CASSA DI RISPARMIO DEL VENETO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

Approvato dal Consiglio di Amministrazione nella seduta del 28 luglio 2010

INDICE

Capitolo 1 – Il contesto normativo

1.1 Il regime di responsabilità amministrativa previsto dal Decreto Legislativo n. 231/2001 a carico delle persone giuridiche, società ed associazioni

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito denominato il "Decreto" o anche "D. Lgs. n. 231/2001"), con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche. In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri e della Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli Enti (da intendersi come società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi nel loro interesse o vantaggio: (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Il catalogo degli "illeciti presupposto" si è dilatato in tempi recenti con l'introduzione, nell'ambito degli illeciti presupposto, anche di alcune fattispecie di illecito amministrativo.

La responsabilità dell'Ente si aggiunge a quella della persona fisica, che ha commesso materialmente l'illecito, ed è autonoma rispetto ad essa, sussistendo anche quando l'autore del reato non è stato identificato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti ivi espressamente previsti, gli Enti che abbiano tratto vantaggio dalla commissione del reato o nel cui interesse siano stati compiuti i reati - o gli illeciti amministrativi - presupposto di cui al Decreto medesimo. A carico dell'Ente sono irrogabili sanzioni pecuniarie e interdittive, nonché la confisca, la pubblicazione della sentenza di condanna ed il commissariamento. Le misure interdittive, che possono comportare per l'Ente conseguenze più gravose rispetto alle

sanzioni pecuniarie, consistono nella sospensione o revoca di licenze e concessioni, nel divieto di contrarre con la pubblica amministrazione, nell'interdizione dall'esercizio dell'attività, nell'esclusione o revoca di finanziamenti e contributi, nel divieto di pubblicizzare beni e servizi.
La suddetta responsabilità si configura anche in relazione a reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

1.2 L'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'Ente

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi".
La medesima norma prevede, inoltre, l'istituzione di un organismo di controllo interno all'Ente con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza dei predetti modelli, nonché di curarne l'aggiornamento.
Il modello di organizzazione, gestione e controllo (di seguito denominati anche "Modelli") deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che: (i) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione e di Gestione idoneo a prevenire reati della specie di quello verificatosi; (ii) il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare l'aggiornamento è stato affidato a un

organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo; (iii) i soggetti hanno commesso il reato eludendo fraudolentemente il Modello; (iv) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi, secondo una valutazione che deve necessariamente essere a priori.

L'art. 6 del Decreto dispone, infine, che il Modello di Organizzazione e di Gestione possa essere adottato sulla base di codici di comportamento redatti da associazioni rappresentative di categoria e comunicati al Ministero della Giustizia.

Si precisa che il Modello della Cassa di Risparmio del Veneto S.p.A. è stato predisposto ed aggiornato attenendosi – nel rispetto delle peculiarità dell'attività della Banca e della sua struttura organizzativa – ai principi ed ai contenuti del Modello della Capogruppo Intesa Sanpaolo S.p.A, ed alle Linee Guida redatte dall'ABI, approvate dal stesso Ministero della Giustizia.

Capitolo 2 - Il Modello di organizzazione, gestione e controllo della Cassa di Risparmio del Veneto S.p.A.

2.1 Gli strumenti aziendali esistenti quali presupposti del Modello

Nella predisposizione del presente Modello si è tenuto innanzitutto conto della normativa, delle procedure e dei sistemi di controllo esistenti e già operanti nella Cassa di Risparmio del Veneto S.p.A., in quanto idonei a valere anche come misure di prevenzione di reati e di comportamenti illeciti in genere, inclusi quelli previsti dal D. Lgs. n. 231/2001.

La Cassa di Risparmio del Veneto S.p.A. (di seguito denominata anche "Banca"), rappresenta una realtà complessa, sia sotto il profilo organizzativo che operativo.

Gli organi della Cassa di Risparmio del Veneto S.p.A. hanno dedicato e continuano a dedicare la massima cura nella definizione delle strutture organizzative e delle procedure operative in linea con le direttive della Capogruppo, sia al fine di assicurare efficienza, efficacia e trasparenza nella gestione delle attività e nell'attribuzione delle correlative responsabilità, sia allo scopo di ridurre al minimo disfunzioni, malfunzionamenti ed irregolarità (tra i quali si annoverano anche comportamenti illeciti o comunque non in linea con quanto indicato dalla Banca).

Il contesto organizzativo della Cassa di Risparmio del Veneto S.p.A. è costituito dall'insieme di regole, strutture e procedure che garantiscono il funzionamento della Banca; si tratta dunque di un sistema articolato che viene definito e verificato internamente anche al fine di rispettare le previsioni normative a cui la Cassa di Risparmio del Veneto S.p.A. è sottoposta sia in qualità di banca che di società appartenente al gruppo bancario Intesa Sanpaolo (Testo Unico Bancario, Istruzioni di Vigilanza Banca d'Italia, Testo Unico dell'intermediazione finanziaria e i relativi regolamenti attuativi).

In tale sua qualità la Banca è sottoposta alla vigilanza di Banca d'Italia e di Consob, ognuna per i profili di rispettiva competenza, le quali svolgono verifiche e controlli sull'operato della Banca e su aspetti relativi alla sua struttura organizzativa, come previsto dalla normativa.

In quanto appartenente al gruppo bancario Intesa Sanpaolo, la Banca è inoltre sottoposta all'attività di indirizzo, governo e supporto esercitata dalla Capogruppo ed è tenuta ad osservare le disposizioni emanate dalla stessa nel quadro delle attività di governo delle proprie partecipate.

E' dunque evidente che tale complesso di norme speciali, nonché la sottoposizione all'esercizio costante della vigilanza da parte delle Authority preposte, costituiscono anche un prezioso

strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sull'attività di impresa, anche in relazione ai reati e agli illeciti da prevenire, la Banca ha individuato ed approvato:

- le regole di corporate governance adottate in recepimento della normativa societaria e regolamentare rilevante e delle direttive emanate dalla Capogruppo;
- i regolamenti interni e le policy aziendali;
- il Codice Etico e il Codice interno di comportamento di Gruppo;
- il sistema dei controlli interni;
- il sistema dei poteri e delle deleghe.

Le regole, le procedure e i principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello ma fanno parte del più ampio sistema di organizzazione, gestione e controllo che lo stesso intende integrare e che tutti i soggetti destinatari, sia interni che esterni, sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Banca.

Nei paragrafi che seguono si intendono illustrare, per grandi linee, esclusivamente i principi di riferimento del Codice Etico e del Codice interno di comportamento di Gruppo, il sistema dei controlli interni, nonché il sistema dei poteri e delle deleghe.

2.1.1 Codice Etico e Codice interno di comportamento di Gruppo

A conferma dell'importanza attribuita ai profili etici ed a coerenti comportamenti improntati a rigore e integrità, la Banca recepisce il Codice Etico ed il Codice interno di comportamento di Gruppo adottati da Intesa Sanpaolo S.p.A..

Il Codice Etico rappresenta la "carta costituzionale" del Gruppo Intesa Sanpaolo che, attraverso esso, rende espliciti i fondamenti della propria cultura aziendale e i valori di riferimento dai quali fa derivare regole concrete di comportamento verso tutti i soggetti interni ed esterni (i c.d. "stakeholder"), che hanno direttamente o indirettamente una relazione con la Banca: i clienti, gli azionisti e i collaboratori in primo luogo, ma anche i fornitori, i partner commerciali, la comunità, i territori e l'ambiente in cui il Gruppo opera.

Il Codice interno di comportamento di Gruppo, applicabile a tutte le Società del Gruppo, è costituito da un insieme, volutamente snello, di regole sia di carattere generale – che definiscono le norme essenziali di comportamento degli esponenti aziendali, dei dipendenti e dei collaboratori esterni che, nell'ambito delle loro funzioni, sono tenuti ad esercitare le loro

attività con professionalità, diligenza, onestà e correttezza - sia di carattere più specifico, ad esempio laddove si vietano determinate operazioni personali.

2.1.2 Le caratteristiche salienti del sistema dei controlli interni

La Cassa di Risparmio del Veneto S.p.A., per garantire una sana e prudente gestione, coniuga la profittabilità dell'impresa con un'assunzione dei rischi consapevole e con una condotta operativa improntata a criteri di correttezza.

Pertanto, la Banca, in linea con la normativa di legge e di Vigilanza ed in coerenza con le indicazioni della Capogruppo, si è dotata di un sistema dei controlli interni idoneo a rilevare, misurare e verificare nel continuo i rischi tipici dell'attività sociale.

Il sistema dei controlli interni di Cassa di Risparmio del Veneto S.p.A. è insito nell'insieme di regole, procedure e strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento delle seguenti finalità:

- efficacia ed efficienza dei processi aziendali;
- salvaguardia del valore delle attività e protezione dalle perdite;
- affidabilità e integrità delle informazioni contabili e gestionali;
- conformità delle operazioni con la legge, la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne.

Il sistema dei controlli interni è delineato da un'infrastruttura documentale (impianto normativo) che permette di ripercorrere in modo organico e codificato le linee guida, le procedure, le strutture organizzative, i rischi ed i controlli presenti in azienda, recependo, oltre agli indirizzi aziendali e le indicazioni degli Organi di Vigilanza, anche le disposizioni di Legge, ivi compresi i principi dettati dal D. Lgs. n. 231/2001.

L'impianto normativo è costituito da "Documenti di Governance", tempo per tempo adottati, che sovraintendono al funzionamento della Banca e del Gruppo (Statuto, Codice Etico, Codice interno di comportamento di Gruppo, Regolamento di Gruppo, Regolamento dei Comitati, Regolamento delle operazioni con parti correlate, Facoltà e poteri, Policy, Linee guida, Funzionigrammi delle Strutture Organizzative, Modelli organizzativi, ecc.) e da norme più strettamente operative che regolamentano i processi aziendali, le singole attività e i relativi controlli (Ordini di Servizio, Note di Servizio, Circolari, Guide Operative, Manuali, etc.).

Più nello specifico le regole aziendali disegnano soluzioni organizzative che:

- assicurano una sufficiente separatezza tra le funzioni operative e quelle di controllo ed evitano situazioni di conflitto di interesse nell'assegnazione delle competenze;

- sono in grado di identificare, misurare e monitorare adeguatamente i principali rischi assunti nei diversi segmenti operativi;
- consentono la registrazione di ogni fatto di gestione e, in particolare, di ogni operazione con adeguato grado di dettaglio, assicurandone la corretta attribuzione sotto il profilo temporale;
- assicurano sistemi informativi affidabili e idonee procedure di reporting ai diversi livelli direzionali ai quali sono attribuite funzioni di controllo;
- garantiscono che le anomalie riscontrate dalle unità operative, dalla funzione di revisione interna o da altri addetti ai controlli siano tempestivamente portate a conoscenza di livelli appropriati dell'azienda e gestite con immediatezza.

Inoltre, le soluzioni organizzative aziendali prevedono attività di controllo a ogni livello operativo che consentano l'univoca e formalizzata individuazione delle responsabilità, in particolare nei compiti di controllo e di correzione delle irregolarità riscontrate.

La Banca, in coerenza con le indicazioni degli Organi di Vigilanza, ha individuato le seguenti quattro macro tipologie di controllo:

- **controlli di linea**, diretti ad assicurare il corretto svolgimento dell'operatività quotidiana e delle singole transazioni. Di norma tali controlli sono effettuati dalle strutture produttive (di business o di supporto) o incorporati nelle procedure informatiche, ovvero eseguiti nell'ambito delle attività di back office;
- **controlli sulla gestione dei rischi**, che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione del rischio, di verificare il rispetto dei limiti assegnati alle varie funzioni operative e di controllare la coerenza dell'operatività delle singole strutture produttive con gli obiettivi di rischio rendimento assegnati. Essi sono affidati di norma a strutture diverse da quelle produttive;
- **controlli di conformità**, costituiti da politiche e procedure in grado di individuare, valutare controllare e gestire il rischio conseguente al mancato rispetto di leggi, provvedimenti delle autorità di vigilanza e norme di autoregolamentazione, nonché di qualsiasi altra norma applicabile alla Banca;
- **revisione interna**, volta a individuare andamenti anomali, violazioni delle procedure e della regolamentazione, nonché a valutare la funzionalità del complessivo sistema dei controlli interni. Essa è condotta da strutture diverse e indipendenti da quelle produttive.

Il sistema dei controlli interni è periodicamente soggetto a ricognizione e adeguamento in relazione all'evoluzione dell'operatività aziendale e al contesto di riferimento.

In particolare, il sistema di controlli interni replica gli strumenti e le modalità attualmente in uso presso Intesa Sanpaolo S.p.A.; eccezion fatta per i controlli di linea e gerarchici, il complesso delle attività è accentrato presso le funzioni di controllo della Capogruppo, prevedendosi,

ovviamente, adeguate linee di reporting agli Organi Amministrativi ed al vertice esecutivo della Banca. In sostanza il sistema di controlli interni adottato dalla Banca prevede che i controlli di linea siano svolti dalle strutture della Cassa di Risparmio del Veneto S.p.A.; la gestione, la misurazione e il controllo dei rischi di credito, finanziari ed operativi siano svolti in outsourcing dalle strutture di Capogruppo; i controlli di audit siano accentrati e svolti dalla Capogruppo in tale veste. Supportano tale scelta le indicazioni contenute nelle disposizioni di Vigilanza che prevedono la possibilità – nell'ambito delle strategie di gruppo – di accentrare la funzione di Internal Audit e di Compliance presso una delle banche del gruppo stesso.

2.1.3 Il sistema dei poteri e delle deleghe

A norma di Statuto, il Consiglio di Amministrazione è investito di tutti i poteri per l'ordinaria e straordinaria amministrazione della Banca.

Inoltre il Consiglio di Amministrazione ha definito l'ambito dei poteri deliberativi e di spesa conferiti al Direttore Generale, in coerenza con le responsabilità organizzative e gestionali attribuite, predeterminandone i limiti e fissando altresì modalità e limiti per l'esercizio delle subdeleghe.

La facoltà di subdelega viene esercitata attraverso un processo trasparente, sempre monitorato, graduato in funzione del ruolo e della posizione ricoperta dal "subdelegato", comunque prevedendo sempre l'obbligo di informativa alla funzione delegante.

Sono inoltre formalizzate le modalità di firma sociale per atti, contratti, documenti e corrispondenza, sia esterna che interna e le relative facoltà sono attribuite ai dipendenti in forma abbinata o singola, a seconda del carattere della documentazione stessa.

Tutte le Strutture operano sulla base di uno specifico Regolamento, che definisce i rispettivi ambiti di competenza e di responsabilità; tale Regolamento è diffuso in modo capillare all'interno della Banca.

Anche le procedure operative, che regolano le modalità di svolgimento dei diversi processi aziendali, sono diramate all'interno della Banca attraverso specifica normativa.

Pertanto i principali processi decisionali ed attuativi riguardanti l'operatività della Banca sono codificati, monitorabili e conoscibili da tutta la struttura.

2.2 Le finalità perseguite con l'adozione del Modello

Nonostante gli strumenti aziendali illustrati nei paragrafi precedenti risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, la Banca ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del Decreto, nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Banca, affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei reati e degli illeciti amministrativi previsti dalla normativa di riferimento.

In particolare, attraverso l'adozione ed il costante aggiornamento del Modello, la Banca si propone di perseguire le seguenti principali finalità:

- determinare, in tutti coloro che operano per conto della Banca nell'ambito di "attività sensibili" (ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto), la consapevolezza di poter incorrere, in caso di violazione delle disposizioni impartite in materia, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative irrogabili nei loro stessi confronti;
- ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse (anche nel caso in cui la Banca fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Banca, in linea con la Capogruppo, intende attenersi nell'esercizio dell'attività aziendale;
- consentire alla Banca, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello.

