



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
DELLA BANCA POPOLARE DI MILANO
EX DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231**

INDICE

DEFINIZIONI	4
INTRODUZIONE	5
I Il Decreto Legislativo n. 231/01 e la normativa di riferimento	5
II Presupposti di esclusione della responsabilità dell'ente	6
III Linee Guida di Gruppo	7
1. RILEVAZIONE DELLE AREE DI RISCHIO	8
1.1 Aree di rischio concernenti i rapporti con la Pubblica Amministrazione	8
1.2 Aree di rischio concernenti reati informatici e trattamento illecito di dati	10
1.3 Aree di rischio concernenti le falsità in monete, carte di pubblico credito e valori in bollo	11
1.4 Aree di rischio concernenti i reati societari	12
1.5 Aree di rischio concernenti i reati e gli illeciti amministrativi di <i>Market Abuse</i>	13
1.6 Aree di rischio concernenti reati aventi finalità di terrorismo o di eversione dell'ordine democratico	14
1.7 Aree di rischio concernenti i reati contro la personalità individuale	15
1.8 Aree di rischio concernenti i reati di criminalità organizzata	16
1.9 Aree di rischio concernenti i reati transnazionali	16
1.10 Aree di rischio concernenti i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	17
1.11 Aree di rischio concernenti i reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro	18
1.12 Aree di rischio concernenti pratiche di mutilazione degli organi genitali femminili	19
1.13 Aree di rischio concernenti la violazione del divieto di abbandono e deposito incontrollati di rifiuti sul suolo, nel suolo e nelle acque	19
1.14 Aree di rischio concernenti i reati contro l'industria e il commercio e i reati di falsità in strumenti o segni di riconoscimento.	19
1.15 Aree di rischio concernenti i reati in materia di violazione del diritto d'autore	21
1.16 Aree di rischio concernenti il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	22
2. REGOLE GENERALI (O <i>STANDARD</i>) DI CONTROLLO	23
2.1 Controlli preventivi di tutte le tipologie di reati ai sensi del Decreto	24
2.2 Controlli specifici per le singole tipologie di reati	25
2.2.1 Controlli preventivi dei reati contro la Pubblica Amministrazione	25
2.2.2 Controlli preventivi dei reati informatici e del trattamento illecito di dati	28
2.2.3 Controlli preventivi dei reati concernenti le falsità in monete, carte di pubblico credito e valori in bollo	29
2.2.4 Controlli preventivi dei reati societari	29
2.2.5 Controlli preventivi dei reati ed illeciti amministrativi di <i>Market Abuse</i>	35
2.2.6 Controlli preventivi dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico. ...	38
2.2.7 Controlli preventivi dei delitti contro la personalità individuale	39
2.2.8 Controlli preventivi dei reati di criminalità organizzata	39
2.2.9 Controlli preventivi dei reati transnazionali	41
2.2.10 Controlli preventivi dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	41
2.2.11 Controlli preventivi dei reati di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro	42
2.2.12 Controlli preventivi dei reati contro l'Industria e il Commercio e dei reati di falsità in strumenti e segni di riconoscimento	42
2.2.13 Controlli preventivi dei reati in materia di violazione del diritto d'autore	43
2.2.14 Controlli preventivi dei reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	43
3. NORMATIVA E DOCUMENTAZIONE AZIENDALE DI RIFERIMENTO	44
4. SISTEMA DISCIPLINARE	45
4.1 Principi generali	45
4.2 Sanzionabilità del tentativo	45
4.3 Sanzioni per i Dipendenti	45
4.4 Sanzioni per i soggetti in posizione apicale	47
4.5 Misure nei confronti degli Amministratori	48
4.6 Misure nei confronti dei Sindaci	48
4.7 Misure nei confronti dei Collaboratori Esterni	48
5. FORMAZIONE	49

5.1	Dirigenti (grado di Direttore Addetto alla Direzione Centrale o superiore)	49
5.2	Altro Personale.....	49
5.3	Collaboratori Esterni	50
ALLEGATI	51

DEFINIZIONI

- **Aree a Rischio:** le aree di attività della Banca nel cui ambito risulta profilarsi, in termini più concreti, il rischio di commissione dei reati e degli illeciti ai sensi del D.Lgs. 231/01.
- **BPM o Banca o la Società:** Banca Popolare di Milano.
- **CCNL:** i Contratti Collettivi Nazionali di Lavoro applicati dalla Banca.
- **Cod.civ.:** codice civile.
- **Codice Etico:** il codice etico adottato dalla Banca e approvato dal Consiglio di Amministrazione in data 13 gennaio 2004 e relativi aggiornamenti.
- **C.P. o cod. pen.:** Codice Penale.
- **Collaboratori Esterni:** tutti i collaboratori esterni complessivamente considerati, vale a dire i Consulenti, i Partner e i Fornitori.
- **Consulenti:** i soggetti che agiscono in nome e/o per conto della Banca in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione professionale.
- **Decreto o D.Lgs. 231/2001:** il Decreto Legislativo 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" e successive modifiche e integrazioni.
- **Decreto Antiriciclaggio:** il D.Lgs. 21 novembre 2007 n. 231 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e successive modifiche e integrazioni.
- **Dipendenti:** i soggetti aventi un rapporto di lavoro subordinato con la Banca, ivi compresi i dirigenti.
- **Fornitori:** i fornitori di beni e servizi non professionali della Banca che non rientrano nella definizione di Partner.
- **Gruppo:** le Società del Gruppo Bipiemme
- **Modello:** il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001.
- **OGI:** Ordinamento Generale d'Istituto.
- **Partner o Partner Commerciali:** le controparti contrattuali con le quali la Banca addivenga ad una qualche forma di collaborazione contrattualmente regolata (ad esempio, *joint venture*, licenza, agenzia, collaborazione in genere), ove destinate a cooperare con la Banca nell'ambito delle Aree a Rischio.
- **Repository:** sistema informativo all'interno del quale sono rappresentati i processi organizzativi della Banca.
- **TUB:** il D.Lgs. 1° settembre 1993, n. 385 e successive modifiche e integrazioni (Testo Unico Bancario).
- **TUF:** il D.Lgs. 24 febbraio 1998, n. 58 e successive modifiche e integrazioni (Testo Unico della Finanza).

INTRODUZIONE

I Il Decreto Legislativo n. 231/01 e la normativa di riferimento

Il Decreto Legislativo 231 dell'8 giugno 2001 (il "Decreto") - emanato in esecuzione della delega di cui all'articolo 11 della legge 29 settembre 2000 n. 300, pubblicato nella Gazzetta Ufficiale del 19 giugno 2001 n. 140 -, reca le disposizioni normative concernenti la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica".

Esaminando nel dettaglio il contenuto del Decreto, l'articolo 5, 1° comma, sancisce la responsabilità della società qualora determinati reati siano stati commessi nel suo interesse o a suo vantaggio:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (ad esempio, Amministratori e Direttori Generali), nonché da persone che esercitano, anche di fatto, la gestione e il controllo della stessa;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla precedente lettera a) (ad esempio, Dipendenti non Dirigenti).

Pertanto, nel caso in cui venga commesso uno dei reati specificamente indicati, alla responsabilità penale della persona fisica che ha realizzato materialmente il fatto si aggiunge, se ed in quanto siano integrati tutti gli altri presupposti normativi, anche la responsabilità "amministrativa" dell'ente.

Sotto il profilo sanzionatorio, per tutti gli illeciti commessi è sempre prevista, a carico della persona giuridica, l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, di licenze o di concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

Quanto ai reati ai quali si applica la disciplina in esame, sono ad oggi contemplati:

(i) reati commessi nei rapporti con la Pubblica Amministrazione;

(ii) reati informatici e trattamento illecito di dati;

(iii) reati di falsità in monete, in carte di pubblico credito e in valori di bollo;

(iv) reati societari;

(v) reati e illeciti amministrativi di abusi di mercato;

(vi) reati con finalità di terrorismo o di eversione dell'ordine democratico;

(vii) reati contro la personalità individuale;

(viii) reati di criminalità organizzata;

(ix) reati transnazionali;

(x) reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;

(xi) reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;

(xii) pratiche di mutilazione degli organi genitali femminili;

(xiii) violazione del divieto di abbandono e deposito incontrollati di rifiuti sul suolo, nel suolo e nelle acque;

(xiv) reati contro l'industria e il commercio e reati di falsità in strumenti o segni di riconoscimento;

(xv) reati in materia di violazione del diritto d'autore;

(xvi) reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

II Presupposti di esclusione della responsabilità dell'ente

Il Decreto prevede, agli articoli 6 e 7, una forma di esonero dalla responsabilità, se l'ente prova di avere adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire la realizzazione dei reati.

Il suddetto Modello deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati;
- prevedere specifiche procedure formalizzate, dirette a programmare la formazione e l'attuazione delle decisioni della società in relazione ai Reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei Reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

E' altresì necessario che:

1. la società abbia provveduto all'istituzione di un organismo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei Modelli, nonché di curarne l'aggiornamento;
2. l'organismo di controllo non sia colpevole di omessa o insufficiente vigilanza in merito all'attuazione e all'osservanza del Modello;
3. la società abbia predisposto un sistema di verifica periodica e di eventuale aggiornamento del Modello;
4. l'autore del reato abbia agito eludendo fraudolentemente le disposizioni del Modello.

Lo stesso Decreto, nonché il relativo Regolamento di attuazione emanato con Decreto Ministeriale del 26 giugno 2003 n. 201, affermano inoltre che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria e comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sulla idoneità di detti codici di comportamento a prevenire i reati.

Nella predisposizione del presente Modello BPM si è ispirata alle Linee Guida dell'associazione di categoria cui appartiene (A.B.I.), quale strumento operativo e di indirizzo maggiormente confacente alla struttura organizzativa della Banca. Eventuali deviazioni rispetto alle indicazioni contenute nelle Linee Guida sono dovute ai necessari adattamenti funzionali alla struttura organizzativa di BPM e non debbono essere interpretate come inadempimento dello stesso né del Decreto.

III Linee Guida di Gruppo

Il Gruppo Bipiemme è un gruppo “integrato” o “strategico” caratterizzato dal comune disegno imprenditoriale pur nell’autonomia decisionale delle singole imprese che ne fanno parte, i cui organi decisionali sono svincolati da quelli della Capogruppo, addivenendo alle loro determinazioni senza necessità di autorizzazione da parte di quest’ultima.

La Banca Popolare di Milano, in qualità di capogruppo del Gruppo Bipiemme, svolge -come previsto dalle Istruzioni di Vigilanza impartite dalla Banca d’Italia - attività di vigilanza consolidata nei confronti delle Società facenti parte del gruppo medesimo.

A tali principi è ispirato il rapporto tra BPM e le società da essa controllate: gli stessi vengono applicati anche con riguardo alle attività volte a realizzare l’adeguamento della struttura organizzativa delle società alle nuove disposizioni di legge in tema di responsabilità amministrativa degli enti.

In tale contesto, la responsabilità, la predisposizione ed il successivo aggiornamento del Modello organizzativo e di gestione, sono demandati alle singole Società; BPM, in qualità di Capogruppo ed al fine di armonizzare la conoscenza all’interno del Gruppo, si limita a fornire alle società del gruppo informative generali sul contenuto del Decreto, analisi propedeutiche alla predisposizione del Modello organizzativo e di gestione, comunicazioni sulle scelte che, conseguentemente ad esso, la Capogruppo medesima ha effettuato/effettuerà al proprio interno.

Ciascuna Società potrà ricorrere alla capogruppo per l’effettuazione di verifiche - di carattere specialistico - sul funzionamento del Modello organizzativo adottato.

La Capogruppo ha facoltà, qualora ne ravvisasse l’esigenza, di avanzare proposte, non vincolanti, alle società controllate in merito all’aggiornamento del Modello organizzativo e di assumere iniziative finalizzate al coordinamento delle attività di verifica e controllo.

Sulla base del suindicato principio di autonomia, ogni società del Gruppo dovrà istituire un proprio Organismo di Vigilanza ai sensi del Decreto, dotato di risorse adeguate e che operi in autonomia ed indipendenza rispetto a quello delle altre Società.

1. RILEVAZIONE DELLE AREE DI RISCHIO

La BPM ha svolto al proprio interno un'analisi al fine di individuare le aree di attività nelle quali possa riscontrarsi in via astratta un rischio di realizzazione di taluna delle fattispecie criminose rilevanti ai sensi del Decreto.

Per la rilevazione delle Aree di Rischio BPM si avvale anche di un *Repository* aziendale (gestito dalla funzione organizzativa) nel quale sono presenti i processi aziendali.

Il *Repository* è monitorato, alimentato ed aggiornato alla luce di nuove normative (o di modifiche e/o integrazioni di quelle esistenti) sia esterne che interne e/o di modifiche organizzative e/o degli sviluppi di attività progettuali connessi ad obiettivi di efficienza di processo.

1.1 Aree di rischio concernenti i rapporti con la Pubblica Amministrazione

Per quanto concerne i rapporti con la Pubblica Amministrazione, si provvede di seguito ad elencare i relativi reati indicati negli artt. 24 e 25 del Decreto.

- Malversazione a danno dello Stato (art. 316-*bis* cod. pen.)
- Indebita percezione di erogazioni in danno dello Stato (art. 316-*ter* cod. pen.)
- Concussione (art. 317 cod. pen.)
- Corruzione per un atto d'ufficio (art. 318 cod. pen.)
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319 cod. pen.)
- Corruzione in atti giudiziari (art. 319-*ter* cod. pen.)
- Corruzione di persona incaricata di un pubblico servizio (art. 320 cod. pen.)
- Pene per il corruttore (art. 321 cod. pen.)
- Istigazione alla corruzione (art. 322 cod. pen.)
- Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-*bis* cod. pen.)
- Truffa (art. 640, co.2, n. 1, cod. pen.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* cod. pen.)
- Frode informatica (art. 640-*ter* cod. pen.)

Ai fini del presente Modello, per Pubblica Amministrazione si deve intendere, oltre a qualsiasi ente pubblico, altresì qualsiasi agenzia amministrativa indipendente, persona, fisica o giuridica, che agisce in qualità di pubblico ufficiale o incaricato di pubblico servizio ovvero in qualità di membro di organo delle Comunità europee o di funzionario delle Comunità europee o di funzionario di Stato estero.

