziative più opportune ed adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto (es.: dichiarazioni nei verbali delle adunanze, convocazione dell'Assemblea dei Soci per deliberare in merito ai provvedimenti nei confronti dei soggetti responsabili della violazione tra cui la revoca della nomina di amministratore e l'eventuale adozione delle azioni di responsabilità previste dalla legge).

### 6.3 *Misure nei confronti dei membri del Collegio Sindacale*

Con riguardo ai componenti del Collegio Sindacale, le violazioni delle prescrizioni contenute nel presente Modello sono segnalate tempestivamente dall'OdV, a tutti i componenti del Collegio Sindacale e a tutti i membri del Consiglio di Amministrazione. Il Collegio Sindacale assume, sentito il parere del Consiglio di Amministrazione, gli opportuni provvedimenti nei confronti dei Sindaci che hanno compiuto le violazioni contestate.

### 6.4 *Sistema sanzionatorio nei confronti del personale dirigente*

In caso di violazione delle disposizioni e delle regole comportamentali contenute nel Modello da parte di dirigenti, - non essendo previsto dal relativo contratto collettivo alcun provvedimento disciplinare di natura "conservativa" stante la particolare natura del vincolo fiduciario di tale categoria di dipendenti – la Banca potrà valutare come le predette violazioni costituiscano adeguato motivo di "giustificatezza" per la risoluzione del rapporto di lavoro con il dirigente medesimo.

### 6.5 *Sistema sanzionatorio nei confronti del personale dipendente*

I comportamenti tenuti dai lavoratori dipendenti (esclusi i dirigenti) in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari.

Con riferimento alle sanzioni comminabili nei riguardi di detti lavoratori dipendenti esse rientrano tra quelle previste dalla Legge 300/1970 ("Statuto dei lavoratori"), aggiornata dalla Legge n. 92 del 28 giugno 2012, e dalle relative disposizioni contenute nel CCNL bancario vigente.

In relazione a quanto sopra, il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio sopra indicato. Tali categorie descrivono i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

Il lavoratore che violi le procedure interne previste dal presente Modello o adotti, nell'espletamento delle proprie attività, un comportamento non conforme alle prescrizioni del Modello stesso e del Codice Etico, dovendosi ravvisare in tali comportamenti una violazione del contratto che comporta un pregiudizio alla disciplina e morale dell'azienda, si applicano i provvedimenti disciplinari previsti, in relazione alla gravità o recidività della mancanza o al grado della colpa, che sono:

a. incorre nel provvedimento di "rimprovero verbale" il lavoratore che violi una delle procedure interne previste nel presente Modello, o adotti un comportamento non conforme alle prescrizioni del Modello stesso;
b. incorre nel provvedimento di "rimprovero scritto" il lavoratore che sia recidivo nel violare le procedure previste dal Modello o nell'adottare un comportamento non conforme alle prescrizioni del Modello stesso;
c. incorre nel provvedimento di "sospensione dal lavoro e dalla retribuzione" (per un massimo di giorni 10) il lavoratore che nel violare le procedure interne previste dal Modello, o adottando nell'espletamento di attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello, arrechi danno, o crei situazioni di potenziale pericolo alla Banca, ovvero il lavoratore che sia incorso con recidiva nelle mancanze di cui al punto b). Tali comportamenti, posti in essere per la mancata osservanza delle disposizioni impartite dalla Banca, potrebbero determinare un danno ai beni della Banca e/o costituiscono atti contrari agli interessi della stessa e/o espongono la Banca a rischi di sanzioni amministrative o interdittive;
d. incorre nel provvedimento di "risoluzione del rapporto di lavoro per giustificato motivo soggettivo" il lavoratore che adotti nell'espletamento delle proprie attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello e ne costituisca un notevole inadempimento, diretto in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/01 o che determini la concreta applicazione a carico della Banca delle misure previste dal D.Lgs. 231/01; tale comportamento costituisce una notevole inosservanza delle disposizioni impartite dalla Banca e/o una grave violazione dell'obbligo del lavoratore di cooperare alla prosperità della Banca;
e. incorre nel provvedimento di "risoluzione del rapporto di lavoro per giusta causa" il lavoratore che adotti nell'espletamento delle proprie attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello e ne costituisca un grave inadempimento, diretto in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/01 o che determini la concreta applicazione a carico della Società delle misure previste dal D.Lgs.

231/01, nonché il lavoratore che sia incorso con recidiva nelle mancanze di cui al punto 3, prima parte. Tale comportamento fa venire meno radicalmente la fiducia della Banca nei confronti del lavoratore costituendo un grave pregiudizio per l'azienda.

Il tipo e l'entità delle sanzioni sopra richiamate comminate al personale dipendente dovranno tenere conto, in sede applicativa, del principio di proporzionalità previsto dall'art. 2106 c.c., considerando per ciascuna fattispecie:

- dell'intenzionalità e del grado di reiterazione del comportamento, del grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- della gravità oggettiva del fatto costituente infrazione disciplinare;
- del comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- delle mansioni del lavoratore;
- della posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- delle altre particolari circostanze che accompagnano la violazione disciplinare.

A titolo esemplificativo e non esaustivo, costituiscono infrazioni disciplinari i seguenti comportamenti:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, dei principi e delle procedure previste dal presente Modello o stabilite per la sua attuazione;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, mediante condotta omissiva, della redazione da parte di altri, di documentazione non veritiera;
- l'omessa redazione della documentazione richiesta dal presente Modello o dalle procedure stabilite per la sua attuazione;

- la sottrazione, la distruzione o l'alterazione della documentazione inerente la procedura per sottrarsi al sistema dei controlli previsto dal Modello;
- l'ostacolo alla attività di vigilanza dell'OdV o dei soggetti dei quali lo stesso si avvale;
- l'impedimento all'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti ai controlli delle procedure e delle decisioni;
- la realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal Modello.

Responsabile della concreta applicazione delle misure disciplinari sopra descritte è il Responsabile della funzione di gestione risorse umane, il quale irrogherà le sanzioni su eventuale segnalazione dell'Organismo di Vigilanza, sentito anche, il parere del superiore gerarchico dell'autore della condotta censurata. Viene comunque attribuito all'Organismo di Vigilanza, in collaborazione con il responsabile della funzione di gestione delle risorse umane, il compito di verificare e valutare l'idoneità del sistema disciplinare ai sensi e per gli effetti del D.Lgs. 231/01.

### 6.6 *Misure nei confronti di collaboratori esterni*

Ogni comportamento posto in essere da parte di altri Destinatari, esterni alla Banca, quali i lavoratori autonomi, i professionisti, i consulenti, i fornitori e i partner commerciali, in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, grazie all'attivazione di opportune clausole inserite nei contratti, la risoluzione del rapporto contrattuale.

La Direzione Legale e Affari Societari cura l'elaborazione, l'aggiornamento e l'inserimento - nelle lettere di incarico o negli accordi di partnership - di tali specifiche clausole contrattuali che prevedranno anche l'eventuale richiesta di risarcimento di danni derivanti alla Banca dall'applicazione da parte del Giudice delle misure previste dal Decreto.

### 6.7 *Misure relative alla normativa sulle segnalazioni*

Il mancato rispetto della normativa relativa alle segnalazioni ai sensi dell'art. 6, comma 2-bis del Decreto è sanzionato dagli organi competenti in base alle regole interne della Banca e del CCNL bancario vigente nei seguenti casi:

- le violazioni delle misure a tutela del segnalante;
- nei confronti del segnalante in caso di segnalazioni effettuate con dolo o colpa grave che si rilevano infondate.

# PARTE SPECIALE

# Finalità della Parte Speciale

Scopo della presente Parte Speciale è fare in modo che tutti i destinatari del Modello (quali, a titolo esemplificativo, i dipendenti, i dirigenti, gli amministratori, i liquidatori, i consulenti, gli agenti in attività finanziaria, i promotori finanziari, i mediatori creditizi, i fornitori, i collaboratori esterni, gli *introducer*, i partner della Banca e, in generale, tutti coloro che sono tenuti a rispettare il presente Modello e, di seguito, i "Destinatari") adottino regole di condotta conformi a quanto prescritto al fine di impedire il verificarsi dei reati in essa considerati.

In particolare, la Parte Speciale ha la funzione di:

a. descrivere i principi procedurali – generali e specifici – che i Destinatari del Modello sono tenuti ad osservare ai fini della corretta applicazione del Modello;
b. fornire all'OdV gli strumenti esecutivi per esercitare l'attività di controllo e verifica previste dal Modello.

Il Decreto legislativo n. 231/2001 individua alcune fattispecie di reato che, se commesse da soggetti che rivestono una posizione apicale all'interno della Banca o da persone sottoposte alla loro direzione o vigilanza (artt. 6-7), costituiscono fonte di responsabilità per gli enti, qualora risultino compiuti nell'interesse o a vantaggio degli stessi.

In considerazione della natura dell'attività svolta da Banca Sistema, sono stati valutati come rilevanti - ossia come potenzialmente a rischio di essere commessi nell'interesse o a vantaggio della società - ai fini della predisposizione del presente Modello, solo i seguenti reati previsti dal Decreto 231/2001:

A) Reati contro la Pubblica Amministrazione (art. 24 e 25)
B) Reati societari (art. 25-*ter*)
C) Reati di abuso di mercato (art. 25-sexies)
D) Reati in materia di salute e sicurezza sul lavoro (art. 25-*septies*)
E) Reati di riciclaggio (art. 25-*octies*)
F) Reati informatici e trattamento illecito dei dati (art. 24-*bis*)

Alla luce delle stesse considerazioni di cui sopra, è stata di contro ritenuta ragionevolmente contenuta la rilevanza degli altri reati presupposto individuati dal D.Lgs. 231/2001 e riportati al Capitolo 1.2 della Parte Generale del presente Modello. Si è ritenuto infatti che il rischio di compimento di tali ultimi reati da parte di un soggetto che opera nella Banca, nello svolgimento di una delle attività della stessa nell'interesse e/o a vantaggio della Banca, rappresenti, anche astrattamente, un'ipotesi difficilmente configurabile.

In ogni caso il presente Modello e l'intero sistema di controllo interno della Banca non trascurano neppure tali fattispecie, cui pertanto sono applicabili le norme comportamentali contenute nella Parte Generale del Modello, nel Codice di Etico di Banca Sistema con la conseguente l'applicazione del sistema di controlli interni già adottati pur senza la necessità di strutturare ulteriori specifici apparati procedurali mirati.