2.3 Gli elementi fondamentali del Modello

Il Modello della Cassa di Risparmio del Veneto S.p.A. è stato predisposto in coerenza con la volontà del Legislatore, tenuto conto delle linee guida emanate dall'ABI e dei criteri e delle linee guida utilizzati da Capogruppo nella redazione del proprio Modello.

Gli elementi fondamentali sviluppati nella definizione del Modello possono essere così brevemente riassunti:

- individuazione delle aree di attività a rischio ovvero delle attività aziendali sensibili nel cui ambito potrebbero configurarsi le ipotesi di reato da sottoporre ad analisi e monitoraggio;
- gestione di processi operativi in grado di garantire:

- la separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- una chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
- corrette modalità di svolgimento delle attività medesime;
- la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali o informatici;
- processi decisionali legati a predefiniti criteri oggettivi (es.: esistenza di albi fornitori, esistenza di criteri oggettivi di valutazione e selezione del personale, ecc.);
- l'esistenza e la tracciabilità delle attività di controllo e supervisione compiute sulle transazioni aziendali;
- la presenza di meccanismi di sicurezza in grado di assicurare un'adeguata protezione/accesso fisico-logico ai dati e ai beni aziendali;

- emanazione di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;
- definizione delle responsabilità nell'adozione, modifica, attuazione e controllo del Modello stesso;
- identificazione dell'Organismo di Vigilanza e attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell'Organismo di Vigilanza;
- definizione e applicazione di disposizioni idonee a sanzionare il mancato rispetto delle misure indicate nel Modello;
- formazione del personale e comunicazione interna in merito al contenuto del Decreto e del Modello ed agli obblighi che ne conseguono.

2.4 La Struttura del Modello

Nel definire il presente "Modello di organizzazione, gestione e controllo" la Cassa di Risparmio del Veneto S.p.A. ha adottato un approccio che ha consentito di utilizzare ed integrare nel Modello stesso le regole e la normativa interna esistenti sulla base della mappatura delle aree e attività sensibili effettuata in occasione dell'adozione del Modello e dei suoi successivi aggiornamenti.

.

Si ricorda infatti che il Consiglio di Amministrazione della Banca, con delibera in data 22 dicembre 2006, approvò i "Principi di riferimento per l'adozione dei modelli di organizzazione, gestione e controllo", successivamente aggiornati ed integrati con delibera del 18 dicembre 2008

Sono state così identificate, per ciascuna categoria di "illeciti presupposto", le aree aziendali "sensibili". Nell'ambito di ogni area sensibile sono state poi individuate le attività aziendali nello svolgimento delle quali è più verosimile il rischio della commissione di illeciti presupposto previsti dal Decreto (c.d. attività "sensibili"), codificando per ciascuna di dette attività principi di comportamento e di controllo - diversificati in relazione allo specifico rischio-reato da prevenire - cui devono attenersi tutti coloro che vi operano.

Il Modello trova poi piena ed efficace attuazione nella realtà della Banca attraverso il collegamento di ciascuna attività "sensibile" con le strutture aziendali coinvolte e con la gestione dinamica dei processi e della relativa normativa interna di riferimento, che deve basarsi sui principi di comportamento e di controllo enunciati per ciascuna di dette attività.

L'approccio seguito:

- consente di valorizzare al meglio il patrimonio conoscitivo già esistente in azienda in termini di politiche, regole e normative interne che indirizzano e governano la formazione e l'attuazione delle decisioni della Banca in relazione agli illeciti da prevenire e, più in generale, la gestione dei rischi e l'effettuazione dei controlli;
- permette di gestire con criteri univoci le regole operative aziendali, incluse quelle relative alle aree "sensibili";
- rende più agevole la costante implementazione e l'adeguamento tempestivo dei processi e dell'impianto normativo interni ai mutamenti della struttura organizzativa e dell'operatività aziendale, assicurando un elevato grado di "dinamicità" del Modello, soprattutto in una fase, come quella attuale, di continuo cambiamento dovuto all'integrazione organizzativa e operativa.

Nella Cassa di Risparmio del Veneto S.p.A. il presidio dei rischi rivenienti dal regime di responsabilità introdotto dal D. Lgs. n. 231/2001 è pertanto assicurato:

- dal presente documento ("Modello di organizzazione, gestione e controllo"), e
- dall'impianto normativo esistente, che ne costituisce parte integrante e sostanziale.

Il "Modello di organizzazione, gestione e controllo" delinea in particolare:

- il contesto normativo di riferimento;

- il ruolo e la responsabilità delle strutture coinvolte nell'adozione, efficace attuazione e modificazione del Modello;
- gli specifici compiti e responsabilità dell' Organismo di Vigilanza;
- i flussi informativi verso l'Organismo di Vigilanza;
- il sistema sanzionatorio;
- le logiche formative;
- le aree "sensibili" in relazione alle fattispecie di illecito di cui al Decreto;
- le attività aziendali nell'ambito delle quali può verificarsi il rischio di commissione degli illeciti presupposto ed i principi di comportamento e le regole di controllo volti a prevenirli (attività "sensibili").

L'impianto normativo della Banca, costituito dai "Documenti di Governance" (Statuto, Codice Etico, Codice interno di comportamento di Gruppo, Regolamenti, Policy, ecc.), Ordini di Servizio, Note di Servizio, Circolari, Manuali, Guide Operative e altri strumenti, regolamenta ai vari livelli l'operatività della Banca nelle aree/attività "sensibili" e costituisce a tutti gli effetti parte integrante del Modello.

L'impianto normativo è contenuto e catalogato, con specifico riferimento ad ogni attività "sensibile", in un apposito repository documentale, diffuso all'interno di tutta la Banca tramite la rete Intranet aziendale e costantemente aggiornato a cura delle funzioni competenti in coerenza con l'evolversi dell'operatività.

Pertanto, dall'associazione dei contenuti del Modello con l'impianto normativo aziendale è possibile estrarre, per ciascuna delle attività "sensibili", specifici, puntuali e sempre aggiornati Protocolli che descrivono fasi di attività, strutture coinvolte, principi di controllo e di comportamento, regole operative di processo e che consentono di rendere verificabile e congrua ogni fase di attività.

2.5 I destinatari del Modello

Il Modello e le disposizioni ivi contenute e richiamate devono essere rispettate dagli esponenti aziendali e da tutto il personale della Cassa di Risparmio del Veneto S.p.A. e, in particolare, da parte di coloro che si trovino a svolgere le attività sensibili.
La formazione del personale e l'informazione interna sul contenuto del Modello vengono costantemente assicurati con le modalità meglio descritte al successivo Capitolo 6.

Al fine di garantire l'efficace ed effettiva prevenzione dei reati, il Modello è destinato anche ai soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) che, in forza di rapporti contrattuali, prestino la loro collaborazione alla Banca per la realizzazione delle sue attività. Nei confronti dei medesimi il rispetto del Modello è garantito mediante l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi del Modello ed a segnalare all'Organismo di Vigilanza eventuali notizie della commissione di illeciti o della violazione del Modello.

2.6. Adozione, efficace attuazione e modificazione del Modello – Ruoli e responsabilità

Adozione del Modello

L'adozione e l'efficace attuazione del Modello costituiscono, ai sensi dell'art. 6, comma I, lett. a) del Decreto, atti di competenza e di emanazione del **Consiglio di Amministrazione** che approva, mediante apposita delibera, il Modello, su proposta del Direttore Generale.

Il Direttore Generale definisce, anche nel suo ruolo di Datore di Lavoro ai sensi del D. Lgs. n. 81/2008, la struttura del Modello da sottoporre all'approvazione del Consiglio di Amministrazione con il supporto, per gli ambiti di rispettiva competenza, delle funzioni Compliance, Internal Audit, Affari Societari e Partecipazioni, Risorse Umane di Capogruppo e della funzione Organizzazione di ISGS, e sentito il parere dell'Organismo di Vigilanza

Efficace attuazione e modificazione del Modello

E' cura del Consiglio di Amministrazione (o di soggetto da questi formalmente delegato) provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'Organo amministrativo si avvale del supporto dell'Organismo di Vigilanza.

Il Consiglio di Amministrazione delega le singole strutture a dare attuazione ai contenuti del Modello ed a curare il costante aggiornamento e implementazione della normativa interna e dei processi aziendali, che costituiscono parte integrante del Modello, nel rispetto dei principi di controllo e di comportamento definiti in relazione ad ogni attività sensibile. Delle modifiche intervenute nei processi e nella normativa aziendale in questione verrà data idonea informativa con cadenza semestrale al Consiglio di Amministrazione e all'Organismo di Vigilanza.

L'efficace e concreta attuazione del Modello è garantita altresì:

- dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole unità organizzative nelle aree sensibili;

- dai responsabili delle varie Unità Organizzative della Banca e/o di Capogruppo in relazione alle attività a rischio dalle stesse svolte.

Il Consiglio di Amministrazione deve inoltre garantire, anche attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendessero necessarie nel futuro.

Specifici ruoli e responsabilità nella gestione del Modello sono inoltre attribuiti alle strutture di seguito indicate.

Funzione Internal Audit

La funzione Internal Audit di Capogruppo assicura in generale una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali.

La funzione Internal Audit supporta direttamente l'Organismo di Vigilanza nel vigilare sule rispetto e sull'adeguatezza delle regole contenute nel Modello, attivando, a fronte delle eventuali criticità riscontrate nel corso della propria attività, le funzioni di volta in volta competenti per le opportune azioni di mitigazione.

Funzione Compliance

La funzione Compliance di Capogruppo è competente a garantire, nel tempo, la presenza di regole, procedure e prassi operative che prevengano efficacemente violazioni o infrazioni alle norme vigenti.

Con specifico riferimento ai rischi di responsabilità amministrativa introdotti dal Decreto, la funzione Compliance di Capogruppo supporta l'Organo di Vigilanza nello svolgimento delle sue attività di controllo mediante:

- la definizione e l'aggiornamento del Modello, congiuntamente alla funzione Organizzazione, e al Datore di lavoro ai sensi del D. Lgs. n. 81/2008, per quanto di competenza in coerenza all'evoluzione della normativa di riferimento ed alle modifiche della struttura organizzativa aziendale e con il supporto della funzione Legale e Contenzioso di Capogruppo per quanto concerne l'interpretazione della normativa, la risoluzione di questioni di diritto e l'identificazione delle condotte che possono configurare ipotesi di reato;

- il monitoraggio nel tempo in merito alla efficacia del Modello, con riferimento alle regole e principi di comportamento per la prevenzione dei reati sensibili; a tal fine la Funzione Compliance:
  - individua annualmente i processi ritenuti a maggior grado di rischiosità in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all'esistenza o meno di specifici presidi a mitigazione del relativo rischio; per i processi individuati la funzione di conformità provvede al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta applicazione dei principi di controllo e di comportamento previsti dal Modello; procede altresì, con un approccio risk based, all'effettuazione di specifiche attività di assurance volte a valutare la conformità dei processi ai "protocolli" previsti dal Modello;
  - analizza le risultanze del processo di autovalutazione e attestazione delle unità organizzative circa il rispetto dei principi di controllo e comportamento prescritti nel Modello;
- l'esame dell'informativa proveniente dalla funzione Internal Audit in merito alle criticità riscontrate nel corso della propria attività di verifica.

Funzione Affari Societari e Partecipazioni

La funzione Affari Societari e Partecipazioni, in coerenza con il suo ruolo istituzionale, ha la responsabilità sia di assicurare consulenza ed assistenza con specifico riferimento alle caratteristiche ed alle attività dell'Organismo di Vigilanza sia di segnalare ai competenti Organi societari, in caso di operazioni societarie o di altra natura che modifichino l'ambito di operatività della Società, l'esigenza di modificare il Modello per tenere conto della nuova situazione.

Funzione Organizzazione

La funzione Organizzazione di ISGS Intesa Sanpaolo Group Services S.c.p.a., al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di governance rispetto agli obiettivi perseguiti col Modello, ha la responsabilità di:

- progettare la struttura organizzativa, definendone missioni, organigrammi e funzioni, al fine di sottoporla all'approvazione del Direttore Generale;
- definire le regole per il disegno, l'ufficializzazione e la gestione dei processi organizzativi;
- supportare la progettazione dei processi organizzativi ovvero validare procedure definite da altre funzioni, garantendone la coerenza con il disegno organizzativo complessivo;
- identificare, per ogni processo aziendale sensibile, l'Unità Organizzativa prevalente responsabile dell'autodiagnosi e dei flussi informativi destinati all'Organismo di Vigilanza;

- collaborare con le Unità Organizzative, con le funzioni Internal Audit, Compliance, Legale e Contenzioso, con il Datore di lavoro ai sensi del D. Lgs. n. 81/2008 e con le altre funzioni aziendali interessate, ognuna per il proprio ambito di competenza, all'adeguamento del sistema normativo e del Modello (a seguito di modifiche nella normativa applicabile, nell'assetto organizzativo aziendale e/o nelle procedure operative, rilevanti ai fini del Decreto);
- diffondere la normativa interna a tutta la struttura della Banca attraverso la rete Intranet aziendale.

Funzione Risorse Umane

Con riferimento al Decreto, la funzione Risorse Umane di Capogruppo, come in dettaglio illustrato al Capitolo 5 ed al Capitolo 6:

- programma piani di formazione e interventi di sensibilizzazione rivolti a tutti i dipendenti sull'importanza di un comportamento conforme alle regole aziendali, sulla comprensione dei contenuti del Modello, del Codice interno di comportamento e del Codice Etico, nonché specifici corsi destinati al personale che opera nelle aree sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio;
- presidia, con il supporto delle funzioni Compliance, Internal Audit e Legale, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio e, a sua volta, fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del Decreto all'Organismo di Vigilanza, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

Unità Organizzative

Alle Unità Organizzative è assegnata la responsabilità dell'esecuzione, del buon funzionamento e della efficace applicazione nel tempo dei processi. La normativa interna individua le Unità Organizzative cui è assegnata la responsabilità della progettazione dei processi.

Agli specifici fini del Decreto, le Unità Organizzative hanno la responsabilità di:

- rivedere - alla luce dei principi di comportamento e di controllo prescritti per la disciplina delle attività sensibili - le prassi ed i processi di propria competenza, al fine di renderli adeguati a prevenire comportamenti illeciti;

- segnalare all'Organismo di Vigilanza eventuali situazioni di irregolarità o comportamenti anomali.

In particolare, le Unità Organizzative per le attività aziendali sensibili devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio ad eventuali carenze di normative o di procedure che potrebbero dar luogo a prevedibili rischi di commissione di "illeciti presupposto" nell'ambito delle attività di propria competenza.

Datore di lavoro ai sensi del D. Lgs. n. 81/2008

Il Datore di Lavoro ai sensi del D. Lgs. n. 81/2008, limitatamente alla gestione dei rischi in materia di sicurezza e salute sul lavoro:

- partecipa alla definizione della struttura del Modello ed all'aggiornamento dello stesso;
- individua e valuta l'insorgenza di fattori di rischio dai quali possano derivare le commissioni di illeciti presupposto;
- promuove le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di non conformità.

2.7 Attività oggetto di outsourcing

Il Modello Organizzativo della Cassa di Risparmio del Veneto S.p.A. prevede l'esternalizzazione (di seguito anche "outsourcing") presso la Capogruppo Intesa Sanpaolo S.p.A. e/o altre Società del Gruppo di una parte delle attività amministrative e di back office della Cassa di Risparmio del Veneto S.p.A. nonché di quelle di supporto all'attività commerciale, ivi compresa la revisione/istruttoria delle pratiche di fido al di sopra di determinati livelli di facoltà.