Sempre ai sensi del presente Modello, nella definizione di ente pubblico sono compresi quei soggetti privati che, per ragioni preminenti di ordine politico-economico, adempiono ad una funzione pubblicistica posta a presidio della tutela di interessi generali, come gli enti gestori dei mercati regolamentati.

In relazione ai reati contro la Pubblica Amministrazione, le aree ritenute più a rischio sono:

- la gestione della tesoreria di enti pubblici e, in genere, di fondi pubblici, sia sotto forma di captazione o erogazione di contributi (in qualsiasi modo denominati) destinati a pubbliche finalità, sia nello svolgimento di attività in regime di concessione (ad esempio, riscossione di tributi);
- il processo per la concessione del credito, con riguardo alle fasi di analisi/istruttoria e di delibera, laddove interessino pratiche nascenti da domande di finanziamento avanzate da enti pubblici ovvero da soggetti operanti all'interno di questi e la concessione di finanziamenti agevolati (ovverosia di quei finanziamenti che godono di agevolazioni concesse da parte di enti pubblici al ricorrere di determinate condizioni);
- la partecipazione a procedure pubbliche di gara e, in genere, a procedure competitive per l'aggiudicazione di concessioni da parte di enti pubblici ovvero la partecipazione a trattative private con tali enti al medesimo fine nonché allo scopo di pervenire al perfezionamento con essi di convenzioni di sponsorizzazione;
- la concessione di condizioni economiche in deroga, laddove si assumano delibere in favore di soggetti rappresentanti di enti pubblici o comunque operanti all'interno dei medesimi;
- l'ottenimento di concessioni o di licenze nel settore edilizio e, in genere, immobiliare ovvero l'ottenimento di contributi pubblici (come quelli connessi alla partecipazione a corsi di formazione organizzati da enti pubblici) o di benefici (quali quelli di natura fiscale connessi ad assunzioni effettuate con contratti di formazione);
- la gestione del Centro Acquisti, con riguardo alle trattative che possono essere instaurate ed agli accordi che possono essere perfezionati con enti pubblici o con soggetti in essi operanti;
- la gestione delle pratiche aventi ad oggetto vicende che generano (o possono generare) contenziosi giudiziari;
- l'attività riferita ai rapporti con gli enti pubblici operanti nei settori tributario e previdenziale;
- le attività che comportano rapporti con Organi e/o Autorità di Vigilanza, quali la Banca d'Italia e la Consob;
- le attività di consulenza o collocamento presso enti pubblici relative a strumenti finanziari ad alto rischio (per esempio: strumenti finanziari derivati);
- le attività che comportano la gestione dei servizi informatici, in particolare aventi ad oggetto la realizzazione e/o la gestione di collegamenti telematici con enti pubblici ovvero la trasmissione a questi ultimi di dati su supporti informatici;
- le attività aventi ad oggetto l'assunzione di personale e/o la gestione di trattamenti previdenziali del personale;
- le attività riguardanti la gestione delle verifiche o delle ispezioni;

- le attività di gestione delle consulenze;
- le attività di gestione delle liberalità.

1.2 Aree di rischio concernenti reati informatici e trattamento illecito di dati

La Legge n. 48 del 18 marzo 2008, in particolare con l'articolo 7, introducendo nel D.Lgs. 231/01 l'art. 24-*bis*, ha esteso la responsabilità amministrativa dell'ente (al ricorrere di un vantaggio o di un interesse per quest'ultimo), alle seguenti fattispecie di reato:

- Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* C.P.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* C.P.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* C.P.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* C.P.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* C.P.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* C.P.)
- 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.)
- Danneggiamento di sistemi informatici o telematici (art. 635-*quater* C.P.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* C.P.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* C.P.).

Le ultime due disposizioni si aggiungono al preesistente art. 640-*ter* c.p. – Frode informatica –, che punisce la condotta di chi procura a sé o ad altri un ingiusto profitto con altrui danno alterando informazioni o programmi contenuti in un sistema informatico o telematico: articolo richiamato dal D.Lgs 231/01 tra i reati contro la pubblica amministrazione, qualora sia commesso in danno di quest'ultima.

- Documenti informatici (art. 491-*bis* C.P.)

Quest'ultima fattispecie ha ad oggetto falsità perpetrate attraverso documenti informatici, la cui realizzazione può avvenire esclusivamente (o, quanto meno, in via prevalente) nell'ambito dell'area della banca funzionalmente deputata a curare i sistemi informatici e di telecomunicazione e, comunque, presuppone una profonda conoscenza di tali sistemi.

Le condotte prese in esame rientrano nelle seguenti categorie:

- accesso abusivo (intenzionale e senza diritto) a tutto o a parte di un sistema informatico;

- attentato all'integrità di un sistema informatico o telematico o dei dati in esso contenuti (danneggiamento, cancellazione, deterioramento, alterazione o soppressione) effettuato intenzionalmente e senza autorizzazione;
- intercettazione intenzionale e illecita di comunicazioni informatiche o telematiche;
- uso intenzionale e senza autorizzazione (consistente nella produzione, vendita, ottenimento per l'uso, importazione, diffusione e in ogni altra forma di messa a disposizione) di dispositivi specialmente concepiti per consentire l'accesso a tutto o a parte di un sistema informatico (parole chiave, codici di accesso o strumenti analoghi) o che, comunque, possano favorire la commissione dei delitti sopraelencati;
- falsità riguardante un documento informatico pubblico o privato;
- frode realizzata da soggetto che presta servizi di certificazione di firma elettronica al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno.

Risulta, quindi, doversi considerare area di rischio in ordine al possibile verificarsi dei reati in esame quella competente a gestire sistemi informatici e di telecomunicazione.

La pena per taluni dei reati indicati risulta aggravata nel caso in cui il comportamento illecito sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o, comunque, di pubblica utilità.

1.3 Aree di rischio concernenti le falsità in monete, carte di pubblico credito e valori in bollo

I reati indicati nell'art. 25-*bis* del Decreto in tema di falsità in monete, carte di pubblico credito e valori di bollo, sono i seguenti:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 cod. pen.)
- Alterazione di monete (art. 454 cod. pen.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 cod. pen.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 cod. pen.)
- Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 cod. pen.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 cod. pen.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 cod. pen.)
- Uso di valori di bollo contraffatti o alterati (art. 464 cod. pen.)

L'art. 25-*bis* è stato in un secondo tempo integrato con il reato di falsità in strumenti o segni di riconoscimento. Quest'ultimo, peraltro, nel presente Modello viene trattato insieme con i reati contro l'industria e il commercio, in considerazione dell'affinità delle aree di rischio e degli standard di controllo.

Nell'attività di BPM, come nell'attività di ogni banca, rientra tipicamente il maneggio di monete, carte di pubblico credito e valori di bollo e la loro messa in circolazione.

Le aree interessate principalmente sono quelle relative:

- alle operazioni di sportello, in relazione alle operazioni effettuate per cassa;
- alle operazioni connesse all'alimentazione dell'apparecchiatura Bancomat;
- all'attività di custodia e gestione di valori nonché l'attività di recupero crediti, laddove vengano ricevuti pagamenti in denaro contante da parte dei debitori.

1.4 Aree di rischio concernenti i reati societari

Si provvede di seguito ad elencare i reati societari indicati all'art. 25-*ter* del Decreto.

- False comunicazioni sociali (art. 2621 cod. civ.)
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622, comma 1 e comma 3, cod. civ.)
- Falso in prospetto (art. 173-*bis* TUF)
- Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 174- *bis* TUF)
- Indebita restituzione dei conferimenti (art. 2626 cod. civ.)
- Illegale ripartizione degli utili o delle riserve (art. 2627 cod. civ.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 cod. civ.)
- Operazioni in pregiudizio dei creditori (art. 2629 cod. civ.)
- Omessa comunicazione del conflitto di interessi (art. 2629-*bis* cod. civ.)
- Formazione fittizia del capitale (art. 2632-*bis* cod. civ.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 cod. civ.)
- Impedito controllo (art. 2625, co. 2, cod. civ.)
- Illecita influenza sull'assemblea (art. 2636 cod. civ.)
- Aggiotaggio (art. 2637 cod. civ.)
- Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638, comma 1 e 2, cod. civ.)

In particolare, le funzioni maggiormente interessate dalle aree a rischio sono quelle relative a: (i) l'attività di relazione con Organi di Vigilanza o altre autorità garanti; (ii) la gestione della contabilità centrale; (iii) la gestione della finanza; (iv) la gestione degli affari societari; (v) la formazione di documenti contabili (in senso lato) e dei documenti che rappresentino situazioni economiche, finanziarie e patrimoniali della Banca; (vi) la rappresentazione e diffusione all'esterno delle informazioni relative alla situazione economica, patrimoniale e finanziaria della Banca; (vii) i servizi tributari; (viii) l'Internal Auditing; (ix) la gestione del centro acquisti; (x) la gestione del patrimonio immobiliare; (xi) l'amministrazione del credito (con riguardo alle determinazioni in tema di dubbi esiti e di passaggio a sofferenza); (xii) l'attività legale (sia con riguardo all'attività di recupero di crediti sia a quella di gestione di contenziosi e reclami in genere); (xiii) la gestione delle risorse umane (con riguardo alla gestione degli aspetti di natura amministrativa, fiscale e previdenziale nonché relativi alla pianificazione dei costi); (xiv) i rapporti con la società di revisione; (xv) le

attività in cui possono sorgere conflitti di interesse tra la Banca e i suoi esponenti: concessione del credito, compravendita e locazione di immobili, gestione delle condizioni economiche dei rapporti bancari, rapporti con consulenti e fornitori.

Particolarmente coinvolte nel rischio di realizzazione dei reati in esame sono le figure apicali, ovverosia coloro che rivestono funzioni di rappresentanza, deliberazione e amministrazione, controllo (soprattutto contabile) e direzione dell'ente.

1.5 Aree di rischio concernenti i reati e gli illeciti amministrativi di *Market Abuse*

Si provvede di seguito ad elencare i reati di abuso di mercato indicati all'art. 25-*sexies* del Decreto.

Detti reati e l'art. 25-*sexies* del Decreto sono stati introdotti dalla Legge n. 62 del 18 aprile 2005 – c.d."Legge Comunitaria 2004".

- Abuso di informazioni privilegiate (art. 184 TUF)
- Manipolazione del mercato (art. 185 TUF)

La Legge Comunitaria 2004 ha altresì introdotto le due fattispecie di illecito amministrativo di abuso di informazione privilegiata e di manipolazione del mercato che, pur avendo ad oggetto le medesime condotte delle fattispecie penali, sono tuttavia sanzionate al solo ricorrere della colpa (senza che sia richiesto l'elemento del dolo).

Le sanzioni pecuniarie previste per le suddette fattispecie di illecito amministrativo sono applicate sia al soggetto che ha materialmente commesso il fatto sia alla Banca, in virtù del rinvio effettuato dall'art. 187-*quinquies* TUF alle norme del Decreto in quanto applicabili.

Si provvede di seguito ad elencare gli illeciti di abuso di mercato.

- Abuso di informazioni privilegiate (art. 187-*bis* TUF)
- Manipolazione del mercato (art. 187-*ter* TUF)

I suddetti reati ed illeciti amministrativi, così come configurati dalla normativa in materia di *Market Abuse*, coinvolgono quelle funzioni che, all'interno della Banca, hanno la possibilità di accedere ad informazioni privilegiate - con ciò intendendosi (ai sensi dell'art. 181 TUF) quelle informazioni concernenti uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari che non sono state rese pubbliche e che, se rese pubbliche, potrebbero influire in modo sensibile sui prezzi di tali strumenti finanziari.¹

Oltre ad esse, rilevano anche le funzioni che svolgono attività di negoziazione o collocamento di strumenti finanziari.

¹ Talvolta il rischio di commissione di illeciti nell'interesse o a vantaggio dell'ente può sorgere dalla combinazione di ruoli e funzioni (cd. "cumulo di funzioni") che la banca svolge laddove ciò consenta di acquisire (e manipolare) informazioni trasversali su clienti, sull'ente stesso, su terzi.

Le Aree di Rischio interessate dai reati ed illeciti amministrativi di *Market Abuse* sono le seguenti:

- a) comunicazioni all'esterno (Borsa Italiana, Consob, analisti finanziari, azionisti, giornalisti, agenzie di rating, etc.);
- b) consulenza all'emissione o al classamento di strumenti finanziari;
- c) consulenza alla clientela in occasione del collocamento di strumenti finanziari;
- d) gestione di eventuali conflitti di interesse;
- e) identificazione delle operazioni sospette così come elencate in modo non esaustivo ed esemplificativo nella Comunicazione Consob DME5078692 del 29 novembre 2005;
- f) negoziazione e/o collocamento di strumenti finanziari;
- g) attività nel cui espletamento siano ricompresi rapporti diretti con le Autorità di Vigilanza o con il mercato, ivi compresi gli studi e le ricerche aventi ad oggetto emittenti o strumenti finanziari quotati, le attività di *trading* (per conto proprio o di terzi, ivi comprese le gestioni di patrimoni) e di *advisory* per operazioni di *corporate finance*.

1.6 Aree di rischio concernenti reati aventi finalità di terrorismo o di eversione dell'ordine democratico

Si provvede di seguito ad elencare i delitti con finalità di terrorismo o di eversione dell'ordine democratico indicati all'art. 25-*quater* del Decreto.

- Associazioni sovversive (art. 270 cod. pen.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordinamento democratico (art. 270-*bis* cod. pen.)
- Assistenza agli associati (art. 270-*ter* cod. pen.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-*quater* cod. pen.)
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies* cod. pen.)
- Condotte con finalità di terrorismo (art. 270-*sexies* cod. pen.)
- Attentato per finalità terroristiche o di eversione (art. 280 cod. pen.)
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280-*bis* cod. pen.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-*bis* cod. pen.)
- Istigazione a commettere alcuno dei delitti contro la personalità dello Stato (art. 302 cod. pen.)
- Cospirazione politica mediante accordo e cospirazione politica mediante associazione (artt. 304 e 305 cod. pen.)
- Banda armata e formazione e partecipazione e assistenza ai partecipi di cospirazione o di banda armata (artt. 306 e 307 cod. pen.)