Pertanto, la presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo risulta suddivisa in sezioni che tengono conto esclusivamente delle diverse tipologie di reato individuate più sopra.

# A) REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Nell'esercizio dell'attività di impresa le società possono entrare in contatto con la Pubblica Amministrazione. Rientrano in questa categoria le società che partecipano a gare o a procedure di appalto, ottengono autorizzazioni, concessioni, licenze, partecipano a procedure per ricevere finanziamenti pubblici, si occupano di prestare servizi o di realizzare opere per la Pubblica Amministrazione.

Per "Pubblica Amministrazione" si intende, in estrema sintesi, qualsiasi Ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- Istituti e scuole di ogni ordine e grado e le istituzioni educative;
- Enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, sezioni fallimentari);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);
- Aziende Sanitarie Locali, Aziende Ospedaliere e altri Enti Pubblici del Servizio Sanitario Nazionale;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA.

Ai sensi dell'art. 357 c.p., primo comma, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

La norma chiarisce solo la nozione di "pubblica funzione amministrativa" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita "pubblica" la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l'art. 358 c.p. definisce i "soggetti incaricati di un pubblico servizio" come quei soggetti "i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della "pubblica funzione", da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di un pubblico servizio colui il quale svolge una pubblica autorità non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni

d'ordine e/o la prestazione d'opera meramente materiale e, in quanto tali, prive di alcun apporto intellettuale e discrezionale.

Nel caso di Banca Sistema, la principale occasione di contatto con la P.A. deriva dall'attività di acquisto pro-soluto, gestione ed incasso di crediti nei confronti della P.A. Ugualmente rilevanti sono i rapporti istituzionali con le Autorità di Vigilanza (Banca d'Italia e Consob).

## 1 Reati contro la Pubblica Amministrazione

I reati contro la Pubblica Amministrazione disciplinati nel D.Lgs. 231/2001 sono:

- **Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)**

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

Tale ipotesi di reato si configura nel caso in cui, dopo aver ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Il reato di malversazione potrebbe quindi essere commesso mediante la destinazione dei fondi agevolati ottenuti a scopi diversi da quelli dichiarati.

Sanzioni pecuniarie *ex* D.Lgs. 231/01: Fino a 500 quote, aumentate da 200 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto o sia derivato un danno grave.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 2)

esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; 3) divieto di pubblicizzare beni o servizi per un periodo da tre mesi a due anni.

- **Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-*ter* c.p.)**

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

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità europea.

Il reato d'indebita percezione di erogazioni a danno dello Stato potrebbe essere commesso nella fase di richiesta di erogazione di un finanziamento concesso (anche a titolo di acconto) ed acquisizione del finanziamento agevolato tramite presentazione di richieste che contengano dichiarazioni o documenti falsi o attestanti cose non vere o omettano informazioni dovute.

Sanzioni pecuniarie *ex* D.Lgs. 231/01: Da 100 a 500 quote, aumentate da 200 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto o sia derivato un danno grave.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 2) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca

di quelli già concessi; 3) divieto di pubblicizzare beni o servizi per un periodo da tre mesi a due anni.

- **Corruzione in atti giudiziari (art. 319-*ter* c.p.)**

Il reato di corruzione in atti giudiziari potrebbe essere commesso nei confronti di Giudici o membri del Collegio Arbitrale competenti a giudicare sul contenzioso/arbitrato di interesse del Gruppo (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia controparte del contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 200 a 600 quote (1° comma), da 300 a 800 quote (2° comma).

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) interdizione dall'esercizio dell'attività, 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, 4) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, 5) divieto di pubblicizzare beni o servizi. Tutti per un periodo non inferiore ad un anno.

- **Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)**

Le disposizioni dell'art. 319 ("Corruzione per un atto contrario ai doveri d'ufficio") si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio; quelle di cui all'art. 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato. In ogni caso, le pene sono ridotte in misura non superiore ad un terzo.

Sanzioni pecuniarie *ex* D.Lgs. 231/01: Medesime sanzioni pecuniarie previste per i reati di cui agli artt. 318 e 319 c.p..

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) interdizione dall'esercizio dell'attività, 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, 4) esclusione da

agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, 5) divieto di pubblicizzare beni o servizi. Tutti per un periodo non inferiore ad un anno.

- **Pene per il corruttore (art. 321 c.p.)**

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: in caso di reati *ex* art. 381 c.p.p. da 100 a 200 quote, in caso di reati *ex* art. 319 e 319-*ter* c.p. da 200 a 600 quote. In caso di reati *ex* artt. 319-bis e 319-*ter* comma 2 c.p. da 300 a 800 quote.

Sanzioni interdittive *ex* D.Lgs. 231/01: non previste.

- **Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)**

La legge 6 novembre 2012, n. 190 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" o c.d. "legge Severino") ha introdotto una nuova fattispecie delittuosa all'art. 319-*quater* c.p. (induzione indebita a dare o promettere utilità).

Le principali novità per il D.Lgs. 231/01 si sostanziano nei seguenti nuovi reati:

> Art. 319-*quater* codice penale, *"induzione indebita a dare o promettere utilità": 1) Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dieci anni e sei mesi. 2) Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni".*

La sanzione pecuniaria prevista va da trecento a ottocento quote (equivalente ad una condanna pecuniaria che può arrivare fino a un milione duecentomila euro), oltre alla possibile misura interdittiva per una durata non inferiore ad un anno.

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

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

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

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

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: in caso di reati *ex* art. 381 c.p.p. da 100 a 200 quote; in caso di reati *ex* art. 319 e 319 *ter* c.p. da 200 a 600 quote; In caso di reati *ex* artt. 319 *bis* e 319 *ter* comma 2, da 300 a 800 quote.

Non sono previste sanzioni interdittive.

- **Truffa (art. 640 c.p.)**

*"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1) se il fatto è commesso a danno dello Stato o di un altro Ente pubblico o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità. Il delitto è punibile a querela della persona offesa, salvo che*

*ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 100 a 500 quote aumentate da 200 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto o sia derivato un danno grave.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 2) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; 3) divieto di pubblicizzare beni o servizi. Per un periodo da tre mesi a due anni.

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

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 100 a 500 quote aumentate da 200 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto o sia derivato un danno grave.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, 2) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, 3) divieto di pubblicizzare beni o servizi. Per un periodo da tre mesi a due anni.

- **Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.)**

*"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad*

*esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*
*La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.*
*Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 100 a 500 quote aumentate da 200 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto o sia derivato un danno grave.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, 2) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, 3) divieto di pubblicizzare beni o servizi. Per un periodo da tre mesi a due anni.

# 2 Aree a rischio reato

Le potenziali aree a rischio reato che Banca Sistema ha individuato nei rapporti con la Pubblica Amministrazione e nell'ambito dei reati di cui al Decreto sono quelle relative alle attività di:

a. acquisto pro-soluto di crediti nei confronti della PA e conseguenti rapporti con la medesima relativi al monitoraggio ed incasso dei crediti ceduti;
b. negoziazione, stipulazione ed esecuzione di contratti/convenzioni con la PA (inclusi atti transattivi concernenti i crediti acquistati di cui al precedente punto a.) mediante procedure negoziate (affidamento diretto o trattativa privata) o ad evidenza pubblica (aperte o ristrette);
c. gestione dei rapporti con la PA – incluse le Autorità Pubbliche di Vigilanza (Banca d'Italia, Consob, UIF, Ministeri, Autorità Garante per la protezione dei dati personali) – che operino quali pubbliche autorità con riferimento a determinate aree di competenza;
d. gestione dei rapporti con la PA per l'ottenimento di permessi/ licenze/autorizzazioni;
e. rapporti con autorità inquirenti (Carabinieri, Polizia di Stato, Polizia Municipale, Guardia di Finanza);
f. gestione dei software di Enti Pubblici (ASL) o forniti da terzi per conto di Enti Pubblici e collegamenti telematici o trasmissione di dati su supporti informatici a Enti Pubblici;
g. rapporti con mandatari, agenti in attività finanziaria, mediatori creditizi, *introducer*, promotori finanziari e intermediari (selezione, instaurazione e regolamento del rapporto, determinazione del compenso, gestione e scioglimento del rapporto) che a loro volta interagiscono con la PA;
h. predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere.
i. gestione di liberalità/omaggi/pubblicità;
j. gestione dei processi di assunzione del personale e dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata;
k. gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (*ex* D.Lgs. 81/08);

l. gestione dei trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
m. verifica del processo di liquidazione delle note spese dei dipendenti.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'OdV.

# 3 Regole di comportamento

*Il sistema dei controlli*

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Banca, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.
In particolare, la presente Parte Speciale prevede l'espresso divieto di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;
2. effettuare prestazioni in favore di fornitori, consulenti, partner e collaboratori in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
3. proporre opportunità commerciali che possano avvantaggiare dipendenti della PA a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della PA, o comunque di soggetti agli stessi collegati;
4. effettuare elargizioni in denaro e regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli

omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere l'immagine della Banca. Tutti i regali offerti – salvo quelli di modico valore – devono essere documentati in modo idoneo per consentire all'OdV di effettuare verifiche al riguardo;

5. comunicare alla PA dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
6. violare i sistemi informativi della PA al fine di ottenere o manipolare informazioni a vantaggio della Banca;
7. stipulare contratti in assenza dei relativi poteri. Il soggetto che intrattiene rapporti o effettua negoziazioni con la PA non può stipulare i contratti che ha negoziato in assenza di specifici poteri: la negoziazione e stipulazione dei contratti avviene solo sulla base di una delega o autorizzazione o procura a tal fine formalizzate con indicazione di vincoli e responsabilità;
8. porre in essere artifici o raggiri tali da indurre la PA a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti, o in generale delle controprestazioni;
9. distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti;
10. effettuare pagamenti in contanti, salvo espressa autorizzazione da parte della Direzione Finance che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'Ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio;
11. presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche;
12. accedere a risorse finanziarie:
    a. l'effettuazione delle spese deve avvenire solo in base ad una delega o autorizzazione o procura formalizzate con limiti di valore, vincoli e responsabilità
    b. le spese possono essere effettuate solo in base a documenti giustificativi con motivazione, attestazione di inerenza e congruità, approvati da adeguato livello gerarchico e archiviati;

13. conferire contratti di consulenza, intermediazione o similari in assenza dei relativi poteri. Nessuno può da solo e liberamente conferire incarichi di consulenza, intermediazione o altra prestazione professionale similare:
    a. il conferimento dell'incarico può essere operato solo in base a una delega o autorizzazione o procura formalizzate, con limiti di spesa, vincoli e responsabilità;
    b. l'incarico viene conferito sulla base di una lista di fornitori/consulenti/ professionisti, gestita dalla funzione competente. L'inserimento/ eliminazione dalla lista è basato su criteri oggettivi. L'individuazione all'interno della lista è motivata e documentata;
    c. gli incarichi possono essere conferiti solo in base a documenti giustificativi con motivazione e nominativi, attestazione di inerenza e congruità, approvati da adeguato livello gerarchico e archiviati.