In particolare, la gestione operativa di tutte le attività inerenti all'organizzazione, alla sicurezza, agli immobili, agli acquisti, ai servizi operativi, ai sistemi informativi e ai servizi di Contact Unit è affidata a ISGS Intesa Sanpaolo Group Services S.C.p.A..

L'affidamento in outsourcing di tali attività è realizzato in conformità alle prescrizioni delle competenti Autorità di Vigilanza ed è formalizzato attraverso la stipula di specifici contratti che assicurano alla Cassa di Risparmio del Veneto S.p.A.:

- di assumere ogni decisione nel rispetto della propria autonomia, mantenendo la necessaria responsabilità su tutte le attività, ivi comprese quelle relative ai servizi esternalizzati;
- di mantenere conseguentemente la capacità di controllo circa la congruità dei servizi resi in outsourcing da Capogruppo Intesa Sanpaolo S.p.A. e/o altre Società del Gruppo.

In particolare, tali contratti prevedono:

- una descrizione dettagliata delle attività esternalizzate;
- le modalità di erogazione dei servizi;
- gli specifici livelli di servizio;
- i poteri di verifica e controllo spettanti alla Banca;
- le modalità di tariffazione dei servizi resi;
- idonei sistemi di reporting;
- adeguati presidi a tutela del patrimonio informativo della Banca e della sicurezza delle transazioni
- l'obbligo dell'outsourcer di operare in conformità alle leggi ed ai regolamenti vigenti nonché di esigere l'osservanza delle leggi e dei regolamenti anche da parte di terzi ai quali si dovesse rivolgere per lo svolgimento delle attività esternalizzate;
- la facoltà per Cassa di Risparmio del Veneto S.p.A. di risolvere il contratto in caso di violazione da parte dell'outsourcer: (i) delle norme legislative e delle disposizioni impartite dall'Autorità di Vigilanza che possano comportare sanzioni a carico del committente; (ii) dell'obbligo di dare esecuzione all'attività nel rispetto dei principi contenuti del Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001 adottato dalla Cassa di Risparmio del Veneto S.p.A. nonché del Codice Etico e del Codice interno di comportamento di Gruppo.

Apposite strutture della Banca verificano nel continuo, anche tramite il controllo dei previsti livelli di servizio, il rispetto delle clausole contrattuali e, di conseguenza, l'adeguatezza delle attività prestate dall'outsourcer (Capogruppo Intesa Sanpaolo S.p.A. e/o altre Società del Gruppo).

Non sono regolate da contratti di outsourcing le attività svolte istituzionalmente dalla Capogruppo in tale sua qualità, tra cui quelle finalizzate a definire le linee strategiche del Gruppo e delle Società che lo compongono e volte a garantire l'uniformità nei processi e nelle azioni.

Come già anticipato, per quanto concerne il sistema di controlli interni, in attuazione della facoltà al riguardo prevista nelle Istruzioni di Vigilanza della Banca d'Italia, lo svolgimento della funzione di Internal Audit e di Compliance è stato accentrato presso la Capogruppo.

2.8 Il ruolo di Capogruppo

Ferma restando l'autonoma responsabilità di ciascuna Società appartenente al Gruppo Intesa Sanpaolo in ordine all'adozione ed all'efficace attuazione di un proprio Modello ai sensi del Decreto, Intesa Sanpaolo, nell'esercizio della sua peculiare funzione di Capogruppo, ha il potere di impartire criteri e direttive di carattere generale e di verificare mediante le funzioni Compliance, Internal Audit e Affari Societari e Partecipazioni, la rispondenza dei Modelli delle società appartenenti al Gruppo a tali criteri e direttive.

2.8.1 Principi di indirizzo di Gruppo in materia di Responsabilità amministrativa degli Enti

Allo scopo di uniformare a livello di Gruppo le modalità attraverso cui recepire ed attuare i contenuti del Decreto predisponendo modalità di presidio del rischio adeguate, vengono di seguito delineati i principi di indirizzo definiti da Capogruppo, a cui tutte le società di diritto italiano, e quindi anche la Cassa di Risparmio del Veneto, devono attenersi, nel rispetto della propria autonomia giuridica e dei principi di corretta gestione societaria.
In particolare, ciascuna società interessata deve:

- adottare il proprio Modello, dopo aver individuato le attività aziendali che presentano un rischio di commissione degli illeciti previsti dal Decreto e le misure più idonee a prevenirne la realizzazione. Nella predisposizione del Modello la società deve attenersi ai principi e ai contenuti del Modello di Capogruppo salvo che sussistano situazioni specifiche relative alla natura, dimensione o al tipo di attività esercitata nonché alla struttura societaria, all'organizzazione e/o all'articolazione delle deleghe interne che impongano o suggeriscano l'adozione di misure differenti al fine di perseguire più efficacemente gli obiettivi del Modello, nel rispetto comunque dei predetti principi nonché di quelli espressi nel Codice Etico e nel Codice interno di comportamento di Gruppo.
  In presenza di rilevanti difformità rispetto ai principi e ai contenuti del Modello di Capogruppo devono essere trasmesse alla funzione Compliance di Capogruppo le ragioni che le hanno motivate, nonché la bozza finale del Modello prima della sua approvazione da parte degli Organi Sociali.
  L'avvenuta adozione del Modello è comunicata dalla società alla predetta funzione di conformità mediante trasmissione di copia del medesimo e della delibera di approvazione da parte del Consiglio di Amministrazione.
  Resta fermo che fino a che il Modello non sia approvato, la società adotta ogni misura idonea per la prevenzione dei comportamenti illeciti;

- provvedere tempestivamente alla nomina dell'Organismo di Vigilanza, in linea con le indicazioni fornite dalla Capogruppo in relazione ai soggetti da nominare.
  L'informativa di avvenuta nomina dell'Organismo è comunicata, mediante trasmissione di copia della delibera del Consiglio di Amministrazione, alla funzioni di Capogruppo, Compliance e Affari Societari e Partecipazioni di Capogruppo; la funzione Affari Societari e Partecipazioni fornisce periodica informativa di aggiornamento al riguardo all'Organismo di Vigilanza di Capogruppo;

- assicurare il sistematico aggiornamento del Modello in funzione di modifiche normative e organizzative, nonché nel caso in cui significative e/o ripetute violazioni delle prescrizioni del Modello lo rendessero necessario. Le modifiche normative sono segnalate alla società dalla funzione Compliance di Capogruppo con apposita comunicazione. L'avvenuto aggiornamento del Modello è comunicato alla predetta funzione Compliance con le modalità sopra illustrate;

- predisporre, coordinandosi con le funzioni Personale e Compliance di Capogruppo, piani di formazione e di comunicazione rivolti indistintamente a tutto il Personale nonché interventi specifici di formazione destinati a figure impegnate in attività maggiormente sensibili al Decreto, con l'obiettivo di creare una conoscenza diffusa e una cultura aziendale adeguata in materia;

- adottare un idoneo presidio dei processi sensibili al Decreto che preveda la loro identificazione, documentazione e pubblicazione all'interno del sistema normativo aziendale. Inoltre, tra i processi sensibili devono essere individuati annualmente, dalla funzione di conformità della società, con un approccio risk based, quelli ritenuti a maggior grado di rischiosità in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all'esistenza o meno di specifici presidi a mitigazione del relativo rischio. Per tali processi la funzione di conformità provvede:
  - al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta applicazione dei principi di controllo e di comportamento previsti dal Modello,
  - all'effettuazione di specifiche attività di assurance volte a valutare la conformità dei processi ai "protocolli" previsti dal Modello;

- avviare, con cadenza annuale, il processo di autodiagnosi sulle attività svolte al fine di attestare il livello di attuazione del Modello, con particolare attenzione al rispetto dei principi di

controllo e comportamento e delle norme operative. L'attivazione del processo di autodiagnosi viene effettuato coordinandosi con le funzioni Risk Management e Compliance di Capogruppo;

- fornire alla funzione Compliance di Capogruppo copia delle relazioni periodiche, comprensive anche delle risultanze del processo di autodiagnosi, presentate dalla funzione di conformità all'Organismo di Vigilanza.

L'Organismo di Vigilanza della società provvede inoltre a trasmettere all'Organismo di Vigilanza di Capogruppo la relazione periodica, di norma semestrale, sull'attività svolta presentata al Consiglio di Amministrazione, corredandola con le eventuali osservazioni del Consiglio stesso.

Con riferimento alle attività sopra illustrate, le competenti funzioni di Capogruppo forniscono alle società supporto e collaborazione, per quanto di rispettiva competenza, nell'espletamento dei compiti alle stesse spettanti.

In ottemperanza alle Linee guida di compliance di Gruppo, per la Cassa di Risparmio del Veneto, la cui operatività è connotata da un elevato livello di integrazione con la Capogruppo, le attività di presidio della conformità in materia di responsabilità amministrativa degli Enti sono accentrate presso la funzione Compliance di Capogruppo, fermo restando che la competenza e la responsabilità per l'approvazione e l'efficace attuazione del Modello e per la nomina dell'Organismo di Vigilanza restano in capo alla Cassa di Risparmio del Veneto. Sono in capo alla Cassa le seguenti attività:

- iter di formalizzazione ed approvazione del Modello presso i competenti Organi sociali;
- supporto alla Capogruppo nell'acquisizione delle informazioni necessarie all'identificazione delle aree e delle attività sensibili specifiche della società;
- archiviazione e conservazione della documentazione concernente i risultati dell'autodiagnosi e delle rendicontazioni predisposte agli Organi sociali;
- trasmissione alla funzione Compliance di Capogruppo di copia dell'avviso di convocazione delle riunioni dell'Organismo di Vigilanza e delle riunioni degli Organi Sociali qualora all'ordine del giorno rientrino argomenti connessi al Decreto.

Capitolo 3 - L'Organismo di Vigilanza

3.1 Individuazione dell'Organismo di Vigilanza

Ai sensi del Decreto, il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere affidato ad un organismo interno all'Ente dotato di autonomi poteri di iniziativa e di controllo (l'"Organismo di Vigilanza").

Le attribuzioni ed i poteri dell'Organismo di Vigilanza (di seguito, anche l'"Organismo") sono conferiti ad un organo collegiale nominato dal Consiglio di Amministrazione e avente caratteristiche di autonomia, indipendenza, professionalità e continuità di azione necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate. Dell'avvenuta nomina dell'Organismo è data formale comunicazione a tutti i livelli aziendali.
L'Organismo di Vigilanza è dotato di poteri di iniziativa e di controllo sulle attività della Società, senza disporre di poteri gestionali e/o amministrativi. Inoltre, onde poter svolgere, in assoluta indipendenza, le proprie funzioni, dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal Consiglio di Amministrazione, su proposta dell'Organismo stesso.

Il funzionamento dell'Organismo di Vigilanza è disciplinato da un apposito Regolamento, approvato dal medesimo.

L'Organismo di Vigilanza si avvale ordinariamente delle strutture della Società per l'espletamento dei suoi compiti di vigilanza e controllo ed in primis della Funzione Internal Audit, struttura istituzionalmente dotata di competenze tecniche e risorse, umane e operative, idonee a garantire lo svolgimento su base continuativa delle verifiche, delle analisi e degli altri adempimenti necessari. Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, può inoltre avvalersi di consulenti esterni.

Per quanto concerne in particolare la materia della tutela della salute e della sicurezza sul luogo di lavoro, l'Organismo potrà avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti (Responsabile del Servizio Prevenzione e Protezione, Rappresentante dei Lavoratori per la sicurezza, Medico competente, ecc.), nonché di quelle previste dalle normative di settore, quali, ad esempio, il D. Lgs. n. 81/2008.

L'Organismo di Vigilanza, direttamente o per il tramite delle varie strutture aziendali all'uopo designate, ha accesso a tutte le attività svolte dalla Società e alla relativa documentazione, sia presso gli uffici centrali sia presso le strutture periferiche.

3.2 Composizione, durata e compensi dell'Organismo di Vigilanza

L'Organismo di Vigilanza è composto da tre membri effettivi, individuati come segue:

- un Amministratore indipendente e non esecutivo, ovvero un Sindaco effettivo qualora nessuno degli amministratori possieda entrambi i suddetti requisiti;
- il Responsabile della Funzione Internal Audit della Società, ovvero, nel caso in cui detta attività sia svolta in outsourcing dalla Capogruppo, il Responsabile dell'Unità organizzativa di Capogruppo (Servizio od Ufficio) che cura le attività di Internal Audit;
- un professionista esterno in possesso di adeguate competenze specialistiche (quali meglio specificate infra).

L'Organismo nomina al proprio interno il Presidente.

Al fine di assicurare l'operatività dell'Organismo di Vigilanza anche nei casi di sospensione ovvero di temporaneo impedimento di un componente, il Consiglio di Amministrazione nomina altresì un componente supplente, da individuarsi fra i Sindaci supplenti, che subentra al componente effettivo che si venga a trovare in una delle predette situazioni.

L'Organismo di Vigilanza resta in carica per la durata stabilita dal Consiglio di Amministrazione all'atto della nomina; in assenza di una specifica determinazione, l'Organismo di Vigilanza dura in carica per tutto il periodo in cui resta in carica il Consiglio di Amministrazione che lo ha nominato. La revoca dei componenti - fatti salvi i casi infra previsti - può avvenire unicamente nel caso di rilevanti inadempimenti nell'assolvimento dei loro compiti.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o decadenza, la maggioranza dei componenti. In tal caso il Consiglio di Amministrazione provvede tempestivamente a nominare i nuovi membri.

Il Consiglio di Amministrazione delibera il compenso spettante ai componenti dell'Organismo di Vigilanza per lo svolgimento delle relative funzioni, stabilendo altresì il compenso spettante al membro supplente dell'Organismo stesso, sotto forma di emolumento fisso in ragione della sua partecipazione alle riunioni.

Ai membri – effettivi e supplente – compete altresì il rimborso delle spese vive e documentate sostenute per intervenire alle riunioni.

3.3 Requisiti di eleggibilità, cause di decadenza e sospensione

3.3.1 Requisiti di professionalità, onorabilità ed indipendenza

Fermo restando per quanto riguarda l'amministratore o il sindaco (e il membro supplente) il possesso dei requisiti disposti dalla disciplina legale e regolamentare applicabile alla Società, gli altri membri dell'Organismo dovranno possedere i requisiti di onorabilità previsti per gli esponenti aziendali delle banche.

In aggiunta a quanto sopra:

- l'amministratore non deve essere destinatario di deleghe esecutive e deve possedere i seguenti requisiti di indipendenza: i) non essere stretto familiare degli amministratori della Società; ii) non rivestire la carica di amministratore della Capogruppo o di presidente o amministratore esecutivo in una società controllata dalla Società o sottoposta a comune controllo; iii) non essere legato alla Società od alle società da questa controllate o alle società che la controllano o a quelle sottoposte a comune controllo da un rapporto di lavoro o da un rapporto continuativo di consulenza o di prestazione d'opera retribuita ovvero da altri rapporti di natura patrimoniale che ne compromettano l'indipendenza. Laddove nessuno degli amministratori abbia i predetti requisiti, viene nominato un sindaco effettivo;
- il professionista esterno deve essere scelto tra esperti (quali, ad esempio, docenti o liberi professionisti) in materie giuridiche, economiche, finanziarie o tecnico-scientifiche ovvero tra magistrati in quiescenza o comunque tra soggetti in possesso di competenze specialistiche adeguate alla funzione derivanti, ad esempio, dall'aver svolto per un congruo periodo di tempo attività professionali in materie attinenti al settore nel quale la Società opera e/o dall'avere una adeguata conoscenza dell'organizzazione e dei principali processi aziendali;
- il professionista esterno non deve avere vincoli di parentela con gli esponenti o con i top manager della Società, né deve essere legato a quest'ultima, alla sua controllante o a

società facenti parte del medesimo gruppo da rapporti di lavoro autonomo o subordinato, ovvero da altri rapporti significativi di natura professionale o patrimoniale che ne compromettano l'indipendenza.