- Reati diversi da quelli indicati nel Codice Penale e nelle leggi speciali, previsti dall'art. 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo di New York del 9 dicembre 1999.

I delitti innanzi elencati, così come configurati dalla normativa di legge in esame, coinvolgono quelle funzioni che, all'interno della Banca, hanno la possibilità, sulla base del contatto diretto che instaurano con la clientela e/o sulla base dell'esame di documentazione ad essa relativa ovvero dell'operatività da essa realizzata, di venire a conoscenza di circostanze tali da far insorgere dubbi in merito al possibile collegamento della clientela medesima con i delitti qui in considerazione.

Le funzioni interessate sono quelle che operano attraverso il contatto diretto con i clienti o, comunque, che hanno la possibilità di accedere all'esame dell'operatività da loro posta in essere e/o di documenti concernenti quest'ultima o, in genere, contenenti informazioni concernenti lo svolgimento della loro attività.² Conseguentemente le funzioni principalmente coinvolte possono essere individuate in quella commerciale e in quelle relative al processo di erogazione del credito.

1.7 Aree di rischio concernenti i reati contro la personalità individuale

L'articolo 25-*quinquies* del Decreto considera i delitti contro la personalità individuale, che qui di seguito vengono elencati:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-*bis* c.p.)
- Pornografia minorile (art. 600-*ter* c.p.)
- Detenzione di materiale pornografico (600-*quater* c.p.)
- Pornografia virtuale (art. 600-*quater*.1 cod. pen)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavi (art. 602 c.p.)

Anche per questa categoria di reati, come per quella dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, le funzioni aziendali che possono venire in considerazione in un'analisi dei rischi sono quelle che, attraverso il contatto diretto con la clientela e/o sulla base dell'esame di documentazione ad essa relativa o dell'operatività da essa realizzata, possono acquisire conoscenza di elementi dai quali sia desumibile un possibile collegamento della clientela medesima con taluno dei delitti qui in esame.

² La banca, infatti, per il tramite di propri operatori (che agiscano con finalità illecite o con la consapevolezza delle altrui finalità illecite), nella fisiologica attività di raccolta ed erogazione del credito, si potrebbe trovare ad instaurare rapporti con clienti che perseguono, direttamente o quali prestanome, finalità di terrorismo o eversione dell'ordine costituzionale, o che appaiono coinvolti in taluna delle attività illecite descritte nell'articolo 25-*quinquies*, così da agevolarli mettendo a loro disposizione risorse finanziarie o comunque incrementandone le disponibilità economiche, che risultino poi strumentali nel perseguimento dei loro criminosi obiettivi.

Trattasi, pertanto, principalmente della funzione commerciale, di quella che presidia la concessione del credito.

1.8 Aree di rischio concernenti i reati di criminalità organizzata

Con la definitiva approvazione, da parte del Senato, del disegno di legge S.733-B recante disposizioni in materia di sicurezza pubblica e convertito nella legge n.94/09, è stato introdotto nel D.Lgs. 231/01 l'art. 24-*ter*, che ha esteso la responsabilità amministrativa dell'ente, (al ricorrere di un vantaggio o di un interesse per quest'ultimo) anche alle seguenti fattispecie di reato:

- Associazione per delinquere (art. 416 c.p.)
- Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.)
- Scambio elettorale politico-mafioso (art. 416 *ter* c.p.)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Reati commessi avvalendosi delle condizioni previste dal predetto art. 416 – *bis*, ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 309/90)
- Reati concernenti l'illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra e parti di esse, di esplosivi, di armi clandestine, nonché di armi comuni da sparo (art. 407 comma 2 lettera a) c.p.p)

Per tutte le succitate tipologie di reato, le aree funzionali interessate appaiono tendenzialmente coincidenti con quelle che operano attraverso il contatto diretto con la clientela o che hanno, comunque, la possibilità di accedere ai contenuti dell'attività di quest'ultima.

Per questi reati, pertanto, le aree principalmente coinvolte possono essere individuate in quella commerciale ed in quella relativa al processo di erogazione del credito.

In particolare rientrano in tali aree di rischio:

- i servizi di apertura e gestione dei conti correnti, dei dossier titoli e di altri rapporti continuativi;
- i servizi di pagamento e incasso prestati dalle Agenzie della Banca;
- i servizi di pagamento e incasso di import/export sull'Estero;
- l'erogazione del credito attraverso l'analisi dei flussi finanziari aziendali

La pena per taluni dei reati indicati risulta aggravata nel caso in cui l'ente o una sua unità organizzativa venga stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati stessi.

1.9 Aree di rischio concernenti i reati transnazionali

La normativa contro il crimine organizzato transnazionale (legge 16 marzo 2006 n. 146) prevede che, a seguito del compimento dei reati di seguito descritti, l'ente

possa essere ritenuto amministrativamente responsabile e, quindi, passibile di sanzioni.

Tali reati transnazionali sono:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-*bis* c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* del Testo Unico di cui al Presidente della Repubblica del 23 gennaio 1973 n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico del Presidente della Repubblica del 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-*bis*, 3-*ter* e 5, del Testo Unico di cui al D.Lgs. 25 luglio 1998, n. 286 e successive integrazioni e modifiche);
- Favoreggiamento personale (art. 378 c.p.).

Peraltro, ognuna di tali fattispecie viene considerata “reato transnazionale”, a norma dell’art. 3 della Legge 16 marzo 2006 n. 146 ove si tratti di « *reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:*

- a) sia commesso in più di uno Stato;*
- b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;*
- c) ovvero sia commesso in uno Stato ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;*
- d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.»*

Per tutte le succitate tipologie di reato, le aree funzionali interessate appaiono sostanzialmente coincidenti con quelle di cui al precedente punto 1.8 relativo ai reati di criminalità organizzata, ovverosia le aree che operano attraverso il contatto diretto con la clientela o che hanno, comunque, la possibilità di accedere ai contenuti dell’attività di quest’ultima. Infatti, la differenza tra le due diverse categorie di reato considerate dal Decreto consiste non tanto nella tipologia dei reati che le compongono, quanto nell’esistenza o meno del requisito della transnazionalità (come innanzi definito).

Per quanto concerne il reato di Favoreggiamento personale (art. 378 c.p.), l’area di rischio nella quale può essere commesso appare essere quella relativa alla gestione delle pratiche aventi ad oggetto vicende che generano (o possono generare) contenziosi giudiziari.

1.10 Aree di rischio concernenti i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Il D.Lgs. 21 novembre 2007, n. 231 (c.d. “Decreto Antiriciclaggio”), attuativo della III Direttiva Antiriciclaggio, ha introdotto nel D.Lgs. 231/2001 l’art. 25-*octies* che disciplina le seguenti fattispecie di reato:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-*bis* c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.).

I reati di Riciclaggio e di Impiego di denaro, beni o utilità di provenienza illecita, precedentemente contemplati dalla legge 16 marzo 2006 n. 146 contro il crimine organizzato di carattere “transnazionale”, vengono, con l'entrata in vigore del Decreto Antiriciclaggio, inseriti nel *corpus* del Decreto Antiriciclaggio stesso (con l'aggiunta del reato di ricettazione), andando a coinvolgere in tal modo la responsabilità amministrativa dell'ente anche in conseguenza di condotte poste in essere all'interno del territorio dello Stato e con effetti rilevanti nell'ambito dello stesso.

Anche per tali reati innanzi elencati, le aree funzionali interessate appaiono essere quelle che operano attraverso il diretto contatto con la clientela ovvero che hanno la possibilità di esaminare documentazione ad essa relativa o, comunque, di accedere a informazioni concernenti la sua attività.

Trattasi, pertanto, principalmente della funzione commerciale e di quella deputata alla concessione del credito. Appare coinvolta anche la funzione finanziaria in relazione al reato di impiego di denaro, beni o utilità di provenienza illecita.

In particolare, rientrano in tale aree di rischio:

- i servizi di apertura e gestione dei conti correnti, dei dossier titoli e di altri rapporti continuativi;
- i servizi di pagamento e incasso prestati dalle Agenzie della Banca;
- i servizi di pagamento e incasso di import/export sull'Estero;
- l'erogazione del credito attraverso l'analisi dei flussi finanziari aziendali;
- l'attività finanziaria (sottoscrizione, compravendita e trasferimento di strumenti finanziari);
- le attività amministrative relative all'attuazione degli adempimenti di registrazione, segnalazione, comunicazione di operazioni bancarie;
- l'attività del Centro Acquisti (con particolare riguardo al reato di ricettazione).

Vengono, inoltre, in considerazione tutte le attività bancarie che siano o possano essere caratterizzate dal maneggio di denaro contante, quali:

- prelievo e versamento;
- pagamento di utenze, bonifici o rate di mutuo;
- cambio assegni.

1.11 Aree di rischio concernenti i reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro

La legge delega n. 123/2007 in materia di “Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa”, ha avviato una riforma sulla sicurezza del lavoro, attuata poi attraverso il D.Lgs. n. 81/2008. Tale provvedimento ha introdotto nel D.Lgs. 231/01 l'art. 25-*septies*, che ha esteso la responsabilità amministrativa dell'ente a due nuove fattispecie di reato:

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose gravi o gravissime (art. 590 c.p.).

Tale responsabilità, peraltro, è subordinata alla condizione che tali reati si realizzino in conseguenza della violazione delle norme poste a tutela della salute e della sicurezza sul lavoro.

Le aree funzionali aziendali che appaiono coinvolte in attività potenzialmente connesse a rischi di tal natura sono quelle che intervengono nella gestione sia dei luoghi e degli spazi in cui si svolge l'attività lavorativa sia dei mezzi e degli strumenti materiali in essa adoperati.

Tale intervento può avere diversa natura:

- a) Progettazione dei lavori e/o definizione e trasmissione di direttive per l'esecuzione dei lavori (a titolo di esempio: istruttoria e valutazione per la realizzazione di una nuova dipendenza; gestione di variazioni nell'assegnazione di spazi all'interno delle agenzie o degli uffici)
- b) Realizzazione dei lavori e manutenzione (ad esempio: esecuzione degli interventi ritenuti necessari a seguito di sopralluoghi negli ambienti di lavoro)
- c) Vigilanza e supervisione (ad esempio: sopralluoghi per l'analisi della sicurezza nei luoghi di lavoro; verifiche su impianti e collaudi).

1.12 Aree di rischio concernenti pratiche di mutilazione degli organi genitali femminili

Con riferimento alla fattispecie di cui all'art. 583 c.p. (Pratiche di mutilazione degli organi genitali femminili), oggi richiamata dall'art. 25-*quater*.1 del Decreto, non si ravvisano aree funzionali della Banca che svolgano attività che presentino profili di rischio ad essa connessi, apparendo doversi escludere l'ipotesi che la Banca possa essere asservita al perseguimento di finalità illecite quali quelle qui in considerazione.

1.13 Aree di rischio concernenti la violazione del divieto di abbandono e deposito incontrollati di rifiuti sul suolo, nel suolo e nelle acque

Con riferimento alla fattispecie di cui agli articoli 192 e 255 del D.Lgs. 3 aprile 2006, n. 152, non si ravvisano aree di rischio per la Banca, in quanto per lo svolgimento delle attività di raccolta, trasporto, avvio al recupero e/o smaltimento dei rifiuti speciali prodotti presso BPM è stato stipulato un apposito contratto di appalto tra quest'ultima e una società esterna.

Il rapporto tra di esse è regolato dalle norme civilistiche in tema di contratto di appalto, che, fra l'altro, sanciscono (art. 1655 Cod. civ.) che l'appaltatore opera "con gestione a proprio rischio".

Inoltre, nel contratto medesimo, una volta identificati i rischi connessi all'attività oggetto dell'accordo, li si pone a carico della società appaltatrice (con esonero della responsabilità del committente), che è tenuta ad adottare tutte le misure idonee a prevenirli (alcune delle quali sono elencate nel contratto stesso).

1.14 Aree di rischio concernenti i reati contro l'industria e il commercio e i reati di falsità in strumenti o segni di riconoscimento.

Con la definitiva approvazione, da parte del Senato, della legge 23 luglio 2009 n.99 è stato integrato l'art.25 *bis* del D.Lgs. 231/01, e introdotto l'art.25 *bis* 1, si da estendere la responsabilità amministrativa dell'ente, (al ricorrere di un vantaggio o di un interesse per quest'ultimo) anche alle seguenti fattispecie di reato:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.)
- Frodi contro le industrie nazionali (art. 514 c.p.)
- Frode nell'esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.)
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.)

Per quanto riguarda le fattispecie di falso (artt. 473 e 474 c.p.), le norme tendono a tutelare la pubblica fede e l'affidamento dei consumatori nella provenienza e genuinità dei marchi, mentre in riferimento ai delitti contro l'industria e il commercio, il bene giuridico protetto è rappresentato dai principi del libero esercizio delle attività produttive (es. artt. 513 e 513-*bis* c.p.), e dell'onestà e correttezza degli scambi commerciali contro il pericolo di frodi nella circolazione dei prodotti (es. artt. 516 e 517 c.p.).

Tra i reati innanzi elencati taluni di essi non appaiono applicabili alla realtà bancaria, talora in quanto espressamente riferiti a specifici settori merceologici o ai soli beni mobili, in altri casi in quanto riferiti a comportamenti che facciano uso di violenza o minaccia.

Appaiono viceversa applicabili alla realtà bancaria le disposizioni sulla tutela dei segni distintivi e dei marchi (art. 473 e 474 c.p.), nonché la disposizione che sanziona l'uso di mezzi fraudolenti atti a turbare l'esercizio di un industria e di un commercio (art. 513 c.p.).

Le aree potenzialmente coinvolte risultano essere quelle che curano la creazione di prodotti, nonché le attività di *marketing* e comunicazione commerciale.