Al fine di prevenire l'attuazione dei comportamenti sopra descritti:

- deve risultare una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla PA (ad esempio, nel caso di contratto stipulato con una ASL, deve essere ben chiara, all'interno della Banca, la segregazione delle funzioni tra (i) chi propone la stipulazione del contratto; (ii) chi effettua l'attività di *risk assessment* per valutare la possibilità di stipulare il contratto; (iii) chi raccoglie e dispone la documentazione necessaria; (iv) chi approva e sottoscrive il contratto);
- gli accordi di associazione con i partner devono essere definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso, in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura e devono essere proposti, verificati ed approvati da almeno due soggetti appartenenti alla Banca;
- nessun tipo di pagamento può essere effettuato in contanti o in natura, al di sopra dei limiti stabiliti dalla Banca;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono

porre particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;

- qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la PA deve essere comunicato all'OdV con nota scritta;
- con riferimento alla gestione dei rapporti con l'amministrazione finanziaria è necessario:
  a. protocollare le procedure che disciplinino la partecipazione alle ispezioni giudiziarie, tributarie, fiscali, amministrative e/o di Vigilanza e la gestione dei rapporti con soggetti pubblici al fine di ottenere autorizzazioni, licenze o altro;
  b. conservare traccia, attraverso la redazione di appositi verbali, di tutto il procedimento relativo all'ispezione. Nel caso in cui il verbale conclusivo evidenziasse delle criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta.

*Contratti con i collaboratori esterni*

I contratti con i collaboratori esterni che hanno rapporti con le PA devono contenere una clausola volta a disciplinare le conseguenze della violazione da parte degli stessi degli obblighi prescritti nel Decreto, nonché dei principi comportamentali dettati dal Modello.

# 4 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'OdV:

a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
b. verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
c. esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
d. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
e. curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

# B) REATI SOCIETARI

# 1 Reati societari

I reati societari che possono dare origine ad una responsabilità amministrativa dell'Ente *ex* art. 25-*ter*[5] del D.Lgs. 231/2001 sono i seguenti:

- **False comunicazioni sociali (art. 2621 c.c.[6])**

*"Fuori dai casi previsti dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni. La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi".*

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 400 quote, sanzioni interdittive non previste.

- **False comunicazioni sociali delle società quotate (art. 2622 c.c.[7])**

*"Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione*

[5] Articolo aggiunto dal D.Lgs. n. 11 aprile 2002, n. 61, art. 3 e modificati dalla Legge n. 262/2005, dalla Legge n. 190/2012, dalla Legge n. 69/2015 e dal D.Lgs. n. 38/2017.
[6] Articolo modificato con la Legge 27 maggio 2015, n. 69.
[7] Articolo modificato con la Legge 27 maggio 2015, n. 69.

*è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni. Alle società indicate nel comma precedente sono equiparate:*

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

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

*3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;*

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

*Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01: per il 1° comma da 400 a 600 quote, per il 3° comma da 400 a 800; sanzioni interdittive non previste.

- **Impedito controllo (art. 2625 c.c., comma 2)**

*"Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro. Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 360 quote, sanzioni interdittive non previste.

- **Indebita restituzione dei conferimenti (art. 2626 c.c.)**

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 360 quote, sanzioni interdittive non previste.

- **Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)**

*"Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 260 quote; sanzioni interdittive non previste.

- **Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)**

*"Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge. Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto."*

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 360 quote, sanzioni interdittive non previste.

- **Operazioni in pregiudizio dei creditori (art. 2629 c.c.)**

*"Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o*

*scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato".*

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 300 a 660 quote, sanzioni interdittive non previste.

- **Omessa comunicazione del conflitto d'interessi (art. 2629-*bis* c.c.)**

"L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del TUF, ovvero di un soggetto sottoposto a vigilanza ai sensi del TUB, del TUF, del D.Lgs. 7.9.2005, n. 209, o del D.Lgs. 21.4.1993, n. 124, che viola gli obblighi previsti dall'art. 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi."

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 400 a 1.000 quote; sanzioni interdittive non previste.

- **Formazione fittizia del capitale (art. 2632 c.c.)**

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 200 a 360 quote; sanzioni interdittive non previste.

- **Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)**

"I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la

reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato".

Sanzioni pecuniarie *ex* D.Lgs. 231/01 da 300 a 360 quote.; sanzioni interdittive non previste.

- **Corruzione tra privati (articolo 2635 del c.c.[8])**

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

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

3. Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

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

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

L'ente risponde qualora uno dei Destinatari compia la condotta descritta dal terzo comma della norma: in altre parole, ad essere punito è solo l'ente nel quale opera il corruttore.

Sanzioni pecuniarie *ex* D.Lgs. 231/01: Da 400 a 600 quote, aumentate da 600 a 900 quote qualora l'Ente abbia conseguito un rilevante profitto.

[8] Aggiunto dalla Legge n. 190/2012 e modificato dal D.Lgs. n. 38/2017.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 4) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; 5) divieto di pubblicizzare beni o servizi. Per un periodo massimo di due anni.

- **Istigazione alla corruzione tra privati (art. 2635-*bis* del codice civile[9])**

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

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: Da 200 a 400 quote, aumentate da 300 a 600 quote qualora l'Ente abbia conseguito un rilevante profitto.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 4) esclusione da

[9] Aggiunto dal D.Lgs. n. 38/2017.

agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; 5) divieto di pubblicizzare beni o servizi. Per un periodo massimo di due anni.

- **Illecita influenza sull'assemblea (art. 2636 c.c.)**

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 300 a 660 quote; sanzioni interdittive non previste.

- **Aggiotaggio (art. 2637 c.c.)**

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

Sanzioni pecuniarie *ex* D.Lgs. n. 231/01 da 400 a 1.000 quote; sanzioni interdittive non previste.

- **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)**

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

Sanzioni pecuniarie *ex* D.Lgs. n. 231/01 da 400 a 800 quote; sanzioni interdittive non previste.

# 2 Aree a rischio reato

Le potenziali aree a rischio reato che la Banca ha individuato nell'ambito dei reati societari sono quelle relative:

a. alla gestione delle informazioni riservate;
b. all'adempimento degli obblighi informativi in tema di conflitto di interessi;
c. alla predisposizione dei bilanci, relazioni e altre comunicazioni sociali previste dalla legge;
d. alla gestione delle partecipazioni, delle operazioni sul capitale sociale e delle operazioni straordinarie;
e. all'attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee, dei Consigli di Amministrazione e delle riunioni del Comitato Esecutivo (se costituito);
f. alla gestione dei rapporti con il Collegio Sindacale, la società di revisione e degli altri organi societari;
g. alle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse.
h. alla gestione dei contenziosi giudiziari, stragiudiziali e degli accordi transattivi;
i. alla selezione e assunzione del personale;
j. alla gestione degli omaggi, delle spese di rappresentanza, delle iniziative di beneficienza e delle sponsorizzazioni;
k. alla gestione dei rimborsi spese.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'OdV.

# 3 Regole di comportamento

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Banca, dalle procedure operative e ogni altra normativa interna relativa al sistema di *corporate governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (*ex* art. 25-*ter* del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca. A questo proposito, è fatto espresso divieto di:
    - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Banca;
    - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Banca;
b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Banca, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività della Banca, fino alle fasi eventuali di liquidazione o cessazione della Banca stessa;
e. assicurare il regolare funzionamento della Banca e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della

Banca previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
   - omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
   - esporre, nelle predette comunicazioni e trasmissioni, fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Banca;
   - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
g. predisporre apposite procedure per la preparazione del bilancio e la gestione delle risorse finanziarie;
h. osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;
i. assumere un comportamento corretto e veritiero con gli organi di stampa, di informazione e con gli analisti finanziari;
j. astenersi dal porre in essere qualsiasi comportamento idoneo a configurare un abuso di mercato;
k. astenersi da effettuare operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari.

In relazione alle aree a rischio individuate nella presente Parte Speciale, si riportano di seguito specifici principi di comportamento da tenere in osservanza del Decreto.

In particolare, i bilanci di esercizio, le relazioni e altre comunicazioni sociali previste dalla legge (presentazione dei dati, elaborazione ed approvazione) devono essere redatti in base a specifiche procedure aziendali che:

- determinino con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati (per esempio, i criteri seguiti nella valutazione di poste di bilancio aventi natura estimativa quali i crediti e il loro presumibile valore di realizzo, il fondo rischi ed oneri, i dividendi, il fondo imposte e tasse, ecc.) e la tempistica per la loro consegna alle funzioni responsabili;
- prevedano la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consenta la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- utilizzino informazioni previsionali condivise dalle funzioni coinvolte ed approvate dagli organi sociali.

Inoltre, per la predisposizione delle comunicazioni ai Soci relative alla situazione economica, patrimoniale e finanziaria della Banca, si dispone che la redazione delle stesse sia effettuata determinando in maniera chiara e completa:

- i dati e le informazioni che ciascuna funzione deve fornire;
- i criteri contabili per l'elaborazione dei dati;
- la tempistica per la loro consegna alle aree aziendali responsabili.

Infine, in aggiunta ai presidi appena previsti e a quelli già adottati dalla Banca, si dispone:

a. la previsione dell'effettuazione di almeno un Consiglio di Amministrazione a trimestre finalizzato alla condivisione di fatti rilevanti, attinenti alla gestione della Banca;
b. la trasmissione agli Amministratori e al Collegio Sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'Assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;
c. la previsione di riunioni periodiche tra il Collegio Sindacale e l'OdV per verificare l'osservanza della disciplina in tema di normativa societaria e di *Corporate Governance.*

I contratti con i collaboratori esterni devono contenere una clausola volta a disciplinare le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché dei principi contenuti nel Modello.