In aggiunta al possesso dei requisiti sopra richiamati i membri effettivi ed il membro supplente dovranno essere in possesso dei seguenti ulteriori **requisiti di onorabilità**, secondo i quali non possono essere eletti componenti dell'Organismo di Vigilanza coloro i quali:

- siano stati condannati, con sentenza irrevocabile o con sentenza non definitiva anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno dei reati tra quelli per i quali è applicabile il D. Lgs. n. 231/2001. Per sentenza di condanna si intende anche quella pronunciata ai sensi dell'art. 444 c.p.p.;
- abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- abbiano subito l'applicazione delle sanzioni amministrative accessorie previste dall'art. 187-quater del D. Lgs. n. 58/1998.

3.3.2 Verifica dei requisiti

L'Organismo di Vigilanza verifica, entro 30 giorni dalla nomina, la sussistenza, in capo ai propri componenti effettivi ed al membro supplente, dei requisiti ulteriori a quelli previsti dalla disciplina legale e regolamentare, sulla base di una dichiarazione resa dai singoli interessati, comunicando l'esito di tale verifica al Consiglio di Amministrazione.

3.3.3 Cause di decadenza

I componenti effettivi e supplenti dell'Organismo di Vigilanza, successivamente alla loro nomina, **decadono da tale carica**, qualora:

- se Consigliere di Amministrazione (o Sindaco) della Società, incorra nella revoca o decadenza da tale carica, anche in conseguenza del venir meno dei requisiti di professionalità, onorabilità e indipendenza prescritti dalla legge o dallo Statuto;
- dopo la nomina, si accerti che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento

definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- siano stati condannati, con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.), anche se a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. per uno dei reati tra quelli per i quali è applicabile il D. Lgs. n. 231/2001;
- subiscano l'applicazione in via definitiva delle sanzioni amministrative accessorie previste dall'art. 187-quater del D. Lgs. n. 58/1998.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause sopra elencate di decadenza.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una causa di decadenza, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Consigliere (o di sindaco), convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'interessato dalla carica di componente dell'Organismo di Vigilanza ed alla sua sostituzione.

In caso di decadenza di un membro supplente subentrerà automaticamente l'altro sindaco supplente.

3.3.4 Cause di sospensione

Costituiscono **cause di sospensione** dalla funzione di componente dell'Organismo di Vigilanza quelle che, ai sensi della vigente normativa di legge e regolamentare, comportano la sospensione dalla carica di Consigliere di Amministrazione ovvero di Sindaco, nonché le ulteriori di seguito riportate:

- si accerti, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- i componenti dell'Organismo di Vigilanza siano stati condannati con sentenza non definitiva, anche a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.) per uno dei reati tra quelli per i quali è applicabile il D. Lgs. n. 231/2001.

In tali casi il Consiglio di Amministrazione dispone la sospensione della qualifica di membro dell'Organismo di Vigilanza e la cooptazione ad interim con il membro supplente.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause di sospensione di cui sopra.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una delle cause di sospensione dianzi citate, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Consigliere (o di sindaco), convoca senza indugio il Consiglio di Amministrazione affinché provveda, nella sua prima riunione successiva, a dichiarare la sospensione del soggetto, nei cui confronti si è verificata una delle cause di cui sopra, dalla carica di componente dell'Organismo di Vigilanza. In tal caso subentra ad interim il membro supplente.

Fatte salve diverse previsioni di legge e regolamentari, la sospensione non può durare oltre sei mesi, trascorsi i quali il Presidente del Consiglio di Amministrazione iscrive l'eventuale revoca fra le materie da trattare nella prima riunione del Consiglio successiva a tale termine. Il componente non revocato è reintegrato nel pieno delle funzioni.

Qualora la sospensione riguardi il Presidente dell'Organismo di Vigilanza, la presidenza è assunta, per tutta la durata della medesima, dal componente più anziano di nomina o, a parità di anzianità di nomina, dal componente più anziano di età.

3.4 Temporaneo impedimento di un componente effettivo

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente effettivo dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria indipendenza ed autonomia di giudizio, questi è tenuto a dichiarare la sussistenza

del legittimo impedimento, e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva astenendosi dal partecipare alle sedute dell'organismo stesso o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.

A titolo esemplificativo, costituiscono cause di temporaneo impedimento:

- la circostanza che il componente sia destinatario di un provvedimento di rinvio a giudizio in relazione ad un reato presupposto;
- la circostanza che il componente apprenda dall'Autorità amministrativa di essere sottoposto alla procedura di irrogazione di una sanzione amministrativa di cui all'art. 187 quater del DecretoLegislativo n. 58/1998;
- malattia o infortunio che si protraggono per oltre tre mesi e impediscano di partecipare alle riunioni dell'Organismo.

Nel caso di temporaneo impedimento subentra automaticamente ed in via temporanea il membro supplente il quale cessa dalla carica quando viene meno la causa che ha determinato il suo subentro.

Resta salva la facoltà per il Consiglio di Amministrazione, quando l'impedimento si protragga per un periodo superiore a sei mesi, prorogabile di ulteriori 6 mesi per non più di due volte, di addivenire alla revoca del componente per il quale si siano verificate le predette cause di impedimento ed alla sua sostituzione con altro componente effettivo.

3.5 Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila in generale:

- sull'efficienza, efficacia ed adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D. Lgs. n. 231/2001, anche di quelli che in futuro dovessero comunque comportare una responsabilità amministrativa della persona giuridica;
- sull'osservanza delle prescrizioni contenute nel Modello da parte dei destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie funzioni aziendali;
- sull'aggiornamento del Modello laddove si riscontrino esigenze di adeguamento, formulando proposte agli Organi Societari competenti, laddove si rendano opportune modifiche e/o

integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, di significativi mutamenti dell'assetto organizzativo e procedurale della Società, nonché delle novità legislative intervenute in materia;

- sull'attuazione del piano di formazione del Personale, di cui al successivo cap. 6.2;
- sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare, a seguito dell'accertata violazione del Modello.

L'Organismo di Vigilanza è inoltre chiamato a vigilare sull'osservanza delle disposizioni in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo dettate dal D. Lgs. 21.11.2007 n. 231 e ad effettuare le conseguenti comunicazioni interne ed esterne previste dall'art. 52 del menzionato Decreto.

L'attività di controllo, eseguita dalla Funzione Internal Audit per conto dell'Organismo di Vigilanza, segue appositi protocolli elaborati e costantemente aggiornati in base alle risultanze dell'analisi dei rischi e degli interventi di controllo.

L'analisi dei rischi è il processo continuo di identificazione, classificazione e valutazione preventiva dei rischi (esterni ed interni) e dei controlli interni, da cui discende il piano degli interventi di audit.

Tale piano, predisposto annualmente, sentito anche l'Organismo di Vigilanza per quanto attiene alle materie di sua competenza, e sottoposto all'approvazione del Consiglio di Amministrazione, tiene anche conto delle eventuali osservazioni e indicazioni ricevute a vario titolo da parte degli Organi Societari.

Durante gli interventi di controllo viene analizzato nel dettaglio il livello dei controlli presenti nell'operatività e nei processi aziendali. I punti di debolezza rilevati sono sistematicamente segnalati alle Unità Organizzative e alle altre funzioni aziendali interessate al fine di rendere più efficienti ed efficaci le regole, le procedure e la struttura organizzativa. Per verificare l'effettiva esecuzione delle azioni da intraprendere, viene poi svolta un'attività di follow-up. Di tali attività la Funzione Internal Audit rendiconta periodicamente l'Organismo di Vigilanza.

Ai fini del Decreto, l'Organismo richiede alla Funzione Internal Audit di inserire nei propri Modelli di Sorveglianza (strumento che costituisce il supporto metodologico e regolamentare per presidiare il sistema dei controlli interni di uno specifico "ambito di controllo") e nel piano

annuale di audit verifiche specifiche volte, in particolare per le aree sensibili, a valutare l'adeguatezza dei controlli a prevenire comportamenti illeciti.

3.6 Modalità e periodicità di riporto agli Organi Societari

L'Organismo di Vigilanza, in ogni circostanza in cui sia ritenuto necessario o opportuno, ovvero se richiesto, riferisce al Consiglio di Amministrazione circa il funzionamento del Modello e l'adempimento agli obblighi imposti dal Decreto.

L'Organismo di Vigilanza, su base almeno semestrale, trasmette al Consiglio di Amministrazione una specifica informativa sull'adeguatezza e sull'osservanza del Modello, che ha ad oggetto:

- l'attività svolta;
- le risultanze dell'attività svolta;
- gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione.

Dopo l'esame da parte del Consiglio di Amministrazione, l'Organismo di Vigilanza provvede ad inoltrare l'informativa - corredata delle eventuali osservazioni formulate dal Consiglio di Amministrazione - all'Organismo di Vigilanza della Capogruppo.

L'Organismo di Vigilanza può scambiare informazioni con il Collegio Sindacale e la società di revisione, se ritenuto necessario o opportuno nell'ambito dell'espletamento delle rispettive competenze e responsabilità.

Capitolo 4 - Flussi informativi verso l'Organismo di Vigilanza

4.1 Flussi informativi da effettuarsi al verificarsi di particolari eventi

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei Dipendenti, dei Responsabili delle Funzioni Aziendali, degli Organi Societari, dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) in merito ad eventi che potrebbero ingenerare responsabilità della Cassa di Risparmio del Veneto S.p.A. ai sensi del Decreto.

Devono essere senza ritardo segnalati:

- le notizie relative alla commissione, o alla ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D. Lgs. n. 231/2001, compreso l'avvio di procedimento giudiziario a carico di dirigenti/dipendenti per reati previsti nel D. Lgs. n. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello.

Le segnalazioni possono essere fatte dai Dipendenti direttamente all'Organismo di Vigilanza, anche mediante l'inoltro di comunicazione elettronica presso la casella di posta OrganismoDiVigilanzaDL231@crveneto.it, ovvero per il tramite della Funzione Internal Audit, alla quale la segnalazione potrà essere effettuata tanto direttamente quanto mediante il Responsabile della struttura di appartenenza.

I soggetti esterni, ivi compresi i soggetti che svolgono attività in outsourcing per conto della Banca, inoltrano la segnalazione direttamente all'Organismo di Vigilanza.

L'Organismo di Vigilanza valuta le segnalazioni ricevute e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

L'Organismo di Vigilanza prenderà in considerazione le segnalazioni, ancorché anonime, che presentino elementi fattuali.

Cassa di Risparmio del Veneto S.p.A. garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della Banca o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono obbligatoriamente ed immediatamente essere trasmesse all'Organismo:

- per il tramite della Funzione Internal Audit, le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti per i quali è applicabile il D. Lgs. n. 231/2001, qualora tali indagini coinvolgano la Banca o suoi Dipendenti od Organi Societari o comunque la responsabilità della Banca stessa;
- i rapporti predisposti dalle funzioni aziendali nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto;
- i procedimenti disciplinari promossi o, nel caso in cui dette violazioni siano commesse da soggetti non dipendenti, le iniziative sanzionatorie assunte;

- per il tramite della funzione Compliance, le segnalazioni di infrazioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo inoltrate alle competenti Autorità ai sensi dell'art. 52 del D. Lgs. n. 231/2007, secondo modalità e tempistiche previste dalle disposizioni interne tempo per tempo vigenti.

Ciascuna struttura aziendale a cui sia attribuito un determinato ruolo in una fase di un processo sensibile deve segnalare tempestivamente all'Organismo di Vigilanza eventuali propri comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento.

La funzione Internal Audit, in caso di eventi che potrebbero ingenerare gravi responsabilità di Cassa di Risparmio del Veneto S.p.A. ai sensi del D. Lgs. n. 231/2001, informa tempestivamente il Presidente dell'Organismo di Vigilanza e predispone specifica relazione che descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, i provvedimenti disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

4.2 Flussi informativi periodici

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi dalle funzioni che svolgono attività di controllo di primo livello (Unità Organizzative), dalle funzioni Internal Audit e Compliance e dal Datore di lavoro ai sensi del D. Lgs. n. 81/2008.

Flussi informativi provenienti dalle Unità Organizzative

Con cadenza annuale i responsabili delle Unità Organizzative coinvolte nei processi "sensibili" ai sensi del D. Lgs. n. 231/2001, mediante un processo di autodiagnosi complessivo sull'attività

svolta, attestano il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative.
Attraverso questa formale attività di autovalutazione, evidenziano le eventuali criticità nei processi gestiti, gli eventuali scostamenti rispetto alle indicazioni dettate dal Modello o più in generale dall'impianto normativo, l'adeguatezza della medesima regolamentazione, con l'evidenziazione delle azioni e delle iniziative adottate o al piano per la soluzione.
Le attestazioni delle Unità Organizzative sono inviate con cadenza annuale alla funzione Compliance, la quale archivierà la documentazione, tenendola a disposizione dell'Organismo di Vigilanza per il quale produrrà una relazione con le risultanze.
La metodologia sull'esecuzione del processo di autodiagnosi, che rientra nel più generale processo di Operational Risk Management della Banca, è preventivamente sottoposta ad approvazione dell'Organismo di Vigilanza.

Flussi informativi provenienti dalla Funzione Internal Audit

Il flusso di rendicontazione ordinario della Funzione Internal Audit verso l'Organismo di Vigilanza è incentrato su relazioni trimestrali, con le quali quest'ultimo è informato sulle verifiche svolte, sulle principali risultanze, sulle azioni riparatrici poste in essere dalle Unità interessate, sugli ulteriori interventi di controllo in programma nel trimestre successivo, in linea con il Piano Annuo di Audit.
Laddove ne ravvisi la necessità, l'Organismo di Vigilanza richiede alla funzione di Internal Audit copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire.

Flussi informativi provenienti dalla Funzione Compliance

Il flusso di rendicontazione ordinario della Funzione Compliance verso l'Organismo di Vigilanza è incentrato su relazioni semestrali, con le quali viene comunicato l'esito dell'attività svolta in relazione all'adeguatezza ed al funzionamento del Modello, alle variazioni intervenute nei processi e nelle procedure (avvalendosi, a tal fine, della collaborazione della funzione Organizzazione) nonché agli interventi correttivi e migliorativi pianificati (inclusi quelli formativi) ed al loro stato di realizzazione.
L'informativa viene estesa al Consiglio di Amministrazione nell'ambito delle relazioni semestrali di compliance.

Flussi informativi da parte del Datore di lavoro ai sensi del D. Lgs. n. 81/2008

Il flusso di rendicontazione ordinario del Datore di lavoro ai sensi del D. Lgs. n. 81/2008 verso l'Organismo di Vigilanza è incentrato su relazioni annuali con le quali viene comunicato l'esito

della attività svolta in relazione alla organizzazione ed al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza.

Capitolo 5 - Il sistema sanzionatorio

Principi generali

L'efficacia del Modello è assicurata - oltre che dall'elaborazione di meccanismi di decisione e di controllo tali da eliminare o ridurre significativamente il rischio di commissione degli illeciti penali ed amministrativi per i quali è applicabile il D. Lgs. n. 231/2001 - dagli strumenti sanzionatori posti a presidio dell'osservanza delle condotte prescritte.