Le condotte prese in esame possono ricondursi ad attività che potrebbero:

- generare confusione utilizzando nomi o segni distintivi legittimamente usati da altri
- imitare servilmente le caratteristiche proprie del prodotto di un concorrente
- compiere, con qualsiasi altro mezzo, atti idonei a creare confusione con i prodotti e con l'attività di un concorrente;
- mediante l'attività di propaganda e comunicazione commerciale appropriarsi indebitamente dei pregi relativi ai prodotti o all'impresa di un concorrente;

- compiere qualsiasi atto volto a turbare il leale esercizio della concorrenza

1.15 Aree di rischio concernenti i reati in materia di violazione del diritto d'autore

La stessa legge n. 99 del 23 luglio 2009 ha introdotto nel perimetro applicativo del D.Lgs. 231/01 l'art. 25-*novies*, che ha esteso la responsabilità amministrativa dell'ente (al ricorrere di un vantaggio o di un interesse per quest'ultimo) anche alle fattispecie di reato contemplate dalla legge sul diritto d'autore n. 633/1941 agli articoli 171, primo comma lettera *a-bis*) e terzo comma (quest'ultimo non applicabile alla realtà bancaria), 171-*bis*, 171-*ter*, 171-*septies* e 171-*octies*.

Le disposizioni in esame riguardano:

- Messa a disposizione del pubblico, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, di un'opera dell'ingegno protetta, o parte di essa, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere (art. 171, primo comma, lett. *a-bis*) della L. n. 633/1941);
- Duplicazione, a scopo di lucro, importazione, distribuzione o vendita di programmi per elaboratore; concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), riproduzione, trasferimento, distribuzione, comunicazione non autorizzati del contenuto di una banca dati (art. 171-*bis*, della L. n. 633/1941);
- Duplicazione, riproduzione o trasmissione abusive di un'opera dell'ingegno anche tramite supporti contenenti videogrammi o fotogrammi senza contrassegno SIAE (art. 171-*ter*, della L. n. 633/1941);
- Duplicazione, riproduzione o trasmissione o diffusione abusive, oltre le 50 copie, di un'opera dell'ingegno tutelata dal diritto d'autore (art. 171-*ter*, comma 2, della L. n. 633/1941);
- Mancata comunicazione alla SIAE dei dati per l'identificazione dei supporti, non soggetti a contrassegno, da parte di produttori o importatori (art. 171-*septies* della L. n. 633/1941);
- Produzione, vendita, installazione e utilizzo fraudolento di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato (per un gruppo chiuso di utenti) effettuate via etere, via satellite e via cavo (art. 171-*octies*, della L. n. 633/1941);

Esse sono dirette a tutelare sia il diritto patrimoniale d'autore, inteso come diritto allo sfruttamento esclusivo a fini commerciali dell'opera dell'ingegno, sia il diritto morale del medesimo a preservare la paternità dell'opera, nonché tutti i diritti connessi all'esercizio del diritto d'autore.

Le suddette fattispecie sono state inserite dal legislatore nel perimetro del Decreto al fine di adeguare costantemente l'apparato normativo alla rapida evoluzione tecnologica.

In tal modo, è stata apprestata una forma di tutela diffusa a fronte di condotte illecite che riguardano tanto la messa a disposizione del pubblico, attraverso rete

telematica, di opere dell'ingegno protette, quanto la duplicazione e commercializzazione di *software* e banche dati su supporti non contrassegnati o, comunque la duplicazione (sia in formato cartaceo che elettronico) e l'utilizzo di opere dell'ingegno senza averne autorizzazione.

Pertanto la principale area operativa della Banca in cui è possibile intravedere rischi di violazione di tali disposizioni, appare essere quella funzionalmente deputata a curare i sistemi informatici e di telecomunicazione.

Con riguardo ad essa peraltro le relative condotte sono già state oggetto di esame al precedente paragrafo 1.2.

Oltre ad essa rileva altresì l'area avente ad oggetto le attività di Formazione rivolte ai dipendenti ed in genere a coloro che operano per conto della Banca.

1.16 Aree di rischio concernenti il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Un discorso a parte va fatto per il reato di:

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.).

Tale tipologia di reato era stata introdotta dapprima nelle fattispecie relative ai reati transnazionali ma, di recente, con l'art. 4 della legge 3 agosto 2009, n. 116 (Ratifica della Convenzione ONU del 31 ottobre 2003 contro la corruzione, firmata dallo Stato italiano il 9 dicembre 2003) è stata prevista, come fattispecie a sé stante, nell'articolo 25-*novies* del Decreto³.

L'area di rischio che può essere coinvolta nella commissione di tale reato appare essere quella relativa alla gestione delle pratiche aventi ad oggetto vicende che generano (o possono generare) contenziosi giudiziari (ordinari, giuslavoristici, tributari, ecc.).

³ Il Legislatore ha emanato, con due normative differenti per tipologia, argomenti, ambito e tempi, delle modifiche al D.Lgs. 231/01 dando a due articoli di diverso contenuto la stessa numerazione "25-*novies*".

2. REGOLE GENERALI (O STANDARD) DI CONTROLLO

Nella realizzazione delle attività che hanno condotto alla formulazione del presente Modello, BPM, dopo avere effettuato un attento esame dei reati considerati dal Decreto, ha proceduto ad individuare i principali controlli generali (definiti “ *standard* di controllo”) volti a presidiare il rischio di commissione dei reati medesimi.

Tali regole, peraltro, si affiancano ai principi etici (di carattere, ovviamente, più generale) cui devono conformarsi l’attività ed il comportamento di tutto il personale, nonché di tutti coloro che collaborano a qualsivoglia titolo con la Banca stessa: principi che sono contenuti nel “Codice Etico ” diffuso presso i Dipendenti, che costituisce parte integrante del presente Modello.

Gli approfondimenti di cui sopra sono stati svolti con riguardo alle diverse categorie di reato considerate dal Decreto.

Gli *standard* di controllo così individuati vengono a costituire il complesso di regole che costituisce il contenuto del Modello di organizzazione, gestione e controllo adottato da BPM.

Peraltro tali regole, nella loro generalità, risultano già da tempo adottate da BPM, essendo presenti nell’Ordinamento Generale d’Istituto allo stato vigente all’interno di quest’ultima, e formano, comunque, oggetto, laddove necessario, di costanti interventi d’implementazione.

L’Ordinamento Generale d’Istituto costituisce il documento in cui sono definiti l’assetto organizzativo, l’ordinamento funzionale e i regolamenti della Banca Popolare di Milano.

Per la pratica attuazione delle norme contenute in tale Ordinamento e per il corretto svolgimento delle attività valgono le istruzioni generali o particolari impartite nel tempo mediante testi unici, circolari, disposizioni operative e comunicazioni di servizio non in contrasto con le seguenti disposizioni, nonché la normativa vigente.

L’OGI è sottoposto a regolare aggiornamento e revisione al fine di garantire un corretto adeguamento alle normative emanate dal Legislatore in materia di normativa bancaria.

Attraverso l’Ordinamento Generale d’Istituto la Banca assicura il regolare svolgimento delle attività aziendali, orientando le proprie azioni e comportamenti ai principi di onestà, integrità, correttezza e trasparenza sui quali si fonda l’Ordinamento medesimo per un corretto perseguimento degli obiettivi aziendali.

Ciascun dipendente è tenuto a conoscere e rispettare tale Ordinamento.

Il Direttore Generale e i Responsabili di funzione hanno l’obbligo di segnalare agli organi preposti ad attività di controllo eventuali anomalie e situazioni che possono determinare rischi rilevanti per la Banca ed il Gruppo.

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, modifica l’Ordinamento su proposta del Direttore Generale.

La composizione dell’OGI e l’indicazione degli altri documenti che formano la normativa aziendale è riportata nel successivo capitolo 3.

2.1 Controlli preventivi di tutte le tipologie di reati ai sensi del Decreto

Con riguardo ai diversi reati previsti dal Decreto, BPM si è dotata di regole preventive (*standard* di controllo) così riassumibili:

- Normativa aziendale.

BPM si è da tempo dotata di un sistema di disposizioni aziendali (Testi Unici, circolari, nonché i regolamenti e i documenti costituenti il sopra menzionato Ordinamento Generale dell'Istituto) idoneo a fornire, a coloro che operano per conto della stessa, i principi di riferimento, sia generali sia specifici, per la regolamentazione delle attività svolte e al rispetto delle quali gli operatori medesimi sono tenuti: un sistema che, peraltro, è soggetto a continui aggiornamenti da parte di funzioni all'uopo specificamente dedicate. L'Ordinamento Generale d'Istituto è costituito da: Ordinamento Funzionale, Regolamento dei Comitati, Regolamenti disciplinanti le principali e più sensibili aree di attività bancaria.

Ad esso si affianca la normativa aziendale di contenuto più operativo (Testi Unici, disposizioni urgenti, ecc.).

Le normative interne contengono le specifiche degli *standard* di controllo di seguito elencati.

- Regole per l'esercizio dei poteri di firma e dei poteri autorizzativi.

L'esercizio dei poteri di firma e dei poteri autorizzativi è rigidamente regolamentato da disposizioni che, in modo specifico e dettagliato, individuano i soggetti ai quali, con riguardo ai diversi atti e alle diverse operatività, sono riconosciuti tali poteri nonché le modalità e le limitazioni con le quali essi devono essere esercitati (limiti d'importo riferiti all'operazione, diversi a seconda del grado ricoperto, e/o modalità di abbinamento di firme di diversi soggetti). Si vedano, in Ordinamento Generale d'Istituto: Poteri delegati (Poteri di Firma e Poteri di *Pricing*) e Regolamento Fidi.

- Segregazione delle attività.

Lo svolgimento delle diverse attività all'interno di BPM è regolamentato sulla base di una rigorosa separazione tra l'attività di chi esegue, l'attività di chi autorizza e quella di chi controlla.

- Tracciabilità dei processi.

L'operatività svolta all'interno di BPM è regolata da meccanismi che consentono l'individuazione delle attività svolte, degli autori, delle fonti e dei relativi elementi informativi.

2.2 Controlli specifici per le singole tipologie di reati

2.2.1 Controlli preventivi dei reati contro la Pubblica Amministrazione

Per la prevenzione dei reati contro la Pubblica Amministrazione BPM ha determinato di avvalersi, oltre che dei controlli di carattere generale innanzi esaminati, anche dei seguenti controlli di natura più specifica.

- Il controllo sui soggetti che gestiscono l'attività di riferimento. In ogni caso, devono rispettarsi i seguenti principi procedurali:

- a) obbligo di partecipazione di almeno due soggetti della Banca agli incontri con la P.A;
- b) obbligo di segnalazione della proposta di contratto con la PA del dipendente che segue la relativa negoziazione al responsabile della funzione aziendale;
- c) autorizzazione scritta alla stipula dell'atto o all'esecuzione di un'operazione rilasciata dalla funzione aziendale competente;
- d) tempestiva registrazione dell'operazione.

- Il divieto di accesso a risorse finanziarie in autonomia (anche solo per autorizzare disposizioni di pagamento) da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione. In ogni caso, viene quanto meno richiesto che sussista:

- a) autorizzazione scritta alla disposizione di pagamento, secondo quanto previsto dall'Ordinamento Generale d'Istituto;
- b) documentazione giustificativa delle risorse finanziarie utilizzate, con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata.

- Il divieto di conferimento in autonomia di contratti di consulenza o similari da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione, o comunque, quanto meno:

- a) autorizzazione scritta al conferimento dell'incarico secondo quanto previsto dall'Ordinamento Generale d'Istituto, con indicazione dei limiti di spesa, vincoli e responsabilità;
- b) lista di Fornitori / Consulenti / professionisti, gestita dal Servizio competente;
- c) gestione della lista di Fornitori (inserimento / eliminazione) basata su criteri oggettivi, di cui, all'interno della lista, deve essere data motivazione e documentazione;
- d) documentazione giustificativa degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata.

- Il divieto di concessione in autonomia di utilità da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione, o comunque, quanto meno:

- a) autorizzazione scritta a conferire utilità rilasciata dal soggetto munito del potere;
- b) elenco degli omaggi gestito dal servizio competente e, comunque, da soggetto diverso da quello che intrattiene rapporti con la Pubblica Amministrazione;

- c) documentazione giustificativa delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata;
- d) lista degli usuali Fornitori, gestita (inserimento / eliminazione) dal Servizio Centro Acquisti in base a criteri oggettivi, con individuazione, all'interno della lista, del fornitore della singola utilità, adeguatamente motivata e documentata;
- e) *budget* e consuntivi che evidenzino separatamente le spese per ciascuna tipologia di utilità;
- f) indicazione di un limite, sotto il profilo economico e quantitativo, agli omaggi a favore della Pubblica Amministrazione.

- Il divieto di assunzione in autonomia di personale da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione o, più in generale, divieto in capo allo stesso di procedere all'instaurazione di rapporti di lavoro con mobilità interna, avanzamenti di carriera, trattamenti economici nominativi e trasferimenti nominativi per i Dirigenti. Tali compiti sono tutti in capo al Consiglio d'Amministrazione o alla struttura aziendale competente delegata, che procederà con modalità operative e responsabilità definite e con oggettivi criteri di selezione dei candidati.

In particolare, con riguardo alla procedura di assunzione del personale, l'attività di ricerca delle risorse umane da avviare ai processi di selezione viene condotta, di norma, dalla struttura aziendale funzionalmente competente, con riguardo ad un bacino di destinatari provenienti da diverse fonti di reclutamento. Il procedimento di selezione deve essere strutturato in modo tale da garantire un esame dei candidati da parte di soggetti distinti.

- L'esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e/o relative alle "best practice" di riferimento, consistenti quanto meno in:

- a) cancellazione dati, liste di controllo e archivi affidata esclusivamente ad una funzione competente, assicurandone la tracciabilità;
- b) liste di controllo degli accessi ai sistemi informativi e segnalazioni automatiche all'amministratore del sistema di operazioni non autorizzate (cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema, ecc.).