# 4 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'OdV:

a. verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, informativa verso gli organi deputati, ecc.);
b. monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;
c. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
d. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
e. curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

# C) REATI DI ABUSO DI MERCATO

## 1 Reati di abuso di mercato

La presente Sezione della Parte Speciale del Modello è stata introdotta a seguito della quotazione di Banca Sistema SpA al mercato STAR gestito da Borsa Italiana SpA, avvenuta a luglio 2015.

I reati di cui all'art. 25-*sexies*[10] del D.Lgs. 231/2001 sono i seguenti:

- **Abuso di informazioni privilegiate[11] (art. 184 D.Lgs. n. 58/1998)**

  1. "È punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

     a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

     b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014;

     c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

  2. La stessa pena di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.

  3. Il Giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del

[10] Articolo aggiunto dalla Legge 18 aprile 2005, n. 62 e modificati dalla Legge n. 262/2005.
[11] Articolo modificato dal D.Lgs. 10 agosto 2018, n. 107.

prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

3-*bis*. Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numeri 2), 2-*bis*) e 2-*ter*), limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni, la sanzione penale è quella dell'ammenda fino a euro centotremila e duecentonovantuno e dell'arresto fino a tre anni.

Secondo l'art. 7 del Regolamento (EU) n. 596/2014 relativo agli abusi di mercato l'informazione, per essere considerata privilegiata:

a. deve avere un carattere preciso (ovvero, se essa fa riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se tale informazione è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto di detto complesso di circostanze o di detto evento sui prezzi degli strumenti finanziari o del relativo strumento finanziario derivato, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base delle quote di emissioni);
b. non deve essere stata resa pubblica;
c. deve essere concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari negoziati non solo in mercati regolamentati ma anche in MTF o OTF o *over-the-counter*;
d. se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati (c.d. *"price sensitive"*).

Rilevante è anche il caso di un processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o

dell'evento futuri, possono essere considerate come informazioni aventi carattere preciso.

- **Manipolazione di mercato[12] (art. 185 D.Lgs. 58/1998[13])**

  "1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da € 20.000,00 a € 5.000.000,00.

  1-bis. Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del Regolamento (UE) n. 596/2014.

  2. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

  2-*bis*. Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numeri 2), 2-bis) e 2-*ter*), limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni, la sanzione penale è quella dell'ammenda fino a € 103.291,00 e dell'arresto fino a tre anni".

  2-*ter*. Le disposizioni del presente articolo si applicano anche: a) ai fatti concernenti i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari di cui all'articolo 180, comma 1, lettera a);

[12] I beni giuridici che la norma intende tutelare sono l'integrità dei mercati finanziari regolamentati e la protezione e l'accrescimento della fiducia degli investitori.
[13] Articolo modificato dal D.Lgs. 10 agosto 2018, n. 107.

b) ai fatti concernenti gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari; c) ai fatti concernenti gli indici di riferimento (*benchmark*).

In entrambe le fattispecie di cui sopra non sono previste sanzioni interdittive.

Si sottolinea inoltre che gli artt. 187-*bis* e 187-*ter* TUF (introdotti dalla Legge Comunitaria)[14] tipizzano, rispettivamente, gli illeciti amministrativi di abuso e comunicazione illecita di informazioni privilegiate e di manipolazione del mercato. Questi ultimi illeciti sono puniti – salve le relative sanzioni penali applicabili. L'articolo 187-*bis* punisce con la sanzione amministrativa pecuniaria da ventimila euro a cinque milioni di euro la condotta di violazione del divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate di cui all'articolo 14 del Regolamento (UE) n. 596/2014.

L'art- 187-*ter* punisce con la sanzione amministrativa pecuniaria da ventimila euro a cinque milioni di euro la violazione del divieto di manipolazione del mercato di cui all'articolo 15 del Regolamento (UE) n. 596/2014.

Si evidenzia che, trattandosi di illeciti amministrativi, le sanzioni previste dal TUF si applicano anche quando le condotte richiamate sono poste in essere a titolo di mera colpa. Il potere di comminare tali sanzioni amministrative è affidato alla Consob dall'art. 187-*ter1* e 187-*quater.*

Il sistema sanzionatorio, sul piano amministrativo, si completa con la previsione dell'art. 187-*quinquies* TUF[15], prevede che la Consob possa applicare sanzioni amministrative.

- **Responsabilità dell'ente (art. 187-*quinques* D.Lgs. n. 58/1998)**

  "1. L'ente è punito con la sanzione amministrativa pecuniaria da ventimila euro fino a quindici milioni di euro, ovvero fino al quindici per cento del fatturato,

[14] Entrambi gli articoli sono stati modificati dal D.Lgs. 10 agosto 2018, n. 107.
[15] Articolo modificato dal D.Lgs. 10 agosto 2018, n. 107.

quando tale importo è superiore a quindici milioni di euro e il fatturato è determinabile ai sensi dell'articolo 195, comma 1-*bis*, nel caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 o del divieto di cui all'articolo 15 del regolamento (UE) n. 596/2014: (a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; (b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

2. Se, in seguito alla commissione degli illeciti di cui al comma 1, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.

3. L'ente non è responsabile se dimostra che le persone indicate nel comma 1 hanno agito esclusivamente nell'interesse proprio o di terzi.

4. In relazione agli illeciti di cui al comma 1 si applicano, in quanto compatibili, gli articoli 6, 7, 8 e 12 del decreto legislativo 8 giugno 2001, n. 231. Il Ministero della giustizia formula le osservazioni di cui all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231, sentita la Consob, con riguardo agli illeciti previsti dal presente titolo. Pertanto, se la fattispecie di illecito presupposto assume rilevanza penale, l'eventuale responsabilità dell'ente sarà accertata in sede giudiziaria; se invece si tratta di un illecito amministrativo - posto in essere comunque nell'interesse o a vantaggio dell'ente - l'accertamento e l'applicazione delle relative sanzioni spetterà alla Consob. Al riguardo, il TUF chiarisce i rapporti tra i procedimenti amministrativo e penale (Capo V, artt. 187-decies e ss.) e, con riferimento ai profili di accertamento delle responsabilità dei soggetti coinvolti, stabilisce che "il procedimento amministrativo di accertamento e il procedimento di opposizione di cui all'art. 187-septies non possono essere sospesi per la pendenza del procedimento penale avente ad oggetto i medesimi fatti o fatti dal cui accertamento dipende la relativa definizione".

Pertanto, una stessa fattispecie/notizia di illecito potrebbe contestualmente essere oggetto di un procedimento penale dinanzi al giudice ordinario e di un

procedimento amministrativo presso la Consob, con un conseguente accertamento della responsabilità dell'ente per la medesima fattispecie sia in sede giudiziaria che amministrativa. In merito, l'art. 187-terdecies prevede che quando per lo stesso fatto è stata applicata a carico del reo, , dell'autore della violazione o dell'ente una sanzione amministrativa pecuniaria ai sensi dell'articolo 187-*septies* ovvero una sanzione penale o una sanzione amministrativa dipendente da reato: a) l'autorità giudiziaria o la Consob tengono conto, al momento dell'irrogazione delle sanzioni di propria competenza, delle misure punitive già irrogate; b) l'esazione della pena pecuniaria, della sanzione pecuniaria dipendente da reato ovvero della sanzione pecuniaria amministrativa è limitata alla parte eccedente quella riscossa, rispettivamente, dall'autorità amministrativa ovvero da quella giudiziaria.

# 2 Aree a rischio reato

*Abuso di informazioni privilegiate*

Un soggetto in posizione apicale o un sottoposto che rientri in una delle categorie di cui all'art. 184, co. 1 TUF utilizza informazioni di cui è entrato in possesso e compie una delle seguenti operazioni:

- acquisto, vendita o altre operazioni, direttamente o indirettamente, su strumenti finanziari emessi dalla società o da società del gruppo;
- comunicazione delle informazioni ad altri soggetti al di fuori dell'ordinario esercizio dell'attività lavorativa;
- raccomandazione ad altri o induzione di altri soggetti ad acquistare, vendere o compiere altre operazioni su strumenti finanziari emessi dalla società o da società del gruppo.

Le stesse operazioni rilevano laddove poste in essere da soggetti sempre in posizione di apicali o sottoposti, che non rientrano tra quelli di cui all'art. 184, co. 1 TUF, ma che comunque vengano in possesso di informazioni privilegiate in

occasione della preparazione o esecuzione di attività delittuose (art. 184, co. 2, TUF).

Con riferimento al solo illecito amministrativo, le stesse operazioni rilevano anche qualora commesse dai soggetti di cui all'art. 187-*bis*, co. 1 del TUF qualora le condotte siano di violazione del divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate di cui all'articolo 14 del Regolamento (UE) n. 596/2014.

Risultano pertanto potenzialmente a rischio illecito le seguenti aree o funzioni:

- Organi sociali;
- Direzione Finanza/Tesoreria
- Area Investor Relations;
- Direzione Affari Legali e Segreteria societaria
- Direzione Marketing e Comunicazione;
- altri soggetti inseriti nei registri delle persone che hanno accesso alle informazioni privilegiate.

*Manipolazione di mercato*

Un soggetto in posizione apicale o un sottoposto che pone in essere uno dei seguenti comportamenti idoneo a provocare una sensibile alterazione del prezzo di strumenti finanziari:

- diffusioni di informazioni false;
- realizzazione di operazioni simulate;
- altri artifici.

Risultano pertanto potenzialmente a rischio illecito la Direzione Finanza/ Tesoreria.

Con riferimento al solo illecito amministrativo, le stesse operazioni rilevano anche qualora commesse dai soggetti di cui all'art. 187-*ter*, co. 1 del TUF qualora le condotte siano di violazione del divieto di manipolazione del mercato di cui all'articolo 15 del Regolamento (UE) n. 596/2014.

Risultano pertanto potenzialmente a rischio illecito le seguenti aree/funzioni:

- componenti degli organi sociali;

- Direzione Finanza/Tesoreria;
- Funzione Affari Societari;
- Investor relations;
- Direzione Marketing;
- Direzione Commerciale Factoring.