I comportamenti dei dipendenti e dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) non conformi ai principi e alle regole di condotta prescritti nel presente Modello - ivi ricomprendendo il Codice Etico, il Codice interno di comportamento di Gruppo e le procedure e norme interne, che fanno parte integrante del Modello - costituiscono illecito contrattuale.

Su tale presupposto, la Banca adotterà nei confronti:

- del personale dipendente, il sistema sanzionatorio stabilito dal Codice disciplinare della Banca e dalle leggi che regolano la materia,
- di tutti i soggetti esterni il sistema sanzionatorio stabilito dalle disposizioni contrattuali e di legge che regolano la materia.

L'attivazione, sulla base delle segnalazioni pervenute dalla funzione di Internal Audit o dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti dei dipendenti sono affidati, nell'ambito delle competenze alla stessa attribuite, alla funzione Risorse Umane, la quale sottoporrà alla previa autorizzazione del Direttore Generale l'adozione dei provvedimenti nei confronti dei dirigenti.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati alla funzione che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore.

Gli interventi sanzionatori nei confronti di eventuali dipendenti distaccati da altre Società del Gruppo sono affidati alla competente funzione Risorse Umane della Società di appartenenza.

Il tipo e l'entità di ciascuna delle sanzioni stabilite, saranno applicate, ai sensi della normativa richiamata, tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione

funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.
Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale, in quanto i principi e le regole di condotta imposte dal Modello sono assunte dalla Banca in piena autonomia ed indipendentemente dai possibili reati che eventuali condotte possano determinare e che l'autorità giudiziaria ha il compito di accertare.
Pertanto, in applicazione dei suddetti criteri, viene stabilito il seguente sistema sanzionatorio.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale procede anche alla segnalazione delle infrazioni di cui venisse a conoscenza nello svolgimento delle funzioni che gli sono proprie.

Personale appartenente alle aree professionali ed ai quadri direttivi
1) il provvedimento del **rimprovero verbale** si applica in caso di:
lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello,

correlandosi detto comportamento ad una "lieve inosservanza delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori" ai sensi di quanto già previsto al **punto a)** del Codice disciplinare vigente;

2) il provvedimento del **rimprovero scritto** si applica in caso:
di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da poter essere considerata ancorché non lieve, comunque, non grave,

correlandosi detto comportamento ad una "inosservanza non grave delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori" ai sensi di quanto previsto al **punto b)** del Codice disciplinare vigente;

3) il provvedimento della **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 ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva,

correlandosi detto comportamento ad una "inosservanza - ripetuta o di una certa gravità - delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori" ai sensi di quanto previsto al **punto c)** del Codice disciplinare vigente;

4) il provvedimento del **licenziamento per giustificato motivo** si applica in caso:
di adozione, nell'espletamento delle attività ricomprese nelle aree sensibili, di un comportamento caratterizzato da notevole inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal presente Modello, anche se sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto,

correlandosi detto comportamento ad una "violazione (. . .) tale da configurare (. . .) un inadempimento "notevole" degli obblighi relativi" ai sensi di quanto previsto al **punto d)** del Codice disciplinare vigente;

5) il provvedimento del **licenziamento per giusta causa** si applica in caso:
di adozione, nell'espletamento delle attività ricomprese nelle aree sensibili, di un comportamento consapevole in contrasto con le prescrizioni e/o le procedure e/o le norme interne del presente Modello, che, ancorché sia solo suscettibile di configurare uno degli illeciti a cui è applicabile il Decreto, leda l'elemento fiduciario che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche provvisoria,

correlandosi detto comportamento ad una "mancanza di gravità tale (o per dolosità del fatto, o per i riflessi penali o pecuniari o per la recidività o per la sua particolare natura) da far venir meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire la prosecuzione del rapporto stesso" ai sensi di quanto previsto alla **lettera e)** del Codice disciplinare vigente.

Personale dirigente

In caso di violazione, da parte di dirigenti, dei principi, delle regole e delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività ricomprese nelle aree sensibili di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili i provvedimenti di seguito indicati, tenuto altresì conto della gravità della/e violazione/i e della eventuale reiterazione. Anche in considerazione del particolare vincolo fiduciario che caratterizza il rapporto tra la Banca e il lavoratore con la qualifica di dirigente, sempre in conformità a quanto previsto dalle vigenti disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti delle imprese creditizie, finanziarie e strumentali si procederà con il **licenziamento con preavviso** e **il licenziamento per giusta causa** che, comunque, andranno applicati nei casi di massima gravità della violazione commessa.

Considerato che detti provvedimenti comportano la risoluzione del rapporto di lavoro, l'Azienda, in attuazione del principio legale della gradualità della sanzione, si riserva la facoltà, per le infrazioni meno gravi di applicare la misura del **rimprovero scritto** - in caso di semplice inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello - ovvero l'altra della **sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni** - in caso di inadempimento colposo di una certa rilevanza (anche se dipendente da recidiva) ovvero di condotta colposa inadempiente ai principi e alle regole di comportamento previsti dal presente Modello.

Soggetti esterni

Ogni comportamento posto in essere da soggetti esterni alla Banca che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla Banca, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto**.**

Componenti del Consiglio di Amministrazione

In caso di violazione del Modello da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione della Banca, l'Organismo di Vigilanza informerà il Collegio

Sindacale, il quale provvederà ad adottare le iniziative ritenute opportune in relazione alla fattispecie, nel rispetto della normativa vigente.

Capitolo 6 - Formazione e comunicazione interna

Il regime della responsabilità amministrativa previsto dalla normativa di legge e l'adozione del Modello di organizzazione, gestione e controllo da parte della Banca formano un sistema che deve trovare nei comportamenti operativi del Personale una coerente ed efficace risposta.

Al riguardo è fondamentale un'attività di comunicazione e di formazione finalizzata a favorire la diffusione di quanto stabilito dal Decreto Legislativo e dal Modello organizzativo adottato nelle sue diverse componenti (gli strumenti aziendali presupposto del Modello, le finalità del medesimo, la sua struttura e i suoi elementi fondamentali, il sistema dei poteri e delle deleghe, l'individuazione dell'Organismo di Vigilanza, i flussi informativi verso quest'ultimo, etc.). Ciò affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura professionale di ciascun collaboratore.

Con questa consapevolezza è stato strutturato il piano di comunicazione interna e formazione che ha definito un percorso pluriennale, rivolto a tutto il Personale, che ha l'obiettivo, anche in funzione delle specifiche attività svolte, di creare una conoscenza diffusa e una cultura aziendale adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

6.1 Comunicazione interna

I neo assunti ricevono, all'atto dell'assunzione, unitamente alla prevista restante documentazione, copia del Modello, del Codice Etico e del Codice interno di comportamento di Gruppo. La sottoscrizione di un'apposita dichiarazione attesta la consegna dei documenti, l'integrale conoscenza dei medesimi e l'impegno ad osservare le relative prescrizioni.
Sull'Intranet aziendale, nel sito Normativa, sono pubblicate e rese disponibili per la consultazione, oltre alle varie comunicazioni interne, il Modello di Organizzazione, Gestione e Controllo della Banca e le normative collegate (in particolare, Codice Etico e Codice interno di comportamento di Gruppo).
I documenti pubblicati sono costantemente aggiornati in relazione alle modifiche che via via intervengono nell'ambito della normativa di legge e del modello organizzativo.
Il sito Notizie Interne di Intranet e la Web Tv, quest'ultima nelle modalità Live e On Demand, informano in tempo reale il Personale delle novità intervenute; la Web Tv, inoltre, con apposite trasmissioni (clip), della durata di dieci minuti circa ciascuna, contenenti anche interviste ai vari

Responsabili, propone adeguati momenti di approfondimento sulle normativa in materia, sulle attività "sensibili", sugli interventi formativi, ecc..

L'house organ ospita poi periodici articoli di approfondimento redatti anche con il contributo di esperti.

In sintesi, l'insieme degli strumenti citati, unitamente alle circolari interne, garantisce a tutto il Personale una informazione completa e tempestiva.

6.2 Formazione

Il piano di formazione ha l'obiettivo di far conoscere il nuovo Modello e, in particolare, di sostenere adeguatamente coloro che sono coinvolti nelle attività "sensibili".

Per garantirne l'efficacia esso è stato costruito tenendo in considerazione le molteplici variabili presenti nel contesto di riferimento; in particolare,

- i target (i destinatari degli interventi, il loro livello e ruolo organizzativo);
- i contenuti (gli argomenti attinenti al ruolo delle persone);
- gli strumenti di erogazione (aula, e-learning, Web Tv);
- i tempi di erogazione e di realizzazione (la preparazione e la durata degli interventi);
- l'impegno richiesto al target (i tempi di fruizione);
- le azioni necessarie per il corretto sostegno dell'intervento (promozione, supporto dei Capi).

Il piano prevede:

- una formazione di base e-learning per tutto il Personale;
- specifici interventi di aula per le persone che lavorano nelle strutture in cui maggiore è il rischio di comportamenti illeciti (in particolare, quelle che operano a stretto contatto con la Pubblica Amministrazione, nell'ambito delle funzioni Acquisti, Finanza, etc.);
- trasmissioni televisive per tutto il Personale, di durata contenuta (10/12 minuti ca.), focalizzate sui Protocolli di più ampio impatto/criticità, sulla normativa interna, sui comportamenti operativi da attivare.

Il supporto formativo e-learning, di durata contenuta (1 ora ca.), attrattivo per veste grafica e modalità di interazione, consente la divulgazione tempestiva e capillare dei contenuti comuni a tutto il Personale – normativa di riferimento (D. Lgs. n. 231/2001 e reati presupposto), Modello e suo funzionamento, contenuti del Codice Etico e del Codice interno di comportamento di Gruppo – ed è arricchito da test di autovalutazione con cui i colleghi possono verificare il loro apprendimento.

La formazione di aula, che interviene dopo la fruizione del prodotto e-learning, declinata per specifico ambito operativo, ha l'obiettivo di diffondere la conoscenza dei reati, le fattispecie

configurabili, i presidi specifici delle aree di competenza degli operatori, e di richiamare alla corretta applicazione del Modello di Organizzazione, Gestione e Controllo. La metodologia didattica è fortemente interattiva e si avvale di case studies.
Le trasmissioni televisive successive alla formazione e-learning e agli interventi in aula, costituiscono per tutte le persone, siano o meno coinvolte nelle attività "sensibili", un momento di acculturamento ulteriore che consente di mantenere sempre viva l'attenzione sul tema, consolidare la conoscenza e interiorizzare sempre più i comportamenti operativi "virtuosi".

I contenuti formativi sono convenientemente aggiornati in relazione all'evoluzione della normativa esterna e del Modello. Se intervengono modifiche rilevanti (ad es. estensione della responsabilità amministrativa dell'ente a nuove tipologie di reati), si procede ad una coerente integrazione dei contenuti medesimi, assicurandone altresì la fruizione.
La fruizione delle varie iniziative di formazione è richiesta a tutto il personale cui le iniziative stesse sono dirette ed è monitorata a cura della competente funzione Risorse Umane, con la collaborazione dei Responsabili ai vari livelli che devono farsi garanti, in particolare, della fruizione dei prodotti "remoti" da parte dei loro collaboratori.
La funzione Risorse Umane ha cura di raccogliere i dati relativi alla partecipazione ai vari programmi e di conservarli in appositi archivi.
L'Organismo di Vigilanza verifica, anche attraverso i flussi informativi provenienti dalla funzione Compliance, lo stato di attuazione del piano di formazione ed ha facoltà di chiedere controlli periodici sul livello di conoscenza, da parte del Personale, del Decreto, del Modello e delle sue implicazioni operative.

Capitolo 7 – Gli illeciti presupposto - Aree, attività e relativi principi di comportamento e di controllo

7.1 Individuazione delle aree sensibili

L'art. 6, comma 2, del D. Lgs. n. 231/2001 prevede che il Modello debba "individuare le attività nel cui ambito possono essere commessi reati".

Sono state pertanto analizzate, come illustrato al paragrafo 2.4, le fattispecie di illeciti presupposto per le quali si applica il Decreto; con riferimento a ciascuna categoria dei medesimi sono state identificate nella Banca le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali aree si sono quindi individuate le singole attività sensibili e qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Il Modello trova poi piena attuazione nella realtà dell'azienda attraverso il collegamento di ciascuna area e attività "sensibile" con le strutture aziendali coinvolte e con la gestione dinamica dei processi e della relativa normativa di riferimento.

Alla luce delle seguenti considerazioni i successivi protocolli ripercorrono in larga misura quelli della Capogruppo Intesa Sanpaolo S.p.A.:

- la Banca ha realizzato un elevato grado di esternalizzazione presso la Capogruppo delle funzioni aziendali di Corporate Centre;
- il modello organizzativo/gestionale delle Strutture periferiche della Banca replica quello di Capogruppo;
- la Banca ha fatto propri normativa, procedure e processi che regolano l'attività della Capogruppo;
- la Banca vede accentrata presso la Capogruppo la Funzione di Internal Audit.

Sarà compito dell'Organismo di Vigilanza svolgere nel continuo la necessaria attività di monitoraggio del livello di adeguatezza del presente Modello, al fine di garantirne una costante funzionalità e conformità alle prescrizioni del Decreto.

In considerazione di tutto quanto sopra, quando nei successivi protocolli si fa riferimento alle Strutture e/o alle Funzioni della Banca ovvero più genericamente al termine ”Struttura”, si intende fare riferimento anche alle Strutture e/o alle Funzioni di Capogruppo e/o di altre Società del Gruppo quando le attività sono svolte in outsourcing.

Sulla base delle disposizioni di legge attualmente in vigore le aree sensibili identificate dal Modello riguardano in via generale:

- Area Sensibile concernente i reati contro la Pubblica Amministrazione;
- Area Sensibile concernente i reati di falsità in moneta (e valori);
- Area Sensibile concernente i reati societari;
- Area Sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona;
- Area Sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- Area Sensibile concernente i reati ed illeciti amministrativi riconducibili ad abusi di mercato;
- Area Sensibile concernente i reati in tema di salute e sicurezza sul lavoro;
- Area Sensibile concernente i reati informatici;
- Area Sensibile concernente i reati contro l’industria ed il commercio ed i reati in materia di violazione del diritto d’autore.

7.2 Area sensibile concernente i reati contro la Pubblica Amministrazione

7.2.1 Fattispecie di reato

Premessa

Gli artt. 24 e 25 del Decreto contemplano una serie di reati previsti dal codice penale accomunati dall'identità del bene giuridico da essi tutelato, individuabile nell'imparzialità e nel buon andamento della Pubblica Amministrazione.

Agli effetti della legge penale si considera Ente della Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi.

A titolo meramente esemplificativo ed avendo riguardo all'operatività della Banca si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione: i) lo Stato, le Regioni, le Province, i Comuni; ii) i Ministeri, i Dipartimenti, le Commissioni; (iii) gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT).

Tra le fattispecie penali qui considerate, il reato di concussione nonché il reato di corruzione, nelle sue varie tipologie, presuppongono il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p..

In sintesi, può dirsi che la distinzione tra le due figure è in molti casi controversa e labile e che la stessa è definita dalle predette norme secondo criteri basati sulla funzione oggettivamente svolta dai soggetti in questione.

La qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. L'esercizio di una pubblica funzione amministrativa solitamente è riconosciuto sussistere in capo a coloro che formano o concorrono a formare la volontà dell'ente pubblico o comunque lo rappresentano di fronte ai terzi, nonché a coloro che sono muniti di poteri autoritativi o certificativi[1].