Inoltre, nei rapporti con la Pubblica Amministrazione devono essere rispettati i seguenti principi:

1. la stipulazione di contratti / convenzioni con soggetti pubblici da parte della Banca a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattativa privata) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello;

2. qualunque tipo di erogazione di fondi: (a) deve essere deliberata previa adeguata istruttoria cui partecipino soggetti e/o funzioni diverse all'interno della Banca, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni all'interno della Banca; (b) presuppone una approfondita conoscenza della clientela, così da consentire una

valutazione della coerenza e della compatibilità dell'operazione con il profilo del cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico;

3. l'erogazione del credito da parte della Banca deve essere eseguita nel rispetto delle prescrizioni contenute nella procedura aziendale interna predisposta in ottemperanza alle norme di riferimento che regolano gli affidamenti (TUB) e alle Istruzioni di Vigilanza sulle aziende di credito;

4. ai Collaboratori Esterni che materialmente intrattengono rapporti con la P.A. per conto della Banca, deve essere formalmente conferito potere in tal senso dalla Banca, con apposita clausola contrattuale;

5. di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A. deve essere informato l'Organismo di Vigilanza con nota scritta;

6. i contratti tra BPM e i Collaboratori Esterni devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti;

7. i Consulenti sono scelti con metodi trasparenti e secondo specifica procedura aziendale, facendo ricorso, ove possibile, ai Consulenti "accreditati" nelle c.d. *recommended list*;

8. i Partner Commerciali devono essere scelti con metodi trasparenti e secondo specifica procedura (es. utilizzando apposite *check list* o una procedura formalizzata di *beauty contest*);

9. nei contratti con i Consulenti e con i Partner Commerciali deve essere contenuta apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al Decreto e delle sue implicazioni per BPM; di non essere mai stati implicati in procedimenti giudiziari relativi ai reati nello stesso contemplati (o se lo sono stati devono comunque dichiararlo ai fini di una maggiore attenzione da parte di BPM in caso si addivenga all'instaurazione del rapporto di consulenza o partnership); di impegnarsi al rispetto delle prescrizioni contenute nel Decreto;

10. nei contratti con i Consulenti e con i Partner Commerciali deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto (es. clausole risolutive espresse, penali);

11. alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs. 81/2008 (Testo Unico sulla Sicurezza), verifiche tributarie, INPS, autorità di vigilanza ecc.) devono partecipare i soggetti a ciò espressamente delegati o da questi ultimi sub-delegati, ovvero i soggetti responsabili delle unità operative. L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, generata dalla segnalazione della possibile commissione di reati ai sensi del Decreto, ovvero condotta da una Autorità indipendente, mediante apposita comunicazione interna, inviata a cura della Direzione della Banca di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali che verranno conservati dall'Organismo di Vigilanza.

2.2.2 Controlli preventivi dei reati informatici e del trattamento illecito di dati

Come si è detto nel paragrafo 1.2, relativo alle aree di rischio riferite ai delitti informatici, la realizzazione di questi ultimi avviene prevalentemente nell'ambito dell'area della banca funzionalmente deputata a curare i sistemi informatici e di telecomunicazione.

In ogni caso anche qualora avvenga in una diversa area funzionale (ad esempio, in un ufficio operativo che produca un documento informatico viziato da falsità), la realizzazione dei delitti si avvale degli strumenti informatici e telematici messi a disposizione dalla Banca.

Pertanto, le misure preventive dei reati non possono che trovare collocazione all'interno della funzione preposta alla cura di tali sistemi, in modo da impedire *ab origine* un loro uso illecito.

All'uopo, sono definite opportune regole sull'uso degli strumenti informatici e telematici e sulla protezione dei dati, sul rispetto delle quali sono previste attività di monitoraggio.

In primo luogo, pertanto, sono realizzate misure e procedure tecnologiche atte a prevenire la commissione di condotte criminose perpetrabili attraverso l'uso del computer e rientranti nella più comunemente definita "pirateria informatica".

La Banca ha quindi provveduto alla realizzazione di un sistema di sicurezza delle reti, di politiche di sicurezza di dettaglio, di metodi di selezione degli strumenti nonché all'adozione di protocolli applicativi che vengono a presidiare eventuali punti di vulnerabilità.

In particolare, quale strumento di prevenzione di episodi di accesso abusivo al sistema informatico della Banca medesima (e/o danneggiamento di esso o dei dati in esso contenuti) da parte di soggetti che operano all'interno di essa, è stata definita una precisa regolamentazione dei diversi livelli di autorizzazione per il compimento delle operazioni che si avvalgono degli strumenti informatici, unita all'uso di *password* personali.

A ciò si affiancano prodotti di autenticazione e di verifica dei profili degli utenti, volti a rilevare tentativi di accesso a risorse non autorizzate.

Particolare attenzione viene data al riscontro di anomalie relative all'accesso a dati di produzione: accesso attraverso cui si può giungere ad effettuare una modifica diretta sui dati medesimi, senza transitare dall' "ambiente di collaudo".

D'altro canto, la realizzazione di condotte che creino danno a sistemi altrui trova ostacolo nell'adozione di apposite politiche di sicurezza, fra le quali rientrano la regolamentazione dell'accesso alla rete Internet nonché l'elaborazione e la diffusione (sia fra i dipendenti sia fra i consulenti) di appositi documenti che dettano severi principi a disciplina dell'uso degli strumenti informatici della Banca (Testo Unico in materia di Sicurezza, Testo Unico in materia di Privacy, ecc.).

Sono specificamente disciplinati altresì gli accessi alle "aree riservate I.T." (intendendosi per tali quei locali in cui sono custodite apparecchiature, materiali e

dati informatici), con livelli di protezione adeguati al grado di criticità delle attività che vi si svolgono e con l'istituzione di un apposito sistema di controllo.

La Banca ha adottato un Regolamento di Sicurezza e, inoltre, aggiorna periodicamente il Documento Programmatico sulla Sicurezza imposto dal D.Lgs. 196/2003.

Il compito di valutazione delle politiche in materia di sicurezza e di coordinamento dei conseguenti programmi d'intervento è demandato ad un apposito Comitato.

2.2.3 Controlli preventivi dei reati concernenti le falsità in monete, carte di pubblico credito e valori in bollo

Anche per la prevenzione dei reati concernenti le falsità, ai controlli di carattere generale innanzi esaminati si aggiungono controlli maggiormente specifici, che, in particolare, consistono in:

- Sussistenza di strumenti idonei alla verifica dell'autenticità del denaro e dei valori bollati.
- Controlli sul soggetto che maneggia denaro contante e/o valori bollati, consistenti alternativamente in:
 - a) vincoli alla disponibilità di denaro contante e valori bollati;
 - b) organizzazione idonea a limitare la disponibilità in denaro contante e valori bollati.

2.2.4 Controlli preventivi dei reati societari

Diversamente dalle categorie di reati sin qui considerate (nonché da quella, di cui si dirà in appresso, dei reati aventi finalità di terrorismo e di quelli contro la personalità individuale), i reati societari che assumono rilevanza ai nostri fini si presentano come una categoria non omogenea bensì composta da fattispecie per molti aspetti diverse fra loro.

Pertanto, in considerazione sia della quantità di tali reati sia delle peculiarità che ciascuno di essi presenta rispetto agli altri, BPM ha ritenuto di individuare *standard* di controllo diversi e specifici per taluno di essi, fermi restando, peraltro, i controlli di carattere generale applicati, come si è già detto, a tutte le tipologie di reati.

Inoltre, resta fermo l'obbligo di attenersi alle disposizioni dettate dal Codice Civile, dalle leggi speciali e dalla normativa degli Organi di Vigilanza al fine di regolamentare la formazione delle comunicazioni sociali e, in generale, dei documenti contabili nonché, comunque, il compimento di attività di rilevanza contabile-amministrativa.

False comunicazioni sociali

Relativamente allo svolgimento di attività potenzialmente connesse al reato di false comunicazioni sociali (predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché adempimenti di oneri informativi obbligatori per legge o per disposizioni di Autorità di Vigilanza), i controlli previsti si attuano tramite:

- Regolamenti di Gruppo: esistono e sono diffuse al personale coinvolto in attività di predisposizione del bilancio, oltre alla generale normativa aziendale, anche norme di gruppo che definiscono con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio civilistico e consolidato e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente integrate/aggiornate dalle indicazioni fornite dall'ufficio competente sulla base delle novità in termini di normativa civilistica e diffuse ai destinatari sopra citati.

- Istruzioni di chiusura contabile: esistono istruzioni chiare rivolte ai servizi/società nelle quali si stabilisce quali dati e notizie debbano essere forniti al servizio competente per la redazione del bilancio civilistico e consolidato, nonché per la redazione di relazioni e comunicazioni sociali, con indicazione altresì di tempi e modalità. Anche le attività in capo alla figura del Dirigente preposto alla redazione dei documenti contabili societari sono disciplinate dalle procedure interne emesse o emanande e soggette a controlli periodici.

- Livello di servizio/ flusso informativo: deve essere effettuata un'attenta verifica della conformità del flusso informativo proveniente dalle diverse funzioni aziendali rispetto alle istruzioni definite e comunicate.

- Lettere di attestazione: è obbligatorio da parte dei vertici dei servizi e delle società del Gruppo, ai fini della redazione del bilancio consolidato, fornire al responsabile una lettera di attestazione sulla veridicità e completezza delle informazioni fornite.

- Formalizzazione / Tracciabilità delle attività svolte: è necessario che la trasmissione dei dati ed informazioni al servizio responsabile avvenga attraverso un sistema informatico, che consenta la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile del servizio deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema.

- Riunioni tra Società di Revisione, Collegio Sindacale ed Audit Committee: è obbligatoria l'effettuazione di almeno una riunione tra la Società di revisione, il Collegio Sindacale e l' *Audit Committee* prima della seduta del Consiglio di Amministrazione che abbia per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle rispettive attività.

- Attività di formazione: esiste un programma di formazione di base rivolto a tutti i responsabili dei servizi coinvolti nella redazione del bilancio e degli altri documenti connessi in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio ed alle relative norme di Gruppo.

- Formalizzazione e conservazione del fascicolo di bilancio: esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dall'approvazione da parte

del Consiglio d'Amministrazione sino al deposito e alla pubblicazione (anche informatica) dello stesso, nonché alla relativa archiviazione.

- Formalizzazione delle modifiche dei dati contabili: la possibilità di effettuare modifiche alle situazioni contabili è riconosciuta esclusivamente al Servizio che le ha generate, con modalità appositamente regolamentate e tali da assicurarne la tracciabilità.

Falso in prospetto

Relativamente allo svolgimento di attività potenzialmente connesse al reato di falso in prospetto (predisposizione di prospetti a fini di sollecitazione all'investimento o di ammissione alla quotazione nei mercati regolamentati, predisposizione di documenti da pubblicare in occasione di un'offerta al pubblico di strumenti finanziari), i principali controlli si attuano tramite:

- Identificazione del responsabile: è garantita l'individuazione dei responsabili delle funzioni aziendali che provvedono direttamente o indirettamente alla redazione di prospetti e/o documenti da pubblicare in occasione di un'offerta al pubblico di strumenti finanziari.

- Formalizzazione / Tracciabilità delle attività svolte: devono essere formalizzate tutte le attività svolte per la redazione del documento/prospetto e deve essere assicurata la tracciabilità dell' iter procedurale.

- Formalizzazione e conservazione del prospetto: esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti di cui sopra e alla relativa archiviazione.

Falsità nelle relazioni o nelle comunicazioni delle società di revisione

Relativamente allo svolgimento di attività potenzialmente connesse a tale reato (gestione dei rapporti con la Società di Revisione contabile in ordine all'attività di comunicazione a terzi relativa alla situazione economica, patrimoniale o finanziaria della società revisionata, nonché dei rapporti con ogni interlocutore della Società di Revisione), i principali controlli si attuano tramite:

- Obblighi di collaborazione: è obbligatorio collaborare strettamente con la Società di Revisione, da parte di tutti coloro che all'interno della Banca abbiano conoscenza di dati incidenti - direttamente o indirettamente - sulla situazione economica, patrimoniale o finanziaria della BPM.

- Selezione della società di revisione e indipendenza del mandato: i criteri di scelta della Società di Revisione e di verifica dell'indipendenza del mandato sono fissati in via preventiva.

- Riunioni tra Società di Revisione, Collegio Sindacale e Audit Committee: è obbligatoria l'effettuazione di almeno una riunione tra la società di revisione, il Collegio Sindacale e l'Audit Committee prima della seduta del Consiglio di Amministrazione, che abbia per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle rispettive attività.

- Formalizzazione / Tracciabilità delle attività svolte: esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti descritti al punto precedente e alla relativa archiviazione, nonché procedure (emesse o emanande) che assicurano la tracciabilità delle attività svolte.

Impedito controllo

Relativamente alle attività potenzialmente connesse al reato di impedito controllo (redazione, tenuta e conservazione dei documenti su cui altri organi societari o i soci potrebbero esercitare il controllo), i principali controlli si attuano tramite:

- Obbligo di collaborazione: è obbligatoria la collaborazione fra le diverse funzioni aziendali che detengono dati della Banca e i soggetti che svolgono una funzione di controllo (Collegio Sindacale e Società di Revisione).

- Esistenza di regole di Corporate Governance e di comportamento: esistono istruzioni chiare per quanto concerne la conservazione dei documenti contabili che concorrono alla formazione del bilancio (da intendersi sia quali regole di Corporate Governance sia quali norme comportamentali).

- Obbligo di informativa verso la funzione Internal Auditing: è stabilito l'obbligo di comunicazione sistematica all'Internal Auditing di ogni richiesta di informazioni o documentazione ricevuta dall'Organo amministrativo o dai suoi delegati e provenienti dai Soci, da altri organi sociali o dalla Società di Revisione.

- Esistenza di Comitati di Controllo e di un Comitato per le Remunerazioni.

- Recepimento del Codice di Autodisciplina delle Società quotate (c.d. "Codice Preda")

- Formalizzazione/Tracciabilità delle attività svolte: esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti di cui sopra (Cfr. paragrafo relativo al reato di Falso in prospetto) e alla relativa archiviazione, nonché procedure (emesse o emanande) che assicurano la tracciabilità delle attività svolte.

Indebita restituzione dei conferimenti e formazione fittizia del capitale

Relativamente alle attività potenzialmente connesse a tali reati (gestione delle incombenze societarie, operazioni sul capitale, operazioni su azioni o quote, operazioni di conferimento di ramo d'azienda o di conferimenti di beni o crediti, operazioni di trasformazione), i principali controlli si attuano tramite:

- Obbligo di preventiva informazione al Collegio Sindacale per ottenere parere preventivo e di segnalazione per iniziative di operazioni su azioni o quote: esistono regole e procedure (emesse o emanande) che obbligano le funzioni aziendali coinvolte in questo tipo di attività ad informare preventivamente il Collegio Sindacale che, a sua volta, dovrà esprimere un parere preventivo, oltre a segnalare agli organi competenti la tipologia dell'operazione.