# 3 Regole di comportamento

In linea generale, ed al fine di prevenire la commissione dei reati di abuso di mercato, i Destinatari, che svolgono la propria attività nell'ambito delle aree a rischio reato individuate in precedenza, e fermo restando quanto indicato dal Codice Etico, sono tenuti al rispetto dei seguenti principi generali di condotta:

a) si astengono dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato sopra riportate;
b) mantengono una condotta improntata ai principi di correttezza, trasparenza, collaborazione e rispetto delle norme di legge nonché regolamentari vigenti, nell'esecuzione di tutte le attività in cui vengano in possesso di informazioni privilegiate o di notizie che possano permettere loro di porre in essere manipolazioni informative o operative di mercato;
c) osservano le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;
d) non agiscono di concerto con una o più persone per acquisire una posizione sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;
e) si astengono dal porre in essere operazioni simulate o altrimenti fraudolente, nonché diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari;

f) assumono un comportamento corretto e veritiero con gli organi di stampa, di informazione e con gli analisti finanziari;
g) si astengono dall'effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interesse, almeno che lo stesso non venga esplicitato nelle forme previste dalla normativa interna.

# 4 Compiti dell'Organismo di Vigilanza

Fermi restando i compiti e le funzioni dell'OdV statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei reati descritti dalla presente Parte Speciale, lo stesso è tenuto a:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello e delle regole di *corporate governance* rispetto all'esigenza di prevenire la commissione dei reati di aggiotaggio e di *market abuse*;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- esaminare eventuali segnalazioni provenienti dagli organi di controllo e da qualsiasi dipendente e disporre gli accertamenti ritenuti necessari;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- vigilare costantemente sull'aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività;
- verificare periodicamente, con il supporto delle funzioni aziendali competenti, che il sistema delle deleghe in vigore sia attinente alla quotidiana operatività della Banca;
- verificare il rispetto delle procedure operative e dei principi ivi contenuti, con particolare riferimento alle operazioni su strumenti finanziari quotati e non;

- verificare eventuali anomalie segnalate nello svolgimento di operazioni che, in base a ragionevoli motivi, possono configurare violazione delle disposizioni sull'abuso delle informazioni privilegiate e sulle manipolazioni di mercato.

Al fine di assolvere efficacemente e tempestivamente ai compiti sopra elencati, all'OdV devono pervenire adeguati flussi informativi, anche in materia di reati di aggiotaggio e di abuso di mercato, così come descritti nella Parte Generale del Modello.

Si ricorda, inoltre, che, tra i suoi compiti, l'OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati di aggiotaggio e di abuso di mercato al Consiglio di Amministrazione nonché al Collegio Sindacale.

# D) REATI DI RICICLAGGIO

## 1 Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Con il Decreto Legislativo 21 novembre 2007, n. 231[16] (c.d. "Decreto Antiriciclaggio") sono stati introdotti nel novero dei reati previsti dal D.Lgs. n. 231/2001, all'art. 25-*octies* i reati di ricettazione (art. 648 c.p.), riciclaggio (art-*bis* c.p.) e impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.), descritti di seguito.

- **Ricettazione (art. 648 c.p.)**

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

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 200 a 800 quote. Qualora il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione pecuniaria da 400 a 1000 quote. Confisca obbligatoria anche per equivalente del prezzo, profitto o prodotto del reato.

Sanzioni interdittive *ex* D.Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 4) esclusione da

[16] Il D.Lgs. n. 231/2007 è stato emanato in attuazione della Direttiva 2005/60/CE ed è concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e modificato dal D.Lgs. n. 90 del 2017 in attuazione della Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE.

agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; 5) divieto di pubblicizzare beni o servizi. Per un periodo massimo di due anni.

- **Riciclaggio (art. 648-bis c.p.)**

"Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita le pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648."

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 200 a 800 quote. Qualora il denaro, i beni o le altre utilità provengano da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione pecuniaria da 400 a 1000 quote, oltre alla confisca obbligatoria per l'equivalente del prezzo, profitto o prodotto del reato.

Sanzioni interdittive *ex* D.Lgs. 231/01: a) interdizione dall'esercizio dell'attività; b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi per un periodo massimo di due anni.

- **Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.), nonché autoriciclaggio (art. 648-*ter*.1 c.p.)**

Art. 648-*ter* c.p. (Impiego di denaro, beni o utilità di provenienza illecita)

"Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-*bis* del c.p., impiega in attività economiche o finanziarie denaro, beni o altre

utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a 25.000. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648. Si applica l'ultimo comma dell'articolo 648."

Art. 648-*ter*.1 (Autoriciclaggio)

L'art. 3, comma 3, della Legge n. 186/2014 ha introdotto nel nostro ordinamento giuridico, dal 1° gennaio 2015, il nuovo reato di autoriciclaggio, includendo questa nuova fattispecie nel cosiddetto "catalogo" dei reati previsti dal D.Lgs. n. 231/2001.

L'autoriciclaggio consiste nell'attività di occultamento dei proventi derivanti da crimini propri, come ad esempio: l'evasione fiscale, la corruzione e l'appropriazione di beni sociali.

L'art. 648- *ter*.1 prevede quanto segue: "Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa. Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni.

Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.
La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Si applica l'ultimo comma dell'articolo 648."

Sanzioni pecuniarie *ex* D.Lgs. 231/01: da 200 a 800 quote. Qualora il denaro, i beni o le altre utilità provengano da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione pecuniaria da 400 a 1000 quote. Confisca obbligatoria anche per equivalente del prezzo, profitto o prodotto del reato.

Sanzioni interdittive *ex* D.Lgs. 231/01: a) interdizione dall'esercizio dell'attività; b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi per un periodo massimo di due anni.

# 2 Aree a rischio reato

Le potenziali aree a rischio reato, nell'ambito dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, che Banca Sistema ha individuato riguardano le attività concernenti:

a. l'acquisto pro-soluto di crediti verso il sistema di sanità nazionale;
b. apertura di conti correnti e adempimenti previsti per l'adeguata verifica dei clienti;
c. svolgimento di servizi finanziari e di investimento per i propri clienti;
d. la negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria;

e. la realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà;
f. la selezione dei partner commerciali/finanziari e la gestione dei relativi rapporti;
g. la gestione dei rapporti con i fornitori;
h. la definizione delle modalità dei mezzi di pagamento;
i. la gestione degli investimenti (quali, ad esempio, acquisizioni di partecipazioni o aziende, accordi strategici, altre operazioni di finanza straordinaria);
j. indebita percezione di contributi pubblici.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'OdV.

La Banca ha adottato una specifica policy interna in materia di antiriciclaggio, approvata dal Consiglio di Amministrazione, e ha nominato un responsabile in materia.

# 3 Regole di comportamento

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dal Decreto Antiriciclaggio e dallo Statuto della Banca nonché le procedure operative e ogni altra normativa interna relativa al sistema di *corporate governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di:

1. assumere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-*octies* del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente diventarlo;
2. intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo,

persone legate all'ambiente del riciclaggio, del terrorismo, al traffico di droga, all'usura, ecc.;

3. utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti;
4. accettare rapporti contrattuali con clienti o altre controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI[17];
5. effettuare elargizioni in denaro ad individui, società od organizzazioni condannate per aver svolto attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico.

Inoltre, è previsto, a carico dei Destinatari, l'espresso obbligo di:

1. con riferimento all'attendibilità commerciale/professionale dei fornitori e dei partner, richiedere tutte le informazioni necessarie al fine di valutarne l'affidabilità e la solidità economica;
2. assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
3. tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti;
4. prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri.

In relazione alle aree a rischio individuate si riportano di seguito specifici principi di comportamento, peraltro già disciplinati dal D.Lgs. n. 231/2007, ai quali la Banca è soggetta in osservanza al Decreto:

a. la Banca deve creare uno specifico dossier clienti e fornitori onde raccogliere e censire le informazioni più significative relative agli stessi (quali, a titolo puramente esemplificativo, il legale rappresentante, la nazione di residenza, il tipo di attività economica, i bilanci societari degli ultimi 2 anni, ecc.) anche

[17] Costituito nel 1989 in occasione del G7 di Parigi, il Gruppo d'Azione Finanziaria Internazionale (GAFI) o Financial Action Task Force (FATF) è un organismo intergovernativo che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo.

al fine di poter desumere i requisiti di onorabilità e professionalità delle controparti con le quali la Banca opera;

b. la Banca deve procedere alla selezione dei fornitori e dei partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri oggettivi e documentabili, verificandone l'attendibilità commerciale (ad esempio, attraverso: visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni estere; referenze da parte di altri soggetti già in rapporti con la Banca o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione; certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere);
c. la Banca non accetta e non effettua pagamenti in contanti, se non sotto una certa soglia e comunque sempre nel rispetto dei limiti stabiliti dalla legge;
d. la Banca effettua un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
e. nel caso di elargizioni di danaro ad individui, società od organizzazioni è necessario controllare la serietà e la professionalità del destinatario del denaro. Inoltre, deve essere redatto un piano di investimento a giustificazione dell'investimento, comprensivo di controlli periodici dell'avanzamento del piano;
f. la Banca verifica *ex ante* che i soggetti con cui intrattiene rapporti contrattuali, anche lavorativi, non siano inseriti nelle *black-list* antiterrorismo.

I contratti con i collaboratori esterni che hanno rapporti con la PA devono contenere una clausola volta a disciplinare le conseguenze della violazione da parte degli stessi degli obblighi prescritti nel Decreto, nonché dei principi comportamentali dettati dal Modello.

# 4 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, è compito dell'OdV:

a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-*octies* del Decreto;
b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale con le altre funzioni di controllo.
c. verificare che venga svolta attività di formazione del personale sulla normativa antiriciclaggio.

A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

# E) REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

## 1 Reati informatici e trattamento illecito dei dati

La Convenzione del Consiglio d'Europa sulla criminalità informatica, siglata a Budapest il 23 novembre 2001, costituisce il primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche. Questo accordo si pone l'obiettivo di realizzare una politica comune sul tema tra gli Stati membri, attraverso l'adozione di una legislazione appropriata che consenta di combattere il crimine informatico in maniera coordinata.

Il legislatore italiano ha ratificato la citata Convenzione con la Legge 18 marzo 2008, n. 48 che ha apportato significative modifiche al nostro *corpus* normativo dal punto di vista sostanziale e processuale.

La conoscenza della struttura e delle modalità con cui si configurano i reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del D.Lgs. n. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e, quindi, all'intero sistema di controlli previsto dal Decreto.