A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, esattore di aziende municipalizzate, assistente universitario, portalettere,

[1] Rientra nel concetto di poteri autoritativi non solo il potere di coercizione ma ogni attività discrezionale svolta nei confronti di soggetti che si trovano su un piano *non paritetico* rispetto all'autorità (cfr. Cass., Sez. Un. 11/07/1992, n.181). Rientrano nel concetto di poteri certificativi tutte quelle attività di documentazione cui l'ordinamento assegna efficacia probatoria, quale che ne sia il grado.

funzionario degli uffici periferici dell'ACI, consiglieri comunali, geometra tecnico comunale, insegnanti delle scuole pubbliche, ufficiale sanitario, notaio, dipendenti dell'INPS.
La qualifica di Incaricato di Pubblico Servizio si determina per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale.
A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, letturisti dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori.

Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato. Con riferimento all'operatività della Banca, determinate attività - in particolare quelle concernenti la distribuzione di titoli del debito pubblico, la riscossione delle imposte, i servizi di tesoreria per conto di un Ente Pubblico, i crediti di scopo legale, i crediti speciali o agevolati - possono assumere, secondo la giurisprudenza, una connotazione di rilevanza pubblicistica tale da far riconoscere anche in capo ai dipendenti ed esponenti bancari, nell'espletamento di dette attività, la qualifica di Incaricato di Pubblico Servizio, con la conseguenza della imputabilità agli stessi dei reati che richiedono il possesso di tale qualifica da parte di colui che pone in essere la condotta punita. Tra questi reati, solo la corruzione e la concussione sono previsti tra gli "illeciti presupposto" che possono far scattare la responsabilità della Banca ai sensi del D. Lgs. n. 231/2001.

Deve porsi particolare attenzione al fatto che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad un'operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la

risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Si illustrano sinteticamente qui di seguito le fattispecie delittuose previste dagli artt. 24 e 25 del Decreto.

Malversazione a danno dello Stato (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto in modo lecito finanziamenti, sovvenzioni o contributi da parte dello Stato italiano o delle Comunità Europee per la realizzazione di opere o attività di interesse pubblico, non si proceda all'utilizzo delle somme per le finalità per cui sono state concesse. Per gli operatori bancari il reato in oggetto potrà verificarsi sia nell'ipotesi in cui le sovvenzioni siano erogate a favore della Banca perché ne fruisca direttamente, sia nell'ipotesi in cui la Banca intervenga nel processo di erogazione a favore dei privati destinatari autori del distoglimento dalle finalità pubbliche prestabilite e in concorso con i medesimi.

Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)

La fattispecie criminosa si realizza nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità Europee. A nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si perfeziona nel momento dell'ottenimento dei finanziamenti. Anche tale reato può verificarsi sia per le erogazioni di cui benefici la Banca che per quelle in cui la Banca intervenga da tramite a favore di clienti autori delle false attestazioni e in concorso con i medesimi.

Truffa (art. 640, comma 2, n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui si ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato oppure ad altro Ente Pubblico.

Il reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni supportate da documentazione artefatta, al fine di ottenere l'aggiudicazione della gara stessa.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altro Ente pubblico o delle Comunità Europee.

Gli elementi caratterizzanti il reato in esame sono: rispetto al reato di truffa generica (art. 640, comma 2, n. 1, c.p.), l'oggetto materiale specifico, che per la presente fattispecie consiste nell'ottenimento di erogazioni pubbliche comunque denominate; rispetto al reato di indebita percezione di erogazioni (art. 316-ter c.p.), la necessità dell'ulteriore elemento della attivazione di artifici o raggiri idonei ad indurre in errore l'ente erogante.

Frode informatica (art. 640-ter)

La fattispecie di frode informatica consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati o programmi in essi contenuti, ottenendo un ingiusto profitto. Essa assume rilievo ai fini del D. Lgs. n. 231, soltanto nel caso in cui sia perpetrata ai danni dello Stato o di altro Ente Pubblico.

In concreto, può integrarsi il reato in esame qualora, ad esempio, una volta ottenuto un finanziamento, venisse violato un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente, oppure anche nel caso di modificazione delle risultanze di un conto corrente intestato ad un Ente pubblico, abusivamente accedendo ad un sistema di home banking.

Concussione (art. 317 c.p.)

Tale ipotesi criminosa si realizza nel caso in cui un Pubblico Ufficiale o un Incaricato di un Pubblico Servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Colui che subisce la costrizione non è considerato parte attiva del reato, andando quindi esente da sanzione penale, ma ne è persona offesa.

La responsabilità delle persone giuridiche ai sensi del D. Lgs. n. 231/2001 a titolo di concussione sembrerebbe configurabile solo nella forma del concorso tra un soggetto apicale o tra un subordinato (che agiscano nell'interesse o a vantaggio della persona giuridica) con il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio.

Peraltro, va ricordato che, come illustrato in Premessa, l'esercizio di quelle attività aventi connotazioni di rilevanza pubblicistica comporta secondo la giurisprudenza l'assunzione in capo all'operatore bancario della qualifica di Incaricato di Pubblico Servizio o di Pubblico Ufficiale: in tal caso eventuali condotte estorsive al fine di ottenere denaro o altra utilità per il compimento di dette attività (ad esempio: per dar corso all'erogazione di un finanziamento agevolato) potrebbero comportare la commissione da parte sua del reato in esame e, sussistendone i presupposti, la conseguente responsabilità della Banca.

Corruzione

In generale, il reato di corruzione consiste in un accordo fra un Pubblico Ufficiale o un Incaricato di Pubblico Servizio e un privato, in forza del quale il primo accetta dal secondo un compenso che

non gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria).
La corruzione si manifesta quando le parti, essendo in posizione paritaria fra di loro, pongono in essere un vero e proprio accordo, diversamente dalla concussione, che invece presuppone lo sfruttamento da parte del soggetto rivestente la qualifica pubblica della propria posizione di superiorità, alla quale corrisponde nel privato una situazione di soggezione.
Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, rivestente la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva). La responsabilità della Banca per reato commesso dai dipendenti o dai soggetti apicali anche nell'interesse o a vantaggio della medesima potrebbe conseguire a fronte di ipotesi sia di corruzione attiva che di corruzione passiva. Difatti, come precisato in Premessa, talune attività connotate da riflessi pubblicistici potrebbero comportare l'assunzione in capo all'operatore bancario della qualifica di Incaricato di Pubblico Servizio.
Le fattispecie di corruzione rilevanti ai sensi del D. Lgs. n. 231/2001 sono le seguenti.

Corruzione per un atto d'ufficio (art. 318 c.p.)
Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
Tali ipotesi di reato si configurano nel caso in cui un Pubblico Ufficiale o un Incaricato di Pubblico Servizio riceva, per sé o per altri, denaro o altri vantaggi per compiere oppure omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del Pubblico Ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: Pubblico Ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).
Ai sensi dell'art. 320 c.p. il reato di cui all'art. 319 c.p. può essere imputato ad un Incaricato di Pubblico Servizio indipendentemente dal fatto che rivesta o meno la qualità di dipendente pubblico; invece, perché ricorra la responsabilità di un Incaricato di Pubblico Servizio per il reato di cui all'art. 318 c.p. è necessario che il medesimo rivesta la qualifica di pubblico impiegato.

Corruzione in atti giudiziari (art. 319-ter, comma 1, c.p.)
In questa fattispecie di reato la condotta del corrotto o del corruttore è caratterizzata dal fine specifico di favorire o di danneggiare una parte in un processo penale, civile o amministrativo.

Istigazione alla corruzione (art. 322 c.p.)
Tale reato è commesso dal soggetto privato la cui offerta o promessa di denaro o di altra utilità per il compimento di un atto d'ufficio (art. 318 c.p.) o di un atto contrario ai doveri d'ufficio (art. 319 c.p.)

non sia accettata. Per il medesimo titolo di reato risponde il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che solleciti, con esito negativo, tale offerta o promessa.

7.2.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione sono le seguenti:

- Stipula dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informatico di Gruppo;
- Gestione degli interventi agevolativi;
- Gestione della formazione finanziata;
- Gestione dei contenziosi e degli accordi transattivi;
- Gestione dei rapporti con le Autorità di Vigilanza;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del processo di selezione e assunzione del personale;
- Gestione del patrimonio immobiliare e dei beni mobili di valore artistico.

Con riferimento all'attività sensibile concernente la Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo si rimanda al protocollo 7.9.2.1; si riportano di seguito, per ognuna delle sopraelencate attività sensibili, i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili a dette attività e che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime.

7.2.2.1. Stipula dei rapporti contrattuali con la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte in qualsiasi tipologia di stipula di rapporti contrattuali con gli Enti della Pubblica Amministrazione, aventi ad oggetto operazioni quali, a titolo esemplificativo e non esaustivo:

- contratti di tesoreria e servizi di gestione, di incasso e pagamento;
- contratti/convenzioni per la erogazione/gestione di operazioni di finanza agevolata e/o finanziamenti agevolati;
- finanziamenti diretti ad Enti pubblici;
- stipula di contratti di locazione passiva con Enti pubblici;
- stipula di convenzioni con Enti pubblici per l'offerta a dipendenti pubblici di prodotti e servizi bancari, d'investimento e assicurativi;
- stipula di convenzioni con SACE e SIMEST;
- stipula di rapporti contrattuali societari e di patti parasociali con Enti pubblici, funzionali all'instaurazione e alla gestione di rapporti partecipativi.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1] e "truffa ai danni dello Stato".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Descrizione del processo

Il processo di stipula dei rapporti contrattuali con la Pubblica Amministrazione si articola nelle seguenti fasi:

- attività di sviluppo commerciale e individuazione delle opportunità di business;
- gestione dei rapporti pre-contrattuali con la Pubblica Amministrazione anche finalizzati alla stipula di apposite Convenzioni fra la medesima e la Banca;
- partecipazione (laddove richiesta) a gare pubbliche per l'aggiudicazione dei servizi attraverso la:
  - predisposizione e approvazione, della documentazione e modulistica necessaria per la partecipazione ai bandi di gara;
  - presentazione delle domande di partecipazione ai bandi di gara all'Ente pubblico di riferimento;
  - predisposizione e approvazione della documentazione e modulistica necessaria per l'offerta commerciale agli Enti;
  - presentazione delle offerte tecniche ed economiche all'Ente pubblico di riferimento;
- perfezionamento del contratto con l'Ente (predisponendo tutte le informative necessarie alla successiva fase di gestione del contratto stesso).

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - tutti i soggetti che intervengono nella fase di gestione dei rapporti pre-contrattuali con la Pubblica Amministrazione devono essere individuati e autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
  - gli atti che impegnano contrattualmente la Banca devono essere sottoscritti soltanto da soggetti appositamente incaricati;
  - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi inclusi quelli nei confronti della Pubblica

Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di definizione dell'accordo contrattuale con gli Enti pubblici. In particolare:
  - le attività di sviluppo commerciale sono svolte da strutture diverse rispetto a quelle che gestiscono operativamente l'erogazione dei prodotti/servizi contrattualizzati;
  - la definizione dell'accordo è esclusivamente affidata al Responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati; l'atto formale della stipula del contratto avviene in base al vigente sistema dei poteri e delle deleghe;
  - i soggetti deputati alla predisposizione della documentazione per la presentazione dell'offerta tecnica ed economica, ovvero per la partecipazione a bandi di gara pubblica, sono differenti da coloro che sottoscrivono la stessa.

- Attività di controllo:
  - la documentazione relativa alla stipula dei rapporti contrattuali viene sottoposta per il controllo al Responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati che si avvalgono, per la definizione delle nuove tipologie contrattuali, del contributo consulenziale della competente Struttura per quanto concerne gli aspetti di natura legale;
  - tutta la documentazione predisposta dalla Banca per l'accesso a bandi di gara pubblici deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal Responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò facoltizzati.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante degli accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;
  - ogni accordo/convenzione/contratto con Enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica,

nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nelle attività di stipula dei rapporti contrattuali con la Pubblica Amministrazione, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo. In particolare:

- tutti i soggetti che, in fase di sviluppo commerciale e identificazione di nuove opportunità di business, intrattengono rapporti con la Pubblica Amministrazione per conto della Banca, devono essere espressamente autorizzati;
- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca, quali i contratti per la vendita di servizi, devono essere appositamente incaricati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nella stipula dei rapporti contrattuali con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- le procedure aziendali definiscono i criteri e le casistiche in cui il coinvolgimento di soggetti terzi deve essere preventivamente sottoposto al vaglio di una funzione indipendente;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti

esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla Banca;
- minacciare i partecipanti a gare pubbliche di arrecare loro un danno ingiusto al fine di dissuaderli dalla partecipazione o per conoscere le loro offerte e formulare le proprie in modo tale da ottenere l'aggiudicazione della gara;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la Banca;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato);
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare l'instaurazione/sviluppo di rapporti finalizzati alla stipula.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.2. Gestione dei rapporti contrattuali con la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione di rapporti contrattuali con gli Enti della Pubblica Amministrazione, aventi ad oggetto operazioni quali, a titolo esemplificativo e non esaustivo:

- gestione di convenzioni con Enti pubblici per l'offerta rivolta ai dipendenti pubblici di prodotti e servizi bancari, d'investimento e assicurativi;
- gestione di contratti di tesoreria e servizi di gestione, di incasso e pagamento;
- gestione delle operazioni finanziarie con controparte la Banca d'Italia e/o il Tesoro;
- gestione degli accordi e dei rapporti con SACE e SIMEST;
- pagamento delle pensioni in convenzione;
- gestione richieste e successivo incasso di contributi/agevolazioni a supporto di finanziamenti agevolati.

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1], "concussione" e "truffa ai danni dello Stato".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Descrizione dei processi

Il processo di gestione delle convenzioni con gli Enti pubblici si articola nelle seguenti fasi:

- gestione tassi e condizioni (autorizzazione delle condizioni di offerta, acquisizione e aggiornamento dati in procedura);
- mantenimento rapporti commerciali con la controparte.

Il processo di gestione degli incassi e pagamenti diversi per conto degli Enti per i quali la Banca svolge il servizio di tesoreria si articola nelle seguenti fasi:

- gestione amministrativa e contabile dei servizi di tesoreria;
- rendicontazione dei flussi agli Enti interessati.

Le operazioni finanziarie con controparte la Banca d'Italia e/o il Dipartimento del Tesoro ricomprendono le seguenti attività:

- operazioni di politica monetaria attraverso lo strumento "pronti contro termine";
- ottenimento liquidità infragiornaliera;
- sottoscrizione Titoli di Stato;
- operazioni di deposito e compravendita di valute;
- attivazione delle deposit facilities;
- operazioni per conto del Tesoro.

Il processo di gestione degli accordi e dei rapporti con SACE fa riferimento alla definizione e gestione degli adempimenti previsti dall'Accordo Quadro stipulato con SACE relativo alle connesse convenzioni assicurative.

Il processo di gestione degli accordi e dei rapporti con SIMEST fa riferimento alla gestione dell'accordo di collaborazione tra la Banca e SIMEST, che trova applicazione rispetto ad una pluralità di disposizioni legislative quali, a titolo esemplificativo e non esaustivo:

- agevolazioni all'export (D. Lgs. n. 143/98);
- partecipazione al capitale ed investimenti in società estere (L. 100/90);
- finanziamento di programmi di partecipazione commerciale (L. 394/81);
- partecipazione a gare internazionali (L. 304/90);
- studi di fattibilità e assistenza tecnica (D. Lgs. n. 143/98).

Il processo di pagamento delle pensioni in convenzione, prevede i seguenti adempimenti:

- gestione pagamenti disposti dagli Enti convenzionati;

- gestione riaccrediti pensioni;
- controlli, ove previsti dalle singole convenzioni, sull'esistenza in vita dei pensionati:
- gestione prestazioni temporanee.