- Disposizioni aziendali dirette al personale: esistono disposizioni aziendali dirette al personale coinvolto nella predisposizione di documenti per le delibere del Consiglio di Amministrazione in merito ad acconti su dividendi, conferimenti, fusioni e scissioni.

Illegale ripartizione degli utili e delle riserve

Relativamente alle attività potenzialmente connesse a tale reato (gestione delle incombenze societarie; redazione, tenuta e conservazione di bilanci, relazioni e altre documentazioni societarie), i principali controlli si attuano tramite:

- Obbligo di preventiva informazione al Collegio Sindacale: esiste l'obbligo di preventiva informazione per l'ottenimento di pareri preventivi o, quanto meno, l'obbligo di segnalazione di iniziative o deliberazioni in merito alla ripartizione degli utili o delle riserve.

- Disposizioni aziendali concernenti la tenuta e l'archiviazione del bilancio e dei prospetti su operazioni straordinarie: esistono disposizioni aziendali dirette al personale coinvolto nell'archiviazione e nella tenuta del bilancio e dei prospetti su operazioni straordinarie, nonché procedure (emesse o emanande) volte ad assicurare la tracciabilità dell'*iter* procedurale.

Omessa comunicazione del conflitto d'interessi

La legge punisce i soggetti i quali, svolgendo funzioni di amministrazione, direzione o controllo nei "soggetti abilitati" (definiti nell'articolo 2629-bis C.C.), violano gli obblighi previsti appositamente dalla disciplina civilistica in tema di conflitti di interesse.

Gli *standard* di controllo consistono in:

- 1) procedure e *policy* formalizzate per la rilevazione e gestione delle differenti fattispecie originatrici di conflitto;
- 2) flussi informativi inerenti l'individuazione del conflitto;
- 3) presidi specifici di prevenzione atti ad assicurare la rimozione e/o il contenimento dei rischi.

Altri controlli garantiscono la formalizzazione e la tracciabilità delle fonti e delle informazioni prodotte.

Illecite operazioni sulle azioni o quote sociali o della società controllante

Relativamente alle attività potenzialmente connesse a tale reato (operazioni sul capitale e di compravendita di azioni o quote della società o della società controllante), i principali controlli si attuano tramite:

- Disposizioni aziendali dirette al personale: esistono disposizioni aziendali dirette al personale coinvolto nella predisposizione di documenti per le delibere del Consiglio di Amministrazione in merito ad acconti su dividendi, conferimenti, fusioni e scissioni.

- Disposizioni aziendali concernenti la tenuta e l'archiviazione del bilancio e dei prospetti su operazioni straordinarie: esistono disposizioni aziendali dirette al personale coinvolto nell'archiviazione e nella tenuta del bilancio e dei prospetti su operazioni straordinarie nonché procedure (emesse o emanande) volte ad assicurare la tracciabilità dell'*iter* procedurale.

Illecita influenza sull'assemblea

Relativamente alle attività potenzialmente connesse al reato di illecita influenza sull'assemblea (attività di preparazione delle riunioni assembleari, attività di rilevanza societaria e adempimento di oneri societari, contatti con soci, contatti con organi di stampa), i principali controlli si attuano tramite:

- Obblighi informativi: esistono disposizioni aziendali formalizzate che identificano ruoli e responsabilità, relativamente agli obblighi informativi di BPM (nei confronti di Consob e Borsa) con riferimento alla stipulazione di patti parasociali.
- Regolamento assembleare: la Banca è dotata di un regolamento assembleare, adeguatamente diffuso presso i Soci.
- Regole per l'esercizio del diritto di voto: sono definite regole formalizzate per il controllo dell'esercizio del diritto di voto e per il controllo della raccolta e dell'esercizio delle deleghe di voto.
- Gestione del verbale d'assemblea: esistono disposizioni aziendali chiare e formalizzate che identificano ruoli e responsabilità, relativamente alla trascrizione, pubblicazione ed archiviazione del verbale d'assemblea.

Aggiotaggio

Relativamente alle attività sensibili potenzialmente connesse a questa fattispecie di reato (predisposizione e comunicazione di notizie/dati verso l'esterno relativi al Gruppo, operazioni di compravendita di azioni o quote della Società o di altre società del Gruppo), i principali controlli si attuano tramite:

- Formalizzazione/Tracciabilità delle fonti e delle informazioni prodotte: le fonti e le informazioni prodotte verso l'esterno devono essere formalizzate e il soggetto responsabile dell'emissione (ovverosia della predisposizione e comunicazione all'esterno) dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni.
- Sicurezza informatica: devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle *best practice* internazionali.
- Disposizioni aziendali per l'identificazione e diffusione di informazioni *price sensitive*: esistono disposizioni aziendali che contengono le modalità di identificazione delle informazioni *price sensitive* e regolamentano la loro diffusione.
- Vincoli di confidenzialità delle informazioni rilevanti per Dipendenti e Consulenti esterni: esistono vincoli formalizzati (procedure o circolari interne, clausole contrattuali) per il mantenimento della confidenzialità delle informazioni rilevanti di cui Dipendenti/Consulenti esterni vengano a conoscenza. Tali vincoli prevedono il divieto di diffusione dell'informazione rilevante all'interno o all'esterno della Banca, se non tramite il canale istituzionalmente previsto.
- Processo di comunicazione all'esterno ed archiviazione delle evidenze: esistono disposizioni aziendali formalizzate che identificano ruoli e responsabilità per la comunicazione all'esterno e l'archiviazione dei documenti approvati.

- Presidii organizzativi specifici atti a garantire la separatezza tra le diverse unità organizzative aziendali.

Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza

Relativamente alle attività potenzialmente connesse a tale reato (comunicazioni alle Autorità Pubbliche e gestione dei rapporti con le stesse), i principali controlli si attuano tramite:

- Obbligo di collaborazione: esistono direttive che sanciscono obblighi di collaborazione e trasparenza nei rapporti con le Autorità di Vigilanza.

- Formalizzazione/Tracciabilità/Archiviazione e segnalazioni nell'ambito delle attività d'ispezione: in caso di ispezioni, esistono disposizioni aziendali che identificano il soggetto responsabile per la gestione dei rapporti con l'Autorità di Vigilanza appositamente delegato dai vertici aziendali. Tali disposizioni aziendali disciplinano anche le modalità di archiviazione, la tracciabilità delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività.

- Formalizzazione/Tracciabilità/Archiviazione nelle comunicazioni scritte alle Autorità di Vigilanza: il soggetto che redige le comunicazioni scritte alle Autorità di Vigilanza deve assicurare la tracciabilità delle relative fonti e degli elementi informativi, nonché l'archiviazione delle relative richieste pervenute.

- Sicurezza informatica: esistono adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle *best practice* internazionali.

Operazioni in pregiudizio dei creditori

Relativamente alle attività potenzialmente connesse al reato di operazioni in pregiudizio dei creditori, i principali controlli sono basati sia sull'esistenza di disposizioni aziendali in proposito sia su meccanismi che consentono l'individuazione degli autori delle fonti e degli elementi informativi relativi all'operatività in esame.

2.2.5 Controlli preventivi dei reati ed illeciti amministrativi di Market Abuse.

Le regole di controllo relative ai reati e agli illeciti amministrativi di *Market Abuse* sono di seguito indicate:

- Formalizzazione/Tracciabilità delle fonti e delle informazioni prodotte: le fonti e le informazioni prodotte verso l'esterno devono essere formalizzate e il soggetto responsabile dell'emissione (ovverosia della predisposizione e comunicazione all'esterno) dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni;

- Sicurezza informatica: esistono adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle *best practice* internazionali;

- Separatezza tra le diverse unità organizzative aziendali: esistono specifici presidi organizzativi atti a garantire tale separatezza;

Più specificamente, i presidi relativi all'abuso di informazioni privilegiate e manipolazione di mercato possono essere così sintetizzati:

1. disposizioni aziendali contenenti le modalità per l'identificazione e la diffusione delle informazioni *price sensitive*;
2. vincoli formalizzati (procedure o circolari interne, clausole contrattuali) per il mantenimento della confidenzialità delle informazioni rilevanti di cui Dipendenti/Consulenti esterni vengano a conoscenza. Tali vincoli prevedono il divieto di diffusione dell'informazione rilevante all'interno o all'esterno della Banca, se non tramite il canale istituzionalmente previsto;
3. disposizioni aziendali formalizzate che identificano ruoli e responsabilità per la comunicazione all'esterno e l'archiviazione dei documenti approvati;
4. presidi relativi alla gestione dei rapporti con la stampa e all'attività di comunicazione esterna, affidate ad apposite funzioni dedicate secondo le modalità previste dall'Ordinamento Generale d'Istituto (in particolare, l'Ordinamento Funzionale).
5. presidi relativi alla cura della veridicità, della completezza informativa e dell'aggiornamento del sito, con particolare riguardo ai suoi contenuti finanziari. (ad esempio, modulistica, contrattualistica e circolari interne Banca);
6. presidi relativi all'organizzazione dei contenuti del sito in modo coerente e chiaro, privilegiando l'aspetto della fruibilità e della facilità di accesso da parte dell'utente (ad esempio, Direttive e procedure sulla circolazione delle informazioni del Regolamento Registro degli *Insider*);
7. presidi relativi alla disciplina delle informazioni su eventi e circostanze rilevanti (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi dell'art. 114 TUF);
8. presidi relativi alla identificazione dei soggetti rilevanti che hanno effettuato operazioni e relativi adempimenti agli obblighi di comunicazione (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi dell'art. 114 TUF);
9. presidi relativi alla disciplina dei tempi e delle modalità di trasmissione delle comunicazioni alla Consob, alla Società e al Pubblico (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi dell'art. 114 TUF);
10. presidi relativi all'individuazione del soggetto preposto al ricevimento, gestione e diffusione delle informazioni (ad esempio, Codice di

Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi dell'art. 114 TUF);

11. presidii relativi alla disciplina delle operazioni compiute, da soggetti rilevanti oggetto dell'obbligo di comunicazioni, durante il c.d. *Black Out Periods*, ossia 30 gg. precedenti riunioni del Consiglio di Amministrazione e 30 gg. precedenti eventuali assemblee straordinarie/ordinarie (ad esempio, Codice di Comportamento *Internal Dealing*);
12. presidii relativi alla previsione di sanzioni pecuniarie per mancata comunicazione (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi dell'art. 114 TUF);
13. presidii relativi alla previsione dell'obbligo di riservatezza sulle informazioni privilegiate e procedure idonee alla gestione delle informazioni riservate (ad esempio, Regolamento di Gruppo BPM concernente il Registro degli *Insider* ai sensi dell'art. 115-bis TUF e Codice Etico);
14. direttive e procedure sulla circolazione delle informazioni (ad esempio, Regolamento Registro degli *Insider*);
15. presidii relativi all'istituzione di un apposito Registro delle persone che hanno accesso a informazioni privilegiate e alla disciplina dello stesso Registro; in particolare: alimentazione del Registro, tipologia delle informazioni, comunicazioni agli interessati, criteri di gestione del Registro, modalità di tenuta, aggiornamento, ricerca dati nel Registro, conservazione della documentazione e del Registro, direttive e procedure sulla circolazione delle informazioni, divieti imposti ai soggetti iscritti nel Registro, coordinamento con registri terzi (ad esempio, Regolamento di Gruppo BPM concernente il Registro degli *Insider* ai sensi dell'art. 115-bis TUF);
16. presidii relativi al rispetto dei principi di correttezza, trasparenza e veridicità dei dati forniti al mercato e/o ai clienti, sia con riferimento a quelli direttamente attinenti alla Banca, sia a quelli diffusi, con la consulenza o comunque l'ausilio della Banca;
17. presidii relativi al rispetto dei principi di correttezza, adeguatezza, trasparenza e veridicità con riferimento ai comportamenti posti in essere dalla Banca nei confronti dei clienti (ad esempio, la modulistica, la contrattualistica e circolari interne Banca);
18. procedura per segnalazione di operazioni sospette: in ottemperanza al Regolamento Consob n.16191/2007 recante norme di attuazione del decreto legislativo 24 febbraio 1998 n. 58 in materia di mercati, è stata predisposta una procedura informatica che, in base a determinati parametri descritti nel citato Regolamento (art. 43), consente il monitoraggio e la rilevazione automatica di operazioni potenzialmente sospette mediante l'utilizzo dei c.d. diagnostici. Le operazioni suddette comprendono tutti gli strumenti finanziari (inclusi i derivati) ammessi o per i quali sia stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro

paese dell'Unione Europea o in un sistema multilaterale di negoziazione italiano. Gli ordini e/o gli eseguiti "sospetti" di un abuso vengono aggregati per deposito e per titolo, e successivamente sottoposti ad apposita analisi (test del ragionevole sospetto) per determinare la necessità della loro segnalazione alle Autorità;

19. presidi relativi alla definizione e attuazione delle politiche di gestione e di incentivazione del personale appartenente a tutti i livelli aziendali, realizzati e attuati in modo da non generare l'erroneo convincimento che il raggiungimento di determinati *standard* di produttività sia di per sé, indipendentemente dalle concrete modalità seguite, oggetto di valutazione positiva da parte della Banca (ad esempio, Codice Etico e Codice di Comportamento del Settore Bancario e Finanziario).

2.2.6 Controlli preventivi dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico.

Al fine della prevenzione di tali reati BPM si avvale degli *standard* generali di controllo già esaminati con riguardo a tutte le categorie di reati.

Con riferimento ai reati in considerazione, tali controlli riguardano essenzialmente la fase di istruttoria relativa alla valutazione dei clienti della Banca – italiani e soprattutto stranieri – e delle attività da essi svolte.

A tali controlli, di carattere generale, si aggiungono dei controlli specifici, relativi ai reati in esame.