La portata delle modifiche introdotte ha investito anche il D.Lgs. n. 231/01 che, sulla scorta della previsione contenuta al nuovo articolo 24-bis, sancisce la punibilità, ai sensi del citato Decreto, delle condotte criminose delineate dagli articoli novellati del codice penale qualora i reati in questione siano commessi da dipendenti dell'ente, da soggetti ad essi equiparati e/o da soggetti in posizione apicale anche nell'interesse e/o a vantaggio dell'ente stesso.

Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri, obiettivo stesso della condotta e, in altri, lo strumento attraverso cui l'autore intende realizzare un'altra fattispecie penalmente rilevante.

Lo sviluppo della tecnologia informatica ha generato nel corso degli anni modifiche sostanziali nell'organizzazione del business di impresa e ha inciso sensibilmente sulle opportunità a disposizione di ciascun esponente aziendale per realizzare o

occultare non soltanto schemi di condotte criminali già esistenti ma anche fattispecie nuove, tipiche del cd. "mondo virtuale".

Si precisa che la Banca utilizza un sistema informatico e di telecomunicazione finalizzato a gestire la complessità del contesto operativo e normativo in cui opera, come espressamente richiesto anche dalle specifiche normative in materia. In tale contesto, il sistema informativo della Banca è gestito in *full outsourcing* (Application Management e Facility Management) da parte di un fornitore esterno (Consorzio Servizi Bancari).

Di seguito si riporta una breve descrizione dei reati richiamati dall'art. 24-*bis* del D.Lgs. n. 231/2001 i cui protocolli di controllo sono stati definiti nella fase di aggiornamento del presente Modello Organizzativo.

- **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-*bis* c.p.)**

Le disposizioni del codice penale relative alle falsità nei documenti cartacei sono estese anche alle falsità sui documenti informatici: con quest'ultima espressione si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

L'art. 491-*bis* c.p. fornisce una definizione di documento informatico basata sull'elemento materiale del supporto di memoria e non sui dati in esso contenuti: può definirsi supporto informatico qualsiasi supporto di memoria – sia esso interno sia esso esterno all'elaboratore elettronico – sul quale possono essere registrati e conservati per un certo periodo di tempo dei dati destinati ad essere letti ed eventualmente elaborati da un sistema informatico.

Non costituisce supporto informatico ai sensi dell'art. 491-*bis* c.p. il tabulato emesso dal computer al termine del processo di elaborazione: il tabulato – così come ogni output stampato – è infatti normalmente costituito da un foglio di carta sul quale il contenuto dei dati è riprodotto in caratteri alfanumerici per consentirne la lettura da parte dell'uomo; rientrano invece nella nozione di documento informatico le carte di pagamento a banda magnetica e le carte a microprocessore (ad es. carte prepagate, carta a scalare e delle carte telefoniche).

È inoltre documento informatico il supporto informatico che contenga il programma specificamente destinato ad elaborare i dati, ossia il programma memorizzato all'interno del sistema informatico o su un supporto esterno che svolga la funzione di elaborare dati.

- **Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.)**

*"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
*La pena è della reclusione da uno a cinque anni:*

*1) se il fatto è commesso da uno da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
*2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*
*3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*

*Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.*
*Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa, negli altri casi si procede d'ufficio".*

Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico.
In particolare, per sistema informatico, ai fini della configurabilità del delitto di cui all'art. 615-*ter* c.p., deve intendersi una pluralità di apparecchiature destinate

a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche. Il sistema è dunque tale se gestisce ed elabora dati, mentre tutto ciò che in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è sistema informatico.

L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, ossia tutte quelle misure di protezione al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema, quali a titolo esemplificativo codici di accesso, alfabetici o numerici da digitare su una tastiera o memorizzati su una banda magnetica di una tessera da introdurre in apposito lettore. Oltre a queste misure logiche possono rilevare anche misure fisiche quali l'uso di chiavi metalliche per l'accensione dell'elaboratore.

La condotta rilevante consiste nell'introdursi abusivamente in un sistema protetto o nel permanervi contro la volontà espressa o tacita del titolare del diritto di escludere gli altri dall'uso del sistema. Si ha introduzione quando si oltrepassano le barriere logiche e/o fisiche che presidiano l'accesso alla memoria interna del sistema e si è quindi in condizione di richiamare i dati ed i programmi che vi sono contenuti. L'introduzione può avvenire sia da lontano ossia per via elettronica sia da vicino da parte di chi si trovi a diretto contatto con l'elaboratore.

Oltre all'introduzione rileva anche l'ipotesi del mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare dello *ius excludendi*: tale caso ricorre quando in seguito ad un'introduzione involontaria o causale o solo inizialmente autorizzata l'agente permanga nel sistema informatico altrui nonostante il dissenso del soggetto che ha interesse alla riservatezza dei dati e dei programmi in esso contenuti.

È bene precisare che per operatore di sistema deve intendersi solo quella particolare figura di tecnico dell'informatica (c.d. *system administrator*) che all'interno di un'azienda ha il controllo delle diverse fasi del processo di elaborazione dati nonché la possibilità di accedere a tutti i settori della memoria del sistema informatico su cui opera oppure di altri sistemi, qualora vi sia un collegamento in rete.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)**

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

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

L'art. 615-*quater* è rivolto a punire la condotta di detenzione e di diffusione abusiva di codici di accesso che può portare alla commissione di altri reati informatici: infatti chi entra in possesso abusivamente di codici d'accesso, può commettere un accesso abusivo ad un sistema o può diffondere tali codici ad altre persone che a loro volta potrebbero accedere abusivamente al sistema.

L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo: può infatti trattarsi di una password, di un codice d'accesso o semplicemente di informazioni che consentano di eludere le misure di protezione.

La disposizione in esame incrimina due tipi di condotte volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui oppure a procurare ad altri tali mezzi o comunque le informazioni sul modo di eludere le barriere di protezione; non è invece punita la semplice detenzione di codici di accesso o di strumenti similari da parte di chi non sia autorizzato a farne uso.

- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.)**

*"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo*

*funzionamento, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro".*

L'art. 615-*quinques* c.p. è rivolto a tutelare il patrimonio informatico, inteso come hardware, software e dati da attacchi con virus informatici.

La condotta punita è la diffusione (divulgazione), la comunicazione (portare a conoscenza) o la consegna (dare in senso materiale) di un programma informatico che ha lo scopo o l'effetto di danneggiare il sistema informatico o telematico altrui, o di danneggiare dati o programmi in esso contenuti o ad esso pertinenti, oppure l'interruzione parziale o totale del suo funzionamento o la sua alterazione.

La legge non fa distinzione tra virus creati da chi commette il reato o da terzi, né tanto meno tra programma informatico che reca concretamente un danno al sistema informatico e quello che non lo provoca.

Un programma può essere definito infetto ai sensi della disposizione in esame se è in grado non solo di danneggiare le componenti logiche di un sistema informatico, ma anche di interrompere o alterare il funzionamento di quest'ultimo.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.)**

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

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

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

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

*1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;*

*2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;*

*3) da chi esercita anche abusivamente la professione di investigatore privato".*

Ai sensi della disposizione in esame la condotta può consistere alternativamente nell'intercettare fraudolentemente una comunicazione informatica o telematica oppure nell'impedirla o interromperla; il secondo comma prevede poi l'ipotesi della rivelazione in tutto o in parte mediante qualsiasi mezzo di informazione al pubblico del contenuto di una conversazione intercettata.

Intercettare una comunicazione informatica o telematica significa prendere cognizione del suo contenuto intromettendosi nella fase della sua trasmissione; l'intercettazione deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso (ad es. decodificando dei dati trasmessi in forma cifrata o superando delle barriere logiche poste a difesa del sistema che invia o riceve la comunicazione) o comunque in modo tale da rendere non percepibile o riconoscibile a terzi l'intromissione abusiva.

La comunicazione è invece impedita quando se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati; una comunicazione può invece essere interrotta sia agendo sul sistema che invia e che deve ricevere la comunicazione sia ad esempio deviando il flusso dei dati in corso di trasmissione da un elaboratore ad un altro.

- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.)**

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

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

Tale disposizione mira a reprimere una condotta antecedente e preparatoria rispetto a quella prevista dall'art. 617-*quater* c.p. vietando l'installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Il reato previsto dall'art. 617-*quinquies* c.p. è stato ravvisato nel caso di utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione con il sistema rientra nella nozione di "intercettare" di cui alla norma incriminatrice.

- **Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.)**

*"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

*Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".*

Oggetto del danneggiamento può essere innanzitutto un sistema informatico di qualsiasi tipo e dimensione eventualmente collegato a distanza con altri elaboratori come nel caso dei sistemi telematici. L'aggressione può rivolgersi tanto al sistema nel suo complesso quanto a una o più delle sue componenti materiali, quali a titolo esemplificativo le periferiche. Non possono invece essere considerati componenti di un sistema informatico i supporti magnetici o ottici sui quali non siano memorizzati dati o programmi, in quanto il loro danneggiamento non arreca nessun pregiudizio alla funzionalità del sistema informatico nel quale dovrebbero essere utilizzati.

Oltre al sistema informatico il danneggiamento può avere ad oggetto dati e programmi informatici: per dati si intendono quelle rappresentazioni di informazioni o di concetti che, essendo destinate alla elaborazione da parte di un computer, sono codificate in una forma (elettronica, magnetica ottica o similare)

non percettibile visivamente. Suscettibili di danneggiamento possono essere anche dati o programmi immagazzinati nella memoria interna dell'elaboratore oppure su un supporto esterno come un disco magnetico o ottico.

Tra i beni suscettibili di danneggiamento l'art. 635-*bis* c.p. indica anche le informazioni: poiché l'informazione è un'entità di per sé astratta, questa espressione assume significato solo in quanto la si riferisca alle informazioni incorporate su un supporto materiale, cartaceo o di altro tipo.

Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e la inservibilità totale o parziale. L'ipotesi di distruzione di dati e programmi più frequente e significativa è rappresentata dalla loro cancellazione: sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con nuovi dati diversi, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa. Poiché la distruzione deve essere totale, non ricorre questa ipotesi quando i dati o i programmi cancellati siano ancora recuperabili in una zona remota dell'elaboratore, utilizzando un determinato tipo di programma oppure ne sia stata solo impedita la visualizzazione sullo schermo del computer.

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

*"Salvo che il fatto costituisca un più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

*Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.*

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

Per la descrizione degli elementi costitutivi del reato si rimanda alle fattispecie precedenti.