Il processo di gestione degli accordi connessi all'instaurazione e gestione di rapporti partecipativi con Enti pubblici si articola nelle seguenti fasi:

- analisi preliminare dei presupposti per l'esecuzione del contratto;
- esecuzione del contratto;
- monitoraggio sull'esecuzione del contratto.

Il processo di gestione richieste e successivo incasso di contributi/agevolazioni a supporto di finanziamenti agevolati si articola nelle seguenti fasi:

- verifica preliminare della sussistenza dei presupposti normativi;
- elaborazione dei prospetti di rendicontazione/richiesta dei contributi ed invio all' Ente;
- incasso dei contributi provenienti dall'Ente nel caso di competenza della banca essendo già stati anticipati dalla stessa al beneficiario finale;
- riconoscimento dei contributi ai beneficiari in caso di loro competenza;
- quadrature contabili;
- riscontro di eventuali inadempienze da parte degli Enti;
- azione nei confronti degli Enti morosi.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - la gestione dei rapporti con i Funzionari pubblici in costanza di esecuzione degli obblighi di natura contrattuale con gli Enti stessi è organizzativamente demandata a specifiche strutture della Banca che si occupano della erogazione di prodotti / servizi oggetto del contratto. La stipula dei contratti per l'esecuzione di servizi nei confronti della Pubblica Amministrazione è effettuata nel rispetto dei principi di comportamento sanciti dal Protocollo per la "Stipula dei rapporti contrattuali con la Pubblica

Amministrazione" e, in particolare, tutti gli atti che impegnano contrattualmente la Banca nei confronti di terzi devono essere sottoscritti soltanto da soggetti appositamente incaricati;

- nell'ambito di ogni struttura, tutti i soggetti che intervengono nella gestione dei rapporti contrattuali con la Pubblica Amministrazione devono essere individuati e autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
- sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione degli accordi contrattuali con gli Enti pubblici. In particolare:
  - i soggetti deputati alla predisposizione della documentazione per la rendicontazione agli Enti sono differenti da coloro che sottoscrivono la stessa;
  - le Strutture incaricate della gestione operativa dei prodotti/servizi contrattualizzati, sono diverse da quelle incaricate dello sviluppo commerciale.

- Attività di controllo: la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna Struttura interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all'esecuzione dei processi oggetto del presente protocollo. In particolare dovrà essere assicurata la verifica della regolarità delle operazioni nonché della completezza, della correttezza e della tempestività delle scritture contabili che devono essere costantemente supportate da meccanismi di maker e checker.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali verso la Pubblica Amministrazione prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le strutture provvedono alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;
  - ciascuna Struttura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rapporti con la Pubblica Amministrazione.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione derivanti da adempimenti di natura contrattuale con gli Enti stessi, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/esecuzione dei rapporti contrattuali con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- in occasione di operazioni di Tesoreria verso Enti pubblici, ovvero di incassi effettuati agli sportelli di imposte, tasse e contributi a vario titolo, le operazioni dovranno essere svolte secondo le procedure stabilite internamente nel rispetto di quanto definito dagli accordi commerciali presi.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla Banca;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Banca;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato);
- ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dalla Banca o, comunque, un trattamento più favorevole di quello dovuto;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.3. Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso alla Pubblica Amministrazione quali, a titolo esemplificativo e non esaustivo:

- gestione dei rapporti con gli Enti assistenziali e previdenziali e realizzazione, nei tempi e nei modi previsti, degli adempimenti di legge in materia di lavoro e previdenza (INPS, INAIL, INPDAP, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc);
- gestione dei rapporti con gli Enti Locali per l'esecuzione delle attività inerenti al registro delle imprese;
- gestione dei rapporti con gli Enti Locali territorialmente competenti in materia di smaltimento rifiuti;
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti locali (A.S.L., Vigili del Fuoco, Arpa, etc.) per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni (ad esempio pratiche edilizie), permessi, concessioni;
- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con Banca d'Italia per l'esecuzione degli adempimenti in materia di mantenimento della riserva obbligatoria;
- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio competenti per la richiesta di certificati e autorizzazioni;
- gestione dei rapporti con il Ministero dello Sviluppo Economico e con le Camere di Commercio per l'esecuzione di adempimenti connessi alla realizzazione di manifestazioni a premio (legge 449/97 art.19 – DPR 430/2001).

Ai sensi del D. Lgs n. 231/2001, le predette attività potrebbero presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1] e "truffa ai danni dello Stato".

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di richieste di autorizzazioni o esecuzione di adempimenti si articola nelle seguenti fasi:

- predisposizione della documentazione;
- invio della documentazione richiesta e archiviazione della pratica;
- gestione dei rapporti con gli Enti pubblici;
- assistenza in occasione di sopralluoghi ed accertamenti da parte degli Enti;
- gestione dei rapporti con gli Enti pubblici per il ritiro dell'autorizzazione e l'esecuzione degli adempimenti.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - nell'ambito di ogni Struttura, tutti i soggetti che intervengono nella gestione delle attività inerenti alla richiesta di autorizzazioni alla Pubblica Amministrazione devono essere individuati ed autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima; nel caso in cui i rapporti con gli

o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Enti pubblici vengano intrattenuti da soggetti terzi, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;

- la gestione dei rapporti con i Funzionari pubblici in caso di accertamenti/sopralluoghi, effettuati anche allo scopo di verificare l'ottemperanza alle disposizioni di legge che regolamentano l'operatività dell'area di propria competenza, è attribuita al Responsabile della struttura e/o ai soggetti da quest'ultimo appositamente individuati.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione al fine di garantire, per tutte le fasi del processo un meccanismo di maker e checker.

- Attività di controllo: le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - copia della documentazione consegnata all'Ente pubblico per la richiesta di autorizzazione o per l'esecuzione di adempimenti è conservata presso l'archivio della struttura di competenza;
  - il Responsabile della Struttura, ovvero il soggetto aziendale all'uopo incaricato ha l'obbligo di firmare per accettazione il verbale redatto dai Funzionari pubblici in occasione degli accertamenti/sopralluoghi condotti presso la Banca e di mantenerne copia nei propri uffici, unitamente ai relativi allegati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla richiesta di autorizzazioni alla Pubblica Amministrazione .

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di autorizzazioni o esecuzione di adempimenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero l'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente il riscontro da parte della Pubblica Amministrazione;

- promettere o versare somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato);
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.4. Gestione degli interventi agevolativi

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione del processo di erogazione di agevolazioni pubbliche alle imprese e/o privati, a valere su fondi regionali, nazionali e comunitari.

Il processo di gestione degli interventi agevolativi comprende le attività di istruttoria, gestione ed erogazione di tali interventi, che, a titolo esemplificativo e non esaustivo, possono riguardare:

- finanziamenti agevolati e contributi in conto capitale concessi dai Ministeri per agevolazioni a progetti di ricerca e sviluppo;
- Fondo di Garanzia L. 341/95;
- finanziamenti con contribuiti in conto interessi, finanziamenti con fondi di terzi (ad es.: BEI, CEB, ecc.), finanziamenti ordinari correlati ad erogazione di contributi in conto capitale o in conto interessi e mutui con ammortamento a carico dello Stato o con garanzia dello Stato;
- contributi in conto capitale a valere su strumenti quali quelli ex Lege 488/92, di Programmazione Negoziata, strumenti regionali, ecc..

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "concussione", "corruzione"[1], "truffa ai danni dello Stato", "truffa aggravata per il conseguimento di erogazioni pubbliche" e "malversazione".

Si rileva inoltre come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione degli interventi agevolativi si articola nelle seguenti fasi:

- ricezione delle domande di agevolazione e/o di finanziamento;
- istruttoria delle domande di agevolazione e/o di finanziamento;
- acquisizione della documentazione (emessa dalla Amministrazione Pubblica competente, attestante la titolarità dell'agevolazione e necessaria per la stipula del contratto) per l'ottenimento del decreto di concessione;
- stipula di contratti, ove prevista;
- acquisizione della documentazione necessaria per le erogazioni;
- effettuazione degli accertamenti connessi all'erogazione delle agevolazioni;
- richiesta dei fondi, ove previsto, ed erogazione delle agevolazioni e/o del finanziamento;
- richiesta periodica dei contributi in conto interessi;
- comunicazione periodica delle informazioni all'Ente;
- gestione degli eventi societari straordinari successivi alla concessione delle agevolazioni (quali variazioni societarie del richiedente, fusioni, scissioni, procedure concorsuali, trasferimenti di sede, ecc);
- eventuale gestione, ove previsto, delle fasi di ammortamento e recupero crediti.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - tutti i soggetti che intervengono a qualsiasi titolo nella gestione degli interventi agevolativi devono essere individuati ed autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;

- tutte le approvazioni per gli atti impegnativi e le autorizzazioni alle erogazioni dei fondi devono essere rilasciate da soggetti appositamente incaricati; la normativa interna illustra tali meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri di approvazione.

- Segregazione dei compiti tra i differenti soggetti coinvolti, volto a garantire, per tutte le fasi del processo, un meccanismo di maker e checker. In particolare, nel caso in cui il finanziamento venga deliberato dalla Banca, la responsabilità dell'istruttoria compete ad un soggetto diverso da quello responsabile della delibera stessa, fatte salve le eccezioni espressamente previste dalla normativa interna tempo per tempo vigente. Inoltre, ai soggetti deliberanti sono attribuite competenze deliberative differenziate in funzione della classe di merito creditizio (probabilità di default) del cliente.

- Attività di controllo: i controlli di linea che devono essere svolti a cura della Struttura competente per i finanziamenti a valere su fondi ministeriali per agevolazioni a progetti di ricerca e sviluppo, riguardano:
  - la valutazione e approvazione, da parte dei responsabili degli uffici/team operativi, delle relazioni istruttorie e di quelle di controllo sugli stati d'avanzamento degli investimenti, compreso quello finale;
  - l'utilizzo di sistemi informatici dedicati all'operatività, su cui sono implementati, ove possibile, idonei presidi di controllo automatizzato.

Per quanto riguarda invece le Strutture competenti nella gestione delle altre agevolazioni, l'attività di controllo di linea riguarda in particolare:

- verifica, effettuata da parte degli istruttori degli uffici operativi, sulle capacità economico-patrimoniali dei soggetti richiedenti, sulla validità tecnica, economica e finanziaria dei progetti e delle modalità di copertura dei piani finanziari oggetto di valutazione;
- utilizzo di sistemi informatici dedicati all'operatività, su cui sono implementate attività di controllo automatico (check dei dati, warning su errori, ecc.);
- esistenza di procedure di sign off sui documenti principali di progetto;
- verifica, da parte dell'organo proponente, dei requisiti di ammissibilità, congruità della spesa e sostenibilità del piano finanziario;
- verifica tecnica, anche da parte di organi terzi, riguardo la congruità della spesa documentata ed erogabilità del contributo;

- esistenza di verifiche/accertamenti finali sulla correttezza della documentazione allegata alla singola pratica, ad opera del nucleo/ufficio operativo di competenza;
- accertamenti periodici eventualmente derivanti da specifici obblighi di controllo e monitoraggio contenuti nel testo di convenzione con gli Enti.

Inoltre ciascuna Struttura interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all'esecuzione dei processi oggetto del presente protocollo deve assicurare il corretto espletamento dei controlli di linea, la verifica della regolarità delle operazioni nonché la completezza, la correttezza, e la tempestività delle scritture contabili che devono essere costantemente supportate da meccanismi di maker e checker.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione degli interventi agevolativi.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione degli interventi agevolativi sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare:

- tutti i soggetti che, in fase di richiesta e gestione di finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Banca nonché coloro che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Banca (es. pratiche di istruttoria, richieste fondi, ecc.) devono essere espressamente autorizzati;

- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta/gestione del finanziamento o nella successiva esecuzione di attività connesse con progetti/programmi finanziati, i contratti/lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- per ragioni di incompatibilità con il ruolo pubblicistico svolto dalla Banca, i finanziamenti agevolati/contributi in conto capitale e/o in conto interessi concessi alle imprese beneficiarie delle agevolazioni non possono essere oggetto di anticipazione ovvero di cessione delle medesime alla Banca incaricata dell'istruttoria. Pertanto è tassativamente esclusa la possibilità di deliberare affidamenti/anticipazioni assistiti da mandato irrevocabile all'incasso o cessione di contributi spettanti alle imprese per le quali la Banca esegue l'istruttoria;
- i Responsabili delle Strutture interessate devono garantire, nell'ambito delle attività di propria competenza, il costante aggiornamento e sensibilizzazione del personale sulla normativa esterna di riferimento ed attivarsi affinché il personale fruisca delle attività formative messe a disposizione dalle Strutture centrali della Banca;
- i rapporti e gli adempimenti nei confronti della Pubblica Amministrazione, ovvero nei confronti di suoi rappresentanti/esponenti, devono essere adempiuti con la massima trasparenza, diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- accettare e/o esibire consapevolmente documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Banca;
- utilizzare contributi, sovvenzioni, finanziamenti pubblici riconosciuti alla clientela per finalità diverse da quelle per le quali sono stati concessi al fine di procurare un vantaggio alla Banca, anche mediante compensazioni di crediti o mancato riconoscimento degli stessi;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura al Funzionario pubblico a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato);
- accettare omaggi, vantaggi di qualsiasi natura o somme di denaro da imprese, ovvero cedere a raccomandazioni e pressioni da parte delle stesse, al fine di facilitare l'espletamento della pratica e/o garantire il buon esito dell'intervento agevolato richiesto;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare il rapporto con la Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.5. Gestione della formazione finanziata

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione della formazione finanziata.

Attraverso la gestione della formazione finanziata la Banca, laddove sussistano i presupposti, ricorre ai finanziamenti, sovvenzioni e contributi per la formazione concessi da soggetti pubblici nazionali ed esteri tra i quali si citano a titolo esemplificativo e non esaustivo quelli concessi a valere su:

- Fondo Sociale Europeo (Finanziamenti alla formazione di occupati/disoccupati – Contributi comunitari Regionali e Provinciali);
- Fon.Dir. (Fondo paritetico interprofessionale nazionale per la formazione continua dei dirigenti del terziario);
- For.Te. (Fondo paritetico interprofessionale nazionale per la formazione continua del terziario);
- Fondo di solidarietà per il sostegno del reddito, dell'occupazione e della riconversione e riqualificazione professionale del personale del credito.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1], "truffa aggravata per il conseguimento di erogazioni pubbliche" e "malversazione".

Si dà atto che in base all'attuale assetto organizzativo della Banca, le attività inerenti alla gestione della formazione finanziata, sono demandate operativamente alle competenti Strutture di Capogruppo e/o di altre Società del Gruppo, sulla scorta dei relativi contratti di outsourcing. Ciononostante, anche al fine di assicurare un'adeguata sensibilizzazione di tutto il personale, si riportano nel seguito i principi di controllo e comportamento, applicati dalla Capogruppo e/o da

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

altre Società del Gruppo e condivisi dalla Banca, volti a garantire il rispetto della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità per la corretta attuazione del processo sottodescritto.

Descrizione del processo

Il processo si articola nelle seguenti fasi:

- individuazione iniziative finanziabili;
- predisposizione e presentazione della richiesta di finanziamento/contributo all'Ente pubblico, corredata, laddove previsto, dal verbale di accordo sottoscritto con le competenti OO.SS.LL;
- attuazione dei progetti finanziati;
  - gestione dell'operatività dell'iniziativa finanziata;
  - gestione delle risorse previste dal progetto/iniziativa (economiche e tecniche, interne ed esterne);
- rendicontazione dei costi;
- raccolta dei dati contabili, elaborazione e stesura di report;
- gestione dei rapporti con Enti in occasione di verifiche e ispezioni da parte dell'Ente finanziatore;
- gestione dell'introito del contributo.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - tutti i soggetti che, nell'ambito della "gestione della formazione finanziata", intrattengono rapporti con gli Enti finanziatori devono essere individuati e autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
  - le richieste di finanziamento/contributo sono sottoscritte dal Responsabile della Struttura competente specificamente e formalmente facoltizzati in virtù del vigente sistema dei poteri e delle deleghe; la normativa interna illustra tali meccanismi

autorizzativi, fornendo le indicazioni dei soggetti aziendali cui sono attribuiti i necessari poteri.