In particolare la prevenzione dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico si fonda innanzitutto sul rispetto, da parte della Banca, delle norme dettate per gli intermediari dalla Banca d'Italia e dall'Unità di Informazione Finanziaria in materia di antiriciclaggio e di segnalazione di operazioni finanziarie sospette.

I controlli specificamente previsti risultano pertanto essere:

- Procedure formalizzate di istruttoria per la valutazione dei clienti e delle attività da essi svolte in Italia e all'estero, anche avvalendosi di elenchi di nominativi di soggetti segnalati essere coinvolti (o potenzialmente coinvolti) in attività terroristiche;

- Processi e Procedure per la realizzazione degli adempimenti di legge in tema di identificazione e adeguata verifica della clientela, registrazione delle operazioni, individuazione e segnalazione delle operazioni sospette. I controlli sulle operazioni sospette devono essere costanti nel corso del rapporto continuativo, riportando le transazioni eseguite alla conoscenza che la Banca ha della propria clientela. A questa valutazione, cui si perviene per lo più tramite uno *screening* automatizzato, va sempre aggiunto l'apporto del giudizio critico del personale, al fine di individuare e conseguentemente segnalare le operazioni sospette;

- Relativamente alle operazioni di finanziamento, controlli sui soggetti che gestiscono l'attività di riferimento, in particolare attraverso:

- a) identificazione dei soggetti che svolgono materialmente l'attività istruttoria e del soggetto che autorizza l'operazione con il cliente;
- b) formalizzazione e tracciabilità delle attività svolte;
- c) registrazione delle operazioni come da procedure aziendali;
- d) controlli specifici ulteriori, istituiti in ottemperanza alla normativa antiriciclaggio (attraverso l'uso, fra l'altro, di *check-list* nonché di procedure informatiche volte ad evidenziare operazioni sospette).

2.2.7 Controlli preventivi dei delitti contro la personalità individuale

Con riguardo ai delitti contro la personalità individuale, escludendosi l'ipotesi che la Banca possa essere asservita al perseguimento di finalità illecite connesse alla tratta di persone ovvero a fatti di pedo-pornografia, si deve ritenere che profili di rischio rilevanti con riferimento a detti reati possano ravvisarsi con riferimento ai soli casi in cui sussista un concorso o un'agevolazione di soggetti terzi, finanziandone l'attività.⁴

La prevenzione di tali reati si avvale essenzialmente dei già esaminati standard generali di controllo riguardanti la fase di istruttoria relativa alla valutazione dei clienti e delle attività da essi svolte.

A tali controlli, di carattere generale, si aggiungono dei controlli specifici, relativi ai reati in esame, ed in particolare:

- Procedure formalizzate di istruttoria per la valutazione dei clienti e delle attività da essi svolte in Italia e all'estero, anche avvalendosi di elenchi di nominativi di soggetti segnalati essere coinvolti (o potenzialmente coinvolti) in attività terroristiche.

- Relativamente alle operazioni di finanziamento, controlli sui soggetti che gestiscono l'attività di riferimento, in particolare attraverso:

- a) identificazione dei soggetti che svolgono materialmente l'attività istruttoria e del soggetto che autorizza l'operazione con il cliente;
- b) formalizzazione e tracciabilità delle attività svolte;
- c) registrazione delle operazioni come da procedure aziendali;
- d) controlli specifici ulteriori, istituiti in ottemperanza alla normativa antiriciclaggio (attraverso l'uso, fra l'altro, di *check-list* nonché di procedure informatiche volte ad evidenziare operazioni sospette).

2.2.8 Controlli preventivi dei reati di criminalità organizzata

⁴ Affinché possa configurarsi un concorso dei soggetti in posizione apicale o dipendenti nel reato è necessario che tale condotta si risolva – quanto meno – in un'agevolazione del fatto delittuoso dell'autore e che l'operatore sia a conoscenza della finalità illecita che il cliente persegue. E' evidente che la forma di concorso che presenta maggiori profili di rischio per i soggetti in posizione apicale o dipendenti è quella connessa al finanziamento di soggetti che pongano in essere reati connessi alla tratta di persone o alla pedo-pornografia.

Si rammenta, infine, che affinché sussista la possibilità di imputare l'illecito alla banca, è necessario che il reato sia stato commesso nell'interesse o a vantaggio della banca medesima e non semplicemente avvalendosi della sua struttura per il perseguimento di profitto riferibile esclusivamente al soggetto attivo.

I reati rilevanti ai fini di detta responsabilità dell'ente sono quelli richiamati nel paragrafo 1.8.

Per quanto concerne i reati in esame, i controlli riguardano prevalentemente la fase di istruttoria relativa alla valutazione dei clienti della Banca e le attività da essi svolte anche nel prosieguo del rapporto, comprendendo anche adempimenti imposti dal Decreto Antiriciclaggio (fra i quali, l'identificazione e l'adeguata verifica della clientela, le registrazioni delle operazioni bancarie e la conservazione delle informazioni attraverso l'istituzione di un archivio unico informatico, nonché la rilevazione e la segnalazione delle operazioni sospette).

I controlli devono essere costanti nel corso del rapporto continuativo, rapportando le transazioni eseguite alla conoscenza che la Banca ha della propria clientela. A questa valutazione, cui si perviene per lo più tramite uno *screening* automatizzato, va sempre aggiunto l'apporto del giudizio critico del personale, al fine di individuare e conseguentemente segnalare le operazioni sospette.

A questo riguardo viene in supporto anche la nuova procedura tramite la quale le informazioni relative a indagini giudiziarie di cui la Banca sia stata informata con riguardo a soggetti non clienti, possano (con l'adozione delle opportune misure di tutela della riservatezza) essere trasmesse alla dipendenza che, in un momento successivo, si trovi eventualmente ad instaurare un rapporto commerciale con i medesimi soggetti.

Con riguardo allo svolgimento dell'attività di concessione del credito, le misure preventive dei reati in considerazione poste in essere dalla Banca coincidono con quelle realizzate per la prevenzione dei delitti aventi finalità di terrorismo e di eversione dell'ordine democratico, e pertanto, oltre alle suddette procedure per la realizzazione degli adempimenti di legge:

- procedure formalizzate di istruttoria per la valutazione dei clienti e delle attività da essi svolte in Italia e all'estero, anche avvalendosi di elenchi di nominativi di soggetti segnalati essere coinvolti (o potenzialmente coinvolti) in attività terroristiche;
- controlli sui soggetti che gestiscono l'attività di riferimento, in particolare attraverso:
 - a. identificazione degli addetti che svolgono materialmente l'attività istruttoria e del soggetto che autorizza l'operazione con il cliente;
 - b. formalizzazione e tracciabilità delle attività svolte;
 - c. registrazione delle operazioni come da procedure aziendali;
 - d. controlli specifici ulteriori, istituiti in ottemperanza alla normativa antiriciclaggio (anche attraverso l'uso di *check-list* nonché di procedure informatiche volte ad evidenziare operazioni sospette).

Nell'ambito dello svolgimento dell'attività finanziaria, i presidi costituiti da sistemi automatizzati di monitoraggio della clientela, della movimentazione e dei rapporti, realizzati nella prevenzione degli abusi di mercato, costituiscono anch'essi un supporto all'attività di controllo legata alla normativa antiriciclaggio.

La Banca ha investito un'apposita Funzione del ruolo di "ente gestore antiriciclaggio", con compiti di analisi, monitoraggio e consulenza in merito alla realizzazione degli adempimenti imposti dalla normativa di legge sull'argomento.

2.2.9 Controlli preventivi dei reati transnazionali

Come si è detto nel paragrafo 1.9, relativo alle aree di rischio riferite ai reati transnazionali, anche i controlli preventivi per questi ultimi coincidono sostanzialmente con quelli già esaminati nel paragrafo 2.2.8 riguardanti i reati di criminalità organizzata, stante la sola differenza consistente qui nello specifico riferimento alla loro realizzazione con le caratteristiche di transnazionalità sopra descritte al paragrafo 1.9.

Diversa è, invece, la natura dei controlli approntati con riguardo al reato di Favoreggiamento personale.

Per la prevenzione di esso la Banca ha adottato rigide regole di segregazione delle attività che fanno sì che ad un processo di gestione di una vicenda connessa ad un contenzioso giudiziario prendano parte più soggetti: ciò al fine di impedire la possibilità di realizzare occulti accordi volti ad alterare le dichiarazioni da rendersi all'Autorità giudiziaria o, comunque, ad agevolare l'elusione di investigazioni giudiziarie.

2.2.10 Controlli preventivi dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Per i reati che qui vengono considerati, si rinvia a quanto detto nei paragrafi sui controlli preventivi dei reati di criminalità organizzata e dei reati transnazionali.

Oltre ai controlli in detti paragrafi descritti, un importante presidio è poi costituito dalla partecipazione del personale addetto a specifici programmi di formazione, che li aiutino a riconoscere le attività potenzialmente connesse al riciclaggio o al finanziamento del terrorismo e forniscano loro le necessarie istruzioni sul modo di procedere.

Per ciò che concerne il reato di ricettazione, è fatto divieto di intrattenere rapporti commerciali con soggetti (persone fisiche o giuridiche) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della legalità.

A ciò si aggiunge un'attenta gestione dei rapporti con i fornitori, aggiornando il relativo "portafoglio acquisti" (fornitori/prodotti e servizi) e curandone la valutazione nell'ambito di una lista gestita dal Servizio Centro Acquisti secondo principi e criteri oggettivi (che comprendono sia requisiti tecnici sia requisiti di immagine), nonché acquisendo e archiviando correttamente la documentazione amministrativa di riferimento, al fine di garantire la trasparenza degli accordi.

Peraltro, la gestione dei suddetti rapporti commerciali presuppone gli interventi degli Enti Responsabili di Spesa, chiamati a definire requisiti e specifiche tecniche del bene/servizio richiesto e del Servizio Centro Acquisti per le fasi di negoziazione

(intesa come mezzo per ottenere l'adeguamento del fornitore alle esigenze dell'azienda attraverso le condizioni più favorevoli in termini di prezzo, qualità, servizio e clausole contrattuali) e di emissione degli ordini.

La fase di analisi/scelta del fornitore, infine, viene di solito svolta congiuntamente dalle due suddette funzioni

2.2.11 Controlli preventivi dei reati di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro

Le regole adottate dalla Banca al fine di prevenire la commissione dei reati suindicati assicurano soprattutto l'adozione delle misure tecniche e organizzative imposte dal Testo Unico sulla Sicurezza (D.Lgs. 81/2008).

Tali misure consistono principalmente nelle seguenti:

- individuazione, all'interno dell'azienda, delle figure che ai sensi di legge rivestono un ruolo di responsabilità in ordine all'applicazione della normativa in esame;
- predisposizione e costante aggiornamento del Documento di Valutazione dei Rischi;
- attuazione della sorveglianza sanitaria dei lavoratori ed eventuale allontanamento degli stessi dall'esposizione al rischio a tutela della loro incolumità;
- adozione nei luoghi di lavoro delle misure e dei requisiti tecnico – strutturali imposti dalla nuova normativa e conseguente svolgimento di una regolare attività di manutenzione avente ad oggetto, oltre ai locali, anche gli impianti, le attrezzature e i dispositivi di sicurezza;
- adozione di adeguate misure di primo soccorso, di prevenzione degli incendi e di lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato e, più in generale, di gestione delle emergenze, designando preventivamente i lavoratori incaricati della loro attuazione;
- realizzazione di un'attività di informazione, formazione e addestramento rivolta sia ai lavoratori genericamente intesi sia a determinate figure che, all'interno della Banca, rivestono compiti particolari in merito all'attuazione della normativa sulla sicurezza nei luoghi di lavoro, ma particolarmente a chi tra essi svolge attività che li espone a rischi specifici;
- vigilanza sul rispetto e l'attuazione delle misure di prevenzione e protezione dai rischi;
- attenta scelta dei soggetti incaricati della realizzazione di opere o della fornitura di servizi autonomi;
- perfezionamento dei contratti di appalto, d'opera o di somministrazione secondo le modalità e i requisiti richiesti dalla legge e, in particolar modo, con indicazione in essi dei costi relativi alla sicurezza del lavoro e con la contestuale redazione del D.U.V.R.I. (Documento Unico di Valutazione dei Rischi da Interferenze).

2.2.12 Controlli preventivi dei reati contro l'Industria e il Commercio e dei reati di falsità in strumenti e segni di riconoscimento

Come si è già detto nel paragrafo 1.14, l'area potenzialmente coinvolta in questa tipologia di reati risulta essere quella che cura la creazione di prodotti nonché le attività di *marketing* e comunicazione commerciale.

Pertanto, fermi restando i controlli di carattere generale applicati, come si è già detto, a tutte le tipologie di reati, rileva per lo più in questo caso l'obbligo di attenersi alle disposizioni dettate dal Codice Civile a divieto degli atti di concorrenza sleale (art. 2598 ss.) nonché in materia di azienda e utilizzo del marchio e dei segni distintivi (art. 2555 ss.).

In particolare i controlli preventivi consistono in:

- diffusione, attraverso *policy* e regolamenti interni, di una cultura dei rischi e dei controlli sulle operazioni di business concernenti la creazione e diffusione di nuovi prodotti;
- esistenza di processi e regole per la creazione di nuovi prodotti che definiscano ruoli e responsabilità e che prevedano, tra l'altro, ricerche e analisi sull'utilizzo di denominazioni e segni distintivi da parte di aziende concorrenti, anche attraverso la consultazione di apposite banche dati elettroniche;
- esistenza di processi e regole per l'attività di pubblicità e comunicazione commerciale che pongano adeguati limiti all'utilizzo di descrizioni, immagini, forme grafiche, slogan commerciali e quant'altro che possa generare confusione con prodotti di concorrenti;
- coordinamento tra i responsabili delle attività di creazione di nuovi prodotti e i responsabili delle attività di pubblicità e *marketing*;
- attività di formazione specifica rivolta a coloro che operano nelle aree commerciali e di *marketing*.