- **Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.)**

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

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

Per la descrizione degli elementi costitutivi del reato si rimanda alle fattispecie precedenti.

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.)**

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

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

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

Per la descrizione degli elementi costitutivi del reato si rimanda alle fattispecie precedenti.

- **Frode informatica del certificatore di firma elettronica (art. 640-*quinquies* c.p.)**

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

La direttiva europea 1999/93/CE, recepita con il D.Lgs. 23 gennaio 2002, n. 10, ha regolamentato lo strumento delle firme informatiche nel quadro comunitario con l'obiettivo di promuoverne l'utilizzo e il riconoscimento giuridico con l'introduzione sia di una disciplina organica in materia sia di alcuni servizi di certificazione che ne garantiscano il corretto funzionamento. Gli interventi normativi nazionali volti a promuovere un effettivo adeguamento alla disciplina comunitaria sono stati numerosi e hanno condotto all'emanazione del Codice dell'amministrazione digitale (D.Lgs. n. 82/2005 parzialmente modificato dal D.Lgs. n. 159/2006 e dal D.Lgs. n. 235/2010) che attualmente costituisce la fonte primaria in materia.

# 2 Aree a rischio reato

L'analisi dei processi aziendali di Banca Sistema ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzate le fattispecie di reato richiamate dall'art. 24-*bis* del D.Lgs. n. 231/2001. Di seguito sono pertanto elencate le cosiddette "attività sensibili" o "a rischio" identificate mediante tale analisi, con riferimento ai delitti informatici.

1) Gestione dei profili utente e del processo di autenticazione.
2) Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio.
3) Gestione e protezione della postazione di lavoro.
4) Gestione degli accessi da e verso l'esterno.
5) Gestione e protezione delle reti.
6) Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, ecc.).

# 3 Regole di comportamento

Il sistema dei controlli, perfezionato da Banca Sistema prevede, con riferimento alle attività sensibili individuate:

- principi generali di controllo relativi alle attività sensibili;
- protocolli specifici, applicati alle singole attività sensibili.

***Principi generali di controllo***

I principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo possono essere sintetizzati come segue:

- Procedure/linee guida formalizzate. Sono previste una normativa interna (policy aziendali, procedure, ecc.) e una esterna (leggi, regolamenti, disposizioni di vigilanza, ecc.) di riferimento idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.

- Segregazione dei compiti. In applicazione a tale principio le attività di autorizzazione, esecuzione, contabilizzazione e controllo delle operazioni sono separate e condotte da soggetti diversi al fine di garantire indipendenza ed obiettività dei processi.

- Esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate. I poteri autorizzativi e di firma sono: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Banca.

- Tracciabilità e verificabilità *ex-post* delle transazioni tramite adeguati supporti documentali/informativi. Ogni operazione svolta nell'ambito di un'attività sensibile è adeguatamente documentata e registrata. Il processo di decisione, autorizzazione, svolgimento e controllo dell'attività sensibile è verificabile *ex* post, anche mediante l'ausilio di appositi supporti documentali e, in ogni caso,

sono disciplinati con dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

- Attività di monitoraggio al fine di consentire l'aggiornamento periodico/ tempestivo delle deleghe e del sistema di controllo. Le funzioni competenti monitorano periodicamente, con il supporto delle altre funzioni, il sistema di deleghe e procure in vigore verificandone la coerenza con il sistema decisionale, nonché con l'intero impianto della struttura organizzativa, raccomandando eventuali modifiche, a titolo esemplificativo, nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato ovvero siano state ravvisate altre anomalie.

### ***Principi specifici di controllo***

Di seguito si riportano le principali modalità applicative dei controlli relativamente alle attività sensibili precedentemente individuate.

- Politiche di sicurezza. Le disposizioni in materia di sicurezza rivolte al personale della Banca e a quello esterno (fornitori e terze parti) che accedono alle informazioni aziendali sono disciplinate nel DPS.
- Organizzazione della sicurezza per gli utenti. La Banca ha definito apposite istruzioni interne per disciplinare i comportamenti del personale nell'utilizzo degli strumenti informatici, indicando le regole di sicurezza adottate per garantire la riservatezza, l'integrità e la disponibilità delle informazioni trattate.
  Relativamente al trattamento dei dati personali tutelati dalla normativa privacy sono stati nominati i responsabili del trattamento per le varie funzioni aziendali e gli incaricati del trattamento, a cui sono state impartite le necessarie istruzioni.
- Sicurezza fisica e ambientale. L'accesso ai locali aziendali è monitorato da misure di sicurezza fisiche con apertura degli accessi tramite badge e da strumenti di allarme. Le sale server della Banca posizionate presso i locali del fornitore sono sottoposte alle misure di sicurezza fisica, alle procedure ed alle istruzioni operative indicate nel relativo contratto: in particolare sono implementati strumenti di segregazione fisica con accessi controllati e con meccanismi di

autenticazione che consentono di operare al solo personale autorizzato. Inoltre, presso la sala server sono presenti le principali misure di sicurezza ambientale per la prevenzione dai rischi di incendio e assenza di corrente elettrica.

- Gestione delle comunicazioni e dell'operatività. Il sistema informatico della Banca è protetto contro accessi non autorizzati dall'esterno mediante sistemi firewall e strumenti di sicurezza perimetrale che separano l'ambiente aziendale dall'esterno. Numerose misure sono previste per la limitazione agli accessi internet, per la prevenzione da spam e per la protezione da software pericoloso attraverso l'installazione di programmi antivirus, aggiornati in automatico con da un server centrale, che distribuisce le firme dei virus sia sui server che sui personal computer. È mantenuta evidenza degli accessi e delle operazioni svolte sia dagli utenti applicativi che dagli amministratori di sistema e risultano tracciabili gli interventi di modifica dei sistemi e degli applicativi, anche in situazioni di emergenza.
- Controllo degli accessi. L'attivazione/modifica/disabilitazione degli utenti viene effettuata dalla struttura IT della Banca su richiesta da parte dell'ufficio Personale secondo procedure consolidate. L'accesso alla rete aziendale e quello ai sistemi informativi avvengono mediante codice identificativo individuale che viene assegnato ai singoli utenti e gestito in modo tale che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso ai dati (es. dimissioni o a seguito di *job rotation*) o di mancato utilizzo.

  Il controllo degli accessi ai servizi applicativi della Banca è disciplinato dal contratto con il fornitore incaricato (CSE); l'accesso a tali servizi avviene mediante l'uso di user-id e password che consentono l'autenticazione esclusivamente ai soggetti che possiedono necessarie abilitazioni.
- Gestione degli incidenti e dei problemi di sicurezza informatica. L'analisi degli incidenti e dei problemi di sicurezza relativamente ai servizi applicativi è svolta dalla Banca con il supporto dell'*outsourcer* (CSE), che utilizza una struttura di gestione degli incidenti. Le regole interne adottate prevedono che il fornitore segnali l'incidente alla Banca per la risoluzione del problema secondo procedure

consolidate. In caso di malfunzionamenti viene generato un *incident report* che descrive l'anomalia riscontrata e le soluzioni intraprese.

- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi. Lo sviluppo e la manutenzione dei sistemi informativi centrali della Banca sono disciplinati all'interno del contratto stipulato con il fornitore incaricato (CSE).
  I rilasci di aggiornamenti di software applicativi sono condotti secondo un modello operativo standard che prevede attività e responsabilità ben definite. Gli aggiornamenti dei software di base e di quelli di gestione e controllo sono curati dall'*outsourcer*.
  Lo sviluppo dei sistemi informativi di Banca Sistema viene invece effettuato dall'ufficio IT secondo procedure, *workflow* autorizzativi e strumenti standard per tutti gli applicativi gestiti.
- Audit. Il Piano annuale di internal audit prevede delle verifiche periodiche sia di carattere tecnico sia organizzativo sulle politiche di sicurezza, sulle modalità di assegnazione e modifica degli accounts. Annualmente viene inoltre condotto un IT audit presso l'*outsourcer* (CSE) da una società di revisione esterna incaricata dalle banche "consorziate" sui sistemi informatici utilizzati. I risultati delle verifiche di audit sono regolarmente e tempestivamente condivisi con l'OdV.

Oltre ai principi generali sopra richiamati, la Banca ha adottato altri strumenti di *governance*, descritti nel Modello (Parte Generale), quali il sistema delle deleghe, i documenti sulla struttura organizzativa, le Policy, il Regolamento Interno e il Documento Programmatico sulla Sicurezza.

# 4 Compiti dell'Organismo di Vigilanza

Con riferimento ai reati previsti nella presente Parte Speciale questi sono monitorati mediante specifici IT audit condotti periodicamente dalla Direzione Internal Audit della Banca sui sistemi informativi interni. Le verifiche dei processi IT forniti dall'*outsourcer* (CSE) dei sistemi gestionali della Banca sono effettuati

annualmente tramite una società di consulenza esterna incaricata dalle banche che utilizzano il provider e i cui risultati vengono condivisi con gli stessi aderenti.

# F) REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

## 1 Reati in materia di salute e sicurezza sul lavoro

I reati in materia di salute e sicurezza sul lavoro che possono dare origine ad una responsabilità amministrativa dell'Ente *ex* art. 25-*septies*[18] del D.Lgs. n. 231/2001 sono i seguenti:

- **Omicidio Colposo (art. 589 c.p.)**

"Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da 6 mesi a 5 anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da 1 a 5 anni. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni 12."

Sanzioni pecuniarie *ex* D.Lgs. n. 231/01: in relazione al delitto disciplinato dal primo comma dell'art. 25-*septies* del Decreto, la sanzione pecuniaria è pari a 1000 quote. In relazione al delitto di cui al secondo comma dell'art. 25-*septies* del Decreto, la sanzione pecuniaria è non inferiore a 250 quote e non superiore a 500 quote.

Sanzioni interdittive *ex* D.Lgs. n. 231/01: a) interdizione dall'esercizio dell'attività; b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi. Per il delitto di cui al primo comma, per un periodo massimo di un anno. Per il delitto di cui al secondo comma, per un periodo non inferiore a tre mesi e non superiore ad un anno.

- **Lesioni personali colpose (art. 590 c.p., comma 3)**

[18] Articolo aggiunto dalla Legge 3 agosto 2007, n. 123, art. 9 e modificato dal D.Lgs. n. 81/08.

"[…] Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da Euro 500 a Euro 2.000 e la pena per lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme di circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'art. 186, comma 2, lettera c) del D.Lgs. 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanza stupefacenti o psicotrope la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei messi a quattro anni".

Sanzioni pecuniarie *ex* D.Lgs. n. 231/01: non superiore a 250 quote.

Sanzioni interdittive *ex* D.Lgs. n. 231/01: a) interdizione dall'esercizio dell'attività; b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) divieto di pubblicizzare beni o servizi per un periodo massimo di sei mesi.

# 2 Aree a rischio reato

Le Linee Guida di Confindustria nell'ambito dei reati trattati nella presente Parte Speciale evidenziano l'impossibilità di escludere a priori alcun ambito di attività della società, in quanto i reati in esame potrebbero riguardare tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Ne consegue che le potenziali aree a rischio reato che la Banca ha individuato nell'ambito di tali reati riguardano tutte le attività svolte da Banca Sistema, nonché quelle svolte dal personale esterno (ad es. fornitori di servizi in base a contratti d'appalto, d'opera o somministrazione). Particolare attenzione deve essere dedicata a quelle attività realizzate in associazione con partner o tramite la stipula

di contratti di somministrazione, appalto o con società di consulenza o liberi professionisti.

Anche ai fini della redazione della presente Parte Speciale si devono pertanto considerare i fattori riportati nel "Documento di Valutazione dei Rischi" (di seguito anche "DVR"), tenuto conto che gli stessi non esauriscono le procedure di seguito previste, finalizzate a costituire il complessivo sistema di gestione della sicurezza sul lavoro e dare attuazione al disposto dell'art. 30 D.Lgs. n. 81/2008 secondo i principi espressi dalle Linee Guida UNI – INAIL e dal British Standard OHSAS 18001.

# 3 Regole di comportamento

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso in una delle aree sensibili su indicate, si ritiene particolarmente importante:

a) che il Consiglio di Amministrazione, su indicazioni del RSPP e di concerto con l'OdV, determini le politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Banca per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;

b) che il Consiglio di Amministrazione, su indicazioni del RSPP e di concerto con l'OdV, identifichi e applichi in modo corretto gli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici e tutte le prescrizioni delle leggi e dei regolamenti applicabili in tema di salute e sicurezza sul lavoro;

c) che il Consiglio di Amministrazione, su indicazioni del RSPP e di concerto con l'OdV, identifichi e valuti i rischi per tutte le categorie di lavoratori, con particolare riferimento alla redazione:

- del DVR;
- dei contratti di appalto;
- della valutazione dei rischi derivanti dalle interferenze (DUVRI);
- nel caso in cui la Banca sia costruttrice, dei Piani di Sicurezza e Coordinamento, Fascicolo dell'Opera e Piani Operativi di Sicurezza;

d) che vengano rispettate tutte le misure per la tutela della salute e per la sicurezza dei lavoratori previste per la costruzione di cantieri temporanei o mobili, ovvero qualunque luogo in cui si effettuano lavori edili o di ingegneria civile;

e) che il Consiglio di Amministrazione, su indicazioni del RSPP e di concerto con l'OdV, fissi gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elabori dei programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:

- attribuzioni di compiti e doveri;
- attività del Servizio Prevenzione e Protezione e del Medico Competente;
- attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori;

f) che l'OdV sensibilizzi la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:

- monitoraggio, periodicità, fruizione e apprendimento;
- formazione differenziata per soggetti esposti a rischi specifici;

g) che l'OdV attui adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:

- misure di mantenimento e miglioramento;
- gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
- coerenza tra attività svolta e competenze possedute;

h) che il Consiglio di Amministrazione, su indicazioni del RSPP e di concerto con l'OdV, attui le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei lavoratori così come individuati dall'art. 15 del Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del suddetto decreto si prevede quanto segue.

- Politiche aziendali in tema di sicurezza

La politica per la sicurezza e salute sul lavoro adottata dalla Banca deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Banca, intrattengono rapporti con la stessa.

Tale politica deve essere applicata a tutte le attività svolte da Banca Sistema e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Banca, nell'ottica della salute e sicurezza di tutti i lavoratori.

Tale politica, formata secondo gli standard UNI-INAIL, contiene:

- una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal datore di lavoro al singolo lavoratore nella gestione del sistema di salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- l'impegno a considerare il sistema di salute e sicurezza come parte integrante della gestione aziendale, la cui conoscibilità deve essere garantita ai Destinatari;
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a garantire che i Destinatari nei limiti delle rispettive attribuzioni, siano sensibilizzati e formati per svolgere i propri compiti nel rispetto

delle norme sulla tutela della salute e sicurezza e ad assumere le proprie responsabilità in materia di SSL;

- l'impegno al coinvolgimento ed alla consultazione dei lavoratori, anche attraverso il RLS; in particolare, Banca Sistema definisce modalità adeguate per il coinvolgimento dei lavoratori, anche attraverso il RLS, per attuare la consultazione preventiva in merito all'individuazione e valutazione dei rischi e alla definizione delle misure preventive nonché riunioni periodiche con gli stessi;
- l'impegno ad un riesame periodico della politica per la salute e sicurezza adottato e del relativo sistema di gestione attuato al fine di garantire la loro costante adeguatezza alla struttura organizzativa di Banca Sistema, nonché alla normativa, anche di natura regolamentare, vigente in materia;
- l'impegno a definire e diffondere all'interno della Banca gli obiettivi di Salute e Sicurezza sul Lavoro ed i relativi programmi di attuazione.

La politica è riesaminata annualmente in base ai risultati del monitoraggio del sistema.

Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.

- Processo di pianificazione

La Banca, nell'ambito del processo di pianificazione degli obiettivi in tema di salute e sicurezza:

- definisce gli obiettivi finalizzati al mantenimento e/o miglioramento del sistema;
- determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi;
- predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità;
- definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi

attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse;

- prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.

- **Informazione, formazione e documentazione**

Informazione

L'informazione che la Banca riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

a. le conseguenze derivanti dallo svolgimento della propria attività non conformemente al sistema di SSL adottato dalla Banca;
b. il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di SSL e altra prescrizione relativa al sistema di SSL adottato dalla Banca, nonché ai principi indicati nella presente Parte Speciale.

Ciò premesso, la Banca, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto il Personale, è tenuta ai seguenti oneri informativi:

- la Banca deve fornire adeguata informazione ai Dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- deve essere data evidenza dell'informativa erogata per la gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;
- i dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) devono ricevere informazione sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;

- deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Dipendenti;
- il RSPP e/o il medico competente devono essere coinvolti nella definizione delle informazioni;
- la Banca deve organizzare periodici incontri tra le funzioni preposte alla sicurezza sul lavoro;
- la Banca deve coinvolgere il RLS nella organizzazione della attività di rilevazione e valutazione dei rischi, nella designazione degli addetti alla attività di prevenzione incendi, pronto soccorso ed evacuazione.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

Formazione

- La Banca deve fornire adeguata formazione a tutti i dipendenti in materia di sicurezza sul lavoro;
- il RSPP e/o il medico competente debbono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai rischi della mansione cui il lavoratore è in concreto assegnato;
- deve essere predisposto uno specifico piano di formazione per i lavoratori esposti a rischi gravi ed immediati;
- i lavoratori che cambiano mansione e quelli trasferiti devono fruire di formazione preventiva, aggiuntiva e specifica nonché essere preventivamente ritenuti idonei dal medico competente in caso di lavorazioni che presentino specifici rischi;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso) devono ricevere specifica formazione;
- la Banca deve effettuare periodiche esercitazioni di evacuazione di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Banca deve garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i lavoratori.
Pertanto, la Banca adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

- dal basso verso l'alto: è garantito dalla Banca mettendo a disposizione apposite schede di segnalazione attraverso la compilazione delle quali ciascuno dei lavoratori ha la possibilità di portare a conoscenza del proprio superiore gerarchico osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della SSL;
- dall'alto verso il basso: ha lo scopo di diffondere a tutti i lavoratori la conoscenza del sistema adottato dalla Banca per la gestione della SSL.

A tale scopo la Banca garantisce agli esponenti aziendali un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici.

<u>Documentazione</u>
La Banca dovrà provvedere alla conservazione, su supporto cartaceo oppure informatico, dei seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita e aggiornata dal medico competente e custodita dal datore di lavoro;
- il registro degli infortuni;
- il Documento di Valutazione dei Rischi che indica la metodologia con la quale si è proceduto alla valutazione dei rischi e contiene il programma delle misure di mantenimento e di miglioramento.

La Banca è altresì chiamata a garantire che:

- il RSPP, il medico competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;

- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal medico competente;
- venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- venga conservata la documentazione inerente a regolamenti ed accordi aziendali;
- vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori;
- qualora siano implementate delle procedure per la gestione della salute e sicurezza sui luoghi di lavoro, siano conservate o su supporto cartaceo oppure informatico;
- tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'OdV.
-

➢ **Attività di monitoraggio**

La Banca deve assicurare un costante ed efficace monitoraggio del sistema per la gestione della salute e della sicurezza sui luoghi di lavoro.

A tale scopo:

- assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione;
- compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere.

Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta la Banca, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione.

# 4 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'OdV:

a. effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei reati di cui all'art. 25-*septies* del Decreto. A questo proposito, l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti della Banca eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la tutela della salute e della sicurezza nei luoghi di lavoro, in coerenza con quanto stabilito nel presente Modello e all'art. 30 del Decreto Sicurezza;
c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'OdV può:

- partecipare agli incontri organizzati dalla Banca tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

La Banca garantisce, a favore dell'OdV, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni,

delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

Nell'espletamento delle attività di cui sopra, l'OdV può avvalersi di tutte le risorse competenti della Banca.

Si sottolinea infine che Banca Sistema, con il supporto di una società di consulenza specializzata, ha redatto il Documento Programmatico a seguito di valutazione del rischio e quindi, se integralmente applicato, può costituire (*ex* art. 30 del D.Lgs. n. 81/08 e s.m.i.) la base di un modello organizzativo e gestionale idoneo ad avere efficacia esimente delle responsabilità amministrative per l'Ente, ai sensi del D.Lgs. n. 231/01 e s.m.i., a condizione che sia stato redatto il Codice Etico, nominato l'Organismo di Vigilanza con il suo Regolamento e relativi strumenti disciplinari.