2.2.13 Controlli preventivi dei reati in materia di violazione del diritto d'autore

Poiché, come si è già detto al paragrafo 1.15, l'area potenzialmente coinvolta dai reati sul diritto d'autore risulta essere quella funzionalmente deputata a curare i sistemi informatici, i controlli preventivi coincidono in gran parte con quelli esaminati nel precedente paragrafo 2.2.2, con riguardo all'adozione di apposite politiche e regole di sicurezza dei dati informatici, nonché relative alla regolamentazione e al controllo degli accessi agli strumenti informatici e relativo uso.

Inoltre viene in considerazione l'adozione e la diffusione tra il personale di regole che vietino l'uso e la messa a disposizione non autorizzati di opere dell'ingegno, di banche dati, nonché di qualsiasi supporto che formi oggetto della tutela riconosciuta dalle norme sul diritto d'autore.

Le suddette regole dovranno in particolar modo essere inserite all'interno della regolamentazione delle attività di formazione aziendale.

2.2.14 Controlli preventivi dei reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Per la prevenzione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, la Banca ha adottato rigide regole di segregazione delle attività che fanno sì che ad un processo di gestione di una vicenda connessa ad un contenzioso giudiziario prendano parte più soggetti: ciò al fine di impedire la possibilità di realizzare occulti accordi volti ad alterare le dichiarazioni da rendersi all'Autorità giudiziaria o, comunque, ad agevolare l'elusione di investigazioni giudiziarie.

3. NORMATIVA E DOCUMENTAZIONE AZIENDALE DI RIFERIMENTO

- a. Ordinamento Generale d'Istituto, costituito dalla regolamentazione interna *pro tempore* vigente disciplinante, in particolare: l'Assetto Direzionale dell'Istituto, i Poteri della Direzione Generale, l'Ordinamento Funzionale, i profili di ruolo della Rete commerciale, i Comitati, i Fidi (con i relativi poteri delegati e disposizioni applicative), la Finanza (regolamento Generale e disposizioni applicative, Regolamento deontologico dell'attività in Cambi, regolamento deontologico dell'attività in Titoli), i Promotori Finanziari, il Codice di Comportamento del Settore Bancario e Finanziario, il modello del Sistema di Controllo Interno, il modello di controllo ex L. 262/05 sul Dirigente preposto alla redazione dei documenti contabili societari, la Cassa e Custodia valori, la Sicurezza (e disposizioni applicative), il *telex-swift* e la Rete Nazionale Interbancaria, la Beneficenza, i *Budget* di spesa e degli Acquisti, i Poteri delegati (Poteri di Firma, Poteri di *Pricing*), la gestione del Personale, il Trattamento dei dati personali (e disposizioni applicative), il Gruppo Bipiemme (regolamento e disposizioni applicative), le Operazioni "significative" e con parti correlate, il Registro degli Insider ai sensi dell'art.115-bis TUF, gli obblighi di comunicazione ai sensi dell'art. 114 TUF, l'Internal Dealing, il modello della funzione Compliance, il governo del processo ICAAP, i flussi informativi interni a BPM e al Gruppo, le *policy* MiFID, gli Organi Sociali, nonché il presente Modello di organizzazione, gestione e controllo e il Codice Etico.
- b. Testi Unici Aziendali (conosciuti anche come Circolari) costituiti dalla regolamentazione interna di contenuto operativo (*pro tempore* vigente) delle diverse attività della Banca, nell'ambito delle categorie dei processi di governo, processi commerciali, processi del credito e processi della finanza.

4. SISTEMA DISCIPLINARE

4.1 Principi generali

Ai sensi dell'articolo 6, comma 2, lettera e) del Decreto, il Modello deve contenere un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

In BPM, in caso di violazione delle regole di condotta imposte ai fini della prevenzione dei reati contemplati dal Decreto, lo svolgimento del procedimento disciplinare e l'applicazione delle sanzioni disciplinari sono affidati, nell'ambito delle competenze ad essa attribuite, alla Direzione del Personale, anche su attivazione o segnalazione da parte dell'Organismo di Vigilanza, la quale, nel rispetto delle norme vigenti in BPM, decide in autonomia i provvedimenti disciplinari sino a due giorni di sospensione dal servizio e dal trattamento economico. I provvedimenti da tre a dieci giorni di sospensione dal servizio e dal trattamento economico sono sottoposti per la decisione al Direttore Generale, mentre sono proposti per la delibera al Consiglio di Amministrazione i licenziamenti per giusta causa o giustificato motivo.

Nell'eventualità in cui il destinatario del provvedimento disciplinare sia il dirigente della Direzione del Personale la competenza per l'applicazione di tale provvedimento sarà attribuita al Direttore Generale.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, poiché le regole di condotta imposte dal Modello sono assunte da BPM in piena autonomia, indipendentemente dall'illecito che eventuali condotte possano determinare, nel rispetto di quanto disposto dal CCNL.

BPM da tempo utilizza procedure e modelli di organizzazione e sistemi di controllo, le cui violazioni sono soggette al sistema sanzionatorio vigente.

Viene pertanto espresso – con assoluta ed inequivocabile chiarezza – che nessun comportamento illecito, o illegittimo, o scorretto può essere giustificato o considerato meno grave, in quanto compiuto nell'asserito “*interesse*” o nell'asserito “*vantaggio*” della Banca.

Al contrario, stante l'inequivoca, insuperabile e priva di eccezioni volontà di BPM di non intendere in alcun caso avvalersi di siffatti “*interessi*” o “*vantaggi*”, tale intento – ove posto in essere nonostante le contrarie misure realizzate dall'Azienda – costituirà uno degli specifici campi di intervento del presente sistema disciplinare.

4.2 Sanzionabilità del tentativo

Sono altresì sanzionati gli atti od omissioni diretti in modo non equivoco a violare le regole stabilite da BPM, anche se l'azione non si compie o l'evento non si verifica.

4.3 Sanzioni per i Dipendenti

L'inosservanza delle regole indicate nel Modello adottato dalla BPM ai sensi del Decreto, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte del personale dipendente che non rivesta la qualifica di dirigente, può dar luogo, secondo la gravità dell'infrazione, all'irrogazione di sanzioni disciplinari nel

pieno rispetto delle disposizioni di cui all'art. 7 della legge 20 maggio 1970 n. 300 e della vigente contrattazione collettiva applicabile e precisamente:

- rimprovero verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico, fino ad un massimo di 10 giorni;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

Fermo restando quanto sopra, si precisa peraltro quanto segue:

- rimprovero verbale: si applica in caso di lieve inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di lieve violazione delle procedure e norme interne, nonché delle istruzioni o delle direttive impartite dai superiori, nonché in caso di lieve negligenza nell'espletamento del lavoro;
- rimprovero scritto: si applica nei casi precedenti quando vi siano circostanze particolari che, fermo il carattere lieve della mancanza, richiedano un maggior intervento;
- sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di violazione delle procedure e norme interne, nonché delle istruzioni o delle direttive impartite dai superiori in casi di una certa gravità o connotati da recidiva; in caso di negligenza di una certa gravità o che abbia avuto riflessi negativi per l'azienda o per i terzi; in caso di omessa segnalazione o tolleranza di gravi irregolarità commesse da altri;
- licenziamento per giustificato motivo: si applica in caso di notevole inadempimento dei principi e delle regole di comportamento previste dal presente Modello, ovvero delle procedure e norme interne, ovvero delle istruzioni o delle direttive impartite dai superiori, ovvero in caso di commissione di uno dei reati o degli illeciti amministrativi sanzionati dal Decreto Legislativo n. 231/2001 e successive modifiche;
- licenziamento per giusta causa: si applica in caso di comportamento in contrasto con le prescrizioni e/o le procedure e/o le norme interne previste dal presente Modello, che leda l'elemento fiduciario che caratterizza il rapporto di lavoro o risulti talmente grave da non consentire comunque la prosecuzione nemmeno provvisoria del rapporto stesso.

Particolare rigore sarà osservato in ordine ai casi di responsabilità per omesso controllo da parte di persone investite, in generale o in casi particolari, delle relative funzioni (controllo, vigilanza, sorveglianza).

Restano ferme e si intendono qui richiamate tutte le disposizioni, previste dalla Legge e dai contratti collettivi applicati, relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.

L'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni avverranno nel rispetto di quanto previsto dalla legge (es. Statuto Lavoratori), dal CCNL, dallo Statuto BPM e dalle disposizioni aziendali.

4.4 Sanzioni per i soggetti in posizione apicale

In caso di violazione, da parte di Dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, la Banca provvede ad applicare le misure più idonee, tenuto conto della gravità della violazione e della eventuale reiterazione, del livello di responsabilità e dell'intenzionalità, in conformità a quanto previsto dalla normativa vigente e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti delle imprese creditizie, finanziarie e strumentali.

Tale rapporto di lavoro è peculiare, caratterizzato dal vincolo fiduciario e dalla particolare necessità, per la Banca, di affidarsi a soggetti dalla spiccata professionalità, disponibilità e competenza per l'attuazione dei principi di condotta e per il rispetto dei principi di legge e delle procedure e delle norme aziendali tutte.

Considerato che i provvedimenti contemplati dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti comportano la risoluzione del rapporto di lavoro, gli stessi andranno applicati nei casi di massima gravità della violazione commessa, mentre, per le infrazioni meno gravi, la Banca, in ossequio al principio giuridico della proporzionalità e gradualità della sanzione, si riserva la facoltà di applicare le seguenti sanzioni:

- rimprovero verbale

- nel caso di lieve inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di comportamento non conforme o non adeguato alle prescrizioni del Modello, ovvero di violazione delle procedure e norme interne previste e/o richiamate;

- rimprovero scritto

- mancanze punibili con il rimprovero verbale, ma che, per conseguenze specifiche o per recidiva, abbiano una maggior rilevanza;
- omessa segnalazione o tolleranza di irregolarità in materia lieve commesse da altri.

- licenziamento ex art. 2118 c.c.

- inosservanza delle procedure interne previste dal Modello e negligenza rispetto alle prescrizioni in esso contenute;
- omessa segnalazione o tolleranza di gravi irregolarità commesse da altri appartenenti al Personale;
- adozione di comportamento che possa configurare una possibile ipotesi di reato sanzionato dal D.Lgs. 231/2001 di una gravità tale da esporre la Banca ad una situazione oggettiva di pericolo o tale da determinare riflessi negativi per la stessa.

- licenziamento per giusta causa

- nel caso di adozione di un comportamento palesemente non conforme o non adeguato alle prescrizioni del Modello, tale da determinare la possibile concreta applicazione a carico della Banca delle misure previste dal D.Lgs. 231 /2001 e riconducibile a mancanze di una gravità tale da far venir meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentirne la prosecuzione nemmeno provvisoria.

4.5 Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Collegio Sindacale e l'intero Consiglio affinché possano prendere gli opportuni provvedimenti.

4.6 Misure nei confronti dei Sindaci

In caso di violazione del Modello da parte di uno o più Sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale ed il Consiglio di Amministrazione affinché possano prendere gli opportuni provvedimenti.

4.7 Misure nei confronti dei Collaboratori Esterni

Ogni violazione delle regole previste dal Modello, nonché ogni commissione dei reati, imputabile ai Collaboratori Esterni (ad esempio, società di *service*, Consulenti o Partner), è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti. Resta salva l'eventuale richiesta di risarcimento dei danni eventualmente derivanti alla Banca da tale comportamento, come nel caso di applicazione alla stessa da parte dell'Autorità Giudiziaria delle misure previste dal Decreto.

5. FORMAZIONE

Ai fini dell'efficacia del presente Modello, è obiettivo di BPM garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Dipendenti. Tale obiettivo riguarda tutte le risorse aziendali che rientrano nella categoria anzidetta, sia si tratti di risorse già presenti in azienda sia da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Aree di Rischio.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al Decreto è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari e dell'esistenza o meno in capo ad essi di funzioni di rappresentanza della Banca.

In particolare, la Banca ha previsto livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione per:

1. Dipendenti che rivestono la qualifica di dirigenti;
2. Dipendenti che non rivestono la qualifica di dirigenti;
3. Collaboratori Esterni.

La formazione del personale, al fine della corretta applicazione del Modello, viene gestita dall'Area Pianificazione e Formazione della Direzione del Personale, in collaborazione con i responsabili delle altre Direzioni/Servizi di volta in volta coinvolti nell'applicazione del Modello e con l'Organismo di Vigilanza, che ha anche funzioni di supervisione.

E' prestata particolare attenzione al personale di nuova assunzione.

La formazione è articolata sui livelli di seguito riportati.

5.1 Dirigenti (grado di Direttore Addetto alla Direzione Centrale o superiore)

Realizzazione delle seguenti attività formative:

- consegna di documento informativo sul contenuto del Decreto, con raccolta di conferma di avvenuta ricezione (per i soggetti di nuova assunzione la consegna avviene all'atto dell'assunzione medesima);
- messa a disposizione del Modello attraverso pubblicazione sia in OGI sia sul sito Internet della Banca;
- consegna e/o pubblicazione in OGI del Codice Etico;
- seminari di presentazione delle finalità e dei contenuti del Decreto;
- corso di formazione *on line* (aggiornato alla luce delle modifiche legislative) con certificazione finale;
- illustrazione dei contenuti di legge in occasione di incontri appositamente organizzati.

5.2 Altro Personale

Realizzazione delle seguenti attività formative:

- consegna di documentazione costituita da lettera ai dipendenti, nota esplicativa delle fattispecie di reato e testo del Decreto (per i soggetti di nuova assunzione la consegna avviene all'atto dell'assunzione medesima);
- consegna e/o pubblicazione in OGI del Codice Etico;

- messa a disposizione del Modello attraverso pubblicazione sia in OGI sia sul sito Internet della Banca;
- corso di formazione *on line* (aggiornato alla luce delle modifiche legislative) con certificazione finale;
- previsione di specifiche modalità di erogazione della formazione per i dipendenti con disabilità sensoriali.

5.3 Collaboratori Esterni

Ai soggetti esterni che, a vario titolo, collaborano con BPM, vengono fornite apposite informative sulle politiche e sulle procedure adottate da BPM medesima sulla base del presente Modello.

Inoltre ad essi viene resa nota, attraverso apposita clausola contrattuale, la pubblicazione dei testi del Modello e del Codice Etico sul sito Internet della Banca.

ALLEGATI

1. D.Lgs. 8 giugno 2001, n° 231;
2. Legge 16 marzo 2006, n° 146.