- in caso di eventuale ricorso a consulenti esterni, il processo di attribuzione dell'incarico avviene uniformemente a quanto previsto dalle disposizioni contenute nella specifica sezione dedicata nel presente Modello (protocollo per "la gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali"). La selezione di tali consulenti avviene in ogni caso prevedendo l'acquisizione di una pluralità di offerte e la scelta mediante criteri oggettivi e codificati.

- Segregazione dei compiti tra i differenti soggetti coinvolti, volta a garantire, per tutte le fasi del processo, un meccanismo di maker e checker. In particolare, la Struttura competente attribuisce a ciascun ufficio organizzativamente dipendente, in funzione dei ruoli ricoperti da ciascun addetto, le attività operative e le attività di controllo da effettuare al fine di garantire la contrapposizione di ruoli tra i soggetti che gestiscono le fasi istruttorie del processo della formazione finanziata ed i soggetti deputati alle attività di verifica.

- Attività di controllo da parte di ciascuna Struttura competente ed in particolare:
  - verifica della coerenza dei contenuti del progetto di formazione rispetto a quanto disposto dalle direttive del bando di finanziamento;
  - verifica della regolarità formale della documentazione da consegnare all'Ente per l'accesso al bando di finanziamento;
  - tenuta del registro presenze durante l'erogazione dei progetti formativi e utilizzo di sistemi informatici di supporto per la gestione del personale, in cui sono registrate tutte le informazioni relative alle presenze ed alle attività svolte;
  - puntuale attività di controllo sul processo di rendicontazione delle spese, attraverso:
    - raccolta e verifica dei registri di presenza compilati in ogni loro parte dai partecipanti agli interventi formativi;
    - raccolta della documentazione degli oneri aziendali dei dipendenti partecipanti / docenti, sulla base del corrispettivo orario calcolato a cura dell'ufficio competente in considerazione delle matricole che hanno partecipato all'iniziativa;
    - raccolta e verifica delle parcelle/fatture relative ai costi sostenuti per l'iniziativa;
    - verifica sulla puntuale e corretta contabilizzazione degli introiti.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: tutte le fasi di processo sono documentate, così come previsto dagli stessi bandi per

l'ottenimento dei finanziamenti. In particolare, ciascuna Struttura coinvolta nell'ambito del processo della formazione finanziata, è responsabile dell'archiviazione e della conservazione della documentazione di propria competenza, ivi inclusa quella trasmessa all'Ente finanziatore pubblico anche in via telematica o elettronica.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nell'attività di gestione della formazione finanziata, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.

In particolare:

- tutti i soggetti che, in fase di richiesta e gestione dei finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Banca devono essere espressamente autorizzati;
- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca (es.: pratiche di richiesta, studi di fattibilità, piani di progetto, ecc.) devono essere appositamente incaricati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta / gestione del finanziamento o nella successiva esecuzione di attività connesse con i programmi finanziati, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi e alterati;
- tenere una condotta ingannevole che possa indurre gli Enti finanziatori / erogatori in errore di valutazione tecnico-economica della documentazione presentata;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di accoglimento delle domande di ammissione al contributo;
- destinare contributi, sovvenzioni, finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Banca nell'ottenimento di contributi. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato);
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di facilitare/velocizzare l'iter istruttorio delle pratiche.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

I principi di comportamento illustrati nel presente protocollo devono intendersi altresì estesi, per quanto compatibili, ad ogni eventuale ulteriore processo aziendale concernente la richiesta e la gestione di contributi/incentivi pubblici a favore della Banca concessi a qualsiasi altro titolo.

7.2.2.6. Gestione dei contenziosi e degli accordi transattivi

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione dei contenziosi giudiziali e stragiudiziali (amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con Enti pubblici.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1], "corruzione in atti giudiziari" e "truffa ai danni dello Stato" nonché del reato di "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria"[2].

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo e/o da altre Società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

---

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

[2] Tale reato, punito dall'art. 377-bis c.p., costituisce reato presupposto della responsabilità degli enti ai sensi dell'art. 25-novies del Decreto. Inoltre, ai sensi dell'art. 10 della L. n.146/2006 può dar luogo alla medesima responsabilità anche se commesso in forma transnazionale. Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

Descrizione del Processo

Il processo di gestione del contenzioso si articola nelle seguenti fasi, effettuate sotto la responsabilità delle Strutture competenti per materia, in coordinamento con la Struttura interessata dalla controversia e con gli eventuali professionisti esterni incaricati:

- apertura del contenzioso giudiziale o stragiudiziale;
  - raccolta delle informazioni e della documentazione relative alla vertenza;
  - analisi, valutazione e produzione degli elementi probatori;
  - predisposizione degli scritti difensivi e successive integrazioni, direttamente o in collaborazione con i professionisti esterni;
- gestione della vertenza;
- ricezione, analisi e valutazione degli atti relativi alla vertenza;
- predisposizione dei fascicoli documentali;
- partecipazione, ove utile o necessario, alla causa, in caso di contenzioso giudiziale;
- intrattenimento dei rapporti costanti con gli eventuali professionisti incaricati, individuati nell'ambito dell'apposito albo;
- assunzione delle delibere per:
  - determinazione degli stanziamenti al Fondo Rischi e Oneri in relazione alle vertenze passive e segnalazione dell'evento quale rischio operativo;
  - esborsi e transazioni;
- chiusura della vertenza

Il processo di gestione degli accordi transattivi riguarda tutte le attività necessarie per prevenire o dirimere una controversia attraverso accordi o reciproche rinunce e concessioni, al fine di evitare l'instaurarsi o il proseguire di procedimenti giudiziari.

Il processo si articola nelle seguenti fasi:

- analisi dell'evento da cui deriva la controversia e verifica dell'esistenza di presupposti per addivenire alla transazione;
- gestione delle trattative finalizzate alla definizione e alla formalizzazione della transazione;
- redazione, stipula ed esecuzione dell'accordo transattivo.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti: la gestione dei contenziosi e degli accordi transattivi con la Pubblica Amministrazione prevede l'accentramento delle responsabilità di indirizzo e/o gestione da parte mia e monitoraggio delle singole fasi del processo in capo a diverse Strutture della Banca a seconda che si tratti di profili giuridici di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale. E' inoltre previsto nell'ambito di ciascuna fase operativa caratteristica del processo:
  - il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso ivi incluso quello nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - il conferimento degli incarichi a legali esterni diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dalla Struttura competente è autorizzato dal Responsabile della Struttura medesima o da un suo delegato;
  - la Struttura competente effettua un costante monitoraggio degli sviluppi della vertenza, anche per poter prontamente valutare opportunità transattive che dovessero profilarsi.

- Segregazione dei compiti: attraverso il chiaro e formalizzato conferimento di compiti e responsabilità nell'esercizio delle facoltà assegnate nello svolgimento delle attività di cui alla gestione dei contenziosi e degli accordi transattivi con la Pubblica Amministrazione. In particolare, le procedure aziendali prevedono adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate da funzioni diverse da quelle di business che hanno gestito la relazione con la Pubblica Amministrazione.

- Attività di controllo:
  - rilevazione e monitoraggio periodico delle vertenze pendenti;
  - verifica periodica della regolarità, della completezza e correttezza di tutti gli adempimenti connessi a vertenze / transazioni che devono essere supportati da meccanismi di maker e checker.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta;

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei contenziosi e degli accordi transattivi con la Pubblica Amministrazione.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei contenziosi e degli accordi transattivi con la Pubblica Amministrazione sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Banca devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi con la Pubblica Amministrazione, i contratti / lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- adottare comportamenti contrari alle Leggi, al Codice Etico ed al Codice interno di comportamento di Gruppo, in sede di incontri formali ed informali, anche a mezzo di professionisti esterni e soggetti terzi, per indurre Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della Banca;
- adottare comportamenti contrari alle Leggi, al Codice Etico ed al Codice interno di comportamento di Gruppo, nel corso di tutte le fasi del procedimento, anche a mezzo di professionisti esterni, per:
  - indurre al superamento di vincoli o criticità ai fini della tutela degli interessi della Banca;
  - favorire indebitamente gli interessi della Banca inducendo - con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità - a tacere o a mentire la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
- adottare comportamenti contrari alle Leggi, al Codice Etico ed al Codice interno di comportamento di Gruppo, in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o nominati dall'Organo giudicante, anche a mezzo di professionisti esterni, per influenzarne il giudizio/parere nell'interesse della Banca;
- adottare comportamenti contrari alle Leggi, al Codice Etico ed al Codice interno di comportamento di Gruppo in sede di decisione del contenzioso/arbitrato, anche a mezzo di professionisti esterni, per influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione quando questa sia controparte del contenzioso;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Banca;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione del reato di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare il rapporto con la Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.7. Gestione dei rapporti con le Autorità di Vigilanza

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione dei rapporti con le Autorità di Vigilanza e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste e visite ispettive.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "corruzione"[1] e "ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza" (art. 2638 del codice civile).

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con le Autorità di Vigilanza quali:

- Banca d'Italia;
- Consob;
- ISVAP;
- Autorità Garante per la Privacy;
- Autorità Garante per la Concorrenza e il Mercato (AGCM);
- COVIP.

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

I principi di comportamento contenuti nel presente protocollo si applicano, a livello d'indirizzo comportamentale, anche nei confronti delle Autorità di Vigilanza estere.

Descrizione del Processo

Le attività inerenti la gestione dei rapporti con le Autorità di Vigilanza sono riconducibili alle seguenti tipologie:

- elaborazione/trasmissione delle segnalazioni occasionali o periodiche alle Autorità di Vigilanza;
- richieste/istanze di abilitazioni e/o autorizzazioni;
- riscontri ed adempimenti connessi a richieste/istanze delle Autorità di Vigilanza;
- gestione dei rapporti con i Funzionari delle Autorità di Vigilanza in occasione di visite ispettive.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - ad eccezione delle visite ispettive i rapporti con le Autorità di Vigilanza sono intrattenuti dal Responsabile della Struttura di riferimento o da soggetti dallo stesso appositamente incaricati tramite delega interna, da conservare a cura della Struttura medesima;
  - gli atti che impegnano contrattualmente la Banca devono essere sottoscritti soltanto da soggetti incaricati.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza. In particolare:
  - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle Strutture della Banca, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è preventivamente condivisa con le competenti Strutture;

- è compito del Responsabile della Struttura interessata dalla visita ispettiva, dopo aver accertato l'oggetto dell'ispezione, individuare le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la Banca. La competente funzione Legale, quella di Internal Audit, quella di Compliance e nei casi particolarmente rilevanti l'Organismo di Vigilanza devono essere tempestivamente informate della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità.

- Attività di controllo:
  - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle Autorità di Vigilanza da parte della Struttura interessata per le attività di competenza devono essere supportate da meccanismi di maker e checker;
  - controlli di carattere giuridico sulla conformità alla normativa di riferimento della segnalazione/comunicazione richiesta;
  - controlli automatici di sistema, con riferimento alle segnalazioni periodiche.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - è fatto obbligo a tutte le Strutture della Banca, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico. Tale documentazione deve essere resa disponibile a richiesta alle Strutture aventi funzione Legale, di Internal Audit e Segreteria societaria;
  - ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Banca è documentata/registrata in via informatica ed archiviata presso la Struttura di competenza;
  - fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il personale della Struttura interessata che ha presenziato alla visita ispettiva assiste il Funzionario pubblico nella stesura del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal Funzionario stesso;
  - ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza il Responsabile della Struttura interessata provvede a trasmettere alle Funzioni aziendali competenti copia del verbale rilasciato dal Funzionario pubblico e degli annessi allegati.

Qualora non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il Responsabile della Struttura interessata dall'ispezione od un suo delegato provvede alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa alle Funzioni aziendali competenti. La suddetta documentazione è archiviata dal Responsabile della Struttura interessata dall'ispezione.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con le Autorità di Vigilanza, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un soggetto dell'Autorità di Vigilanza di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso;
- devono essere puntualmente trasmesse le segnalazioni periodiche alle Autorità di Vigilanza e tempestivamente riscontrate le richieste/istanze pervenute dalle stesse Autorità;
- nell'ambito delle ispezioni effettuate da parte dei Funzionari delle Autorità presso la sede della Banca, fatte salve le situazioni in cui i Funzionari richiedano colloqui diretti con personale della Banca specificamente individuato, partecipano agli incontri con i Funzionari stessi almeno due soggetti, se appartenenti alla Struttura interessata dall'ispezione; diversamente, laddove l'ispezione sia seguita da Strutture diverse da quella coinvolta dalla verifica (quali, ad esempio: Personale, Organizzazione, Legale e Audit) è prevista la partecipazione di un unico soggetto agli incontri con i Funzionari.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;

- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza in errore;
- chiedere o indurre i rappresentanti dell'Autorità di Vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle funzioni di Vigilanza;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti dell'Autorità di Vigilanza a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato).

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.8. Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione delle procedure acquisitive dei beni e dei servizi.
Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo[1], mentre tra le prestazioni vanno ricomprese anche quelle a contenuto intellettuale di qualsiasi natura (es. legale, fiscale, tecnica, giuslavoristica, amministrativa, organizzativa, ecc), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "corruzione"[2] e "corruzione in atti giudiziari".
Una gestione non trasparente del processo, infatti, potrebbe consentire la commissione di tali reati, ad esempio attraverso la creazione di fondi "neri" a seguito del pagamento di prezzi superiori all'effettivo valore del bene/servizio ottenuto.
Si intende inoltre prevenire il rischio di acquisire beni o servizi di provenienza illecita, ed in particolare il coinvolgimento nei reati contro l'industria ed il commercio e nei reati in materia di violazione del diritto d'autore.[3]

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

---

[1] Ai sensi dell'art. 2575 del codice civile, le opere dell'ingegno di carattere creativo tutelate dal diritto d'autore sono quelle che appartengono alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì considerate e protette come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.
[2] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).
[3] Si veda al riguardo il Capitolo 7.10.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

L'attività di gestione delle procedure acquisitive dei beni e dei servizi si articola nei seguenti processi:

- definizione e gestione del budget;
- gestione degli approvvigionamenti;
- gestione del ciclo passivo;
- gestione dei fornitori.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti:
  - il budget della Banca, predisposto dal Direttore Generale, è approvato dal Consiglio di Amministrazione;
  - l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna**,** fatte salve esigenze/forniture occasionali. Tali soggetti devono garantire e su richiesta poter documentare – in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi - il rispetto della disciplina in tema di protezione

dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
- l'eventuale affidamento a terzi - da parte dei fornitori della Banca - di attività in sub-appalto, è contrattualmente subordinato ad un preventivo assenso da parte della struttura della Banca che ha stipulato il contratto;
- l'autorizzazione al pagamento della fattura spetta ai Responsabili delle Strutture per le quali è prevista l'assegnazione di un budget e delle relative facoltà di spesa (Centri di Responsabilità) o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle inadempienze/carenze della fornitura adeguatamente documentata e dettagliata a cura delle predette Strutture;
- il pagamento delle fatture è effettuato da una specifica Struttura aziendale dedicata.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive. In particolare:
  - le attività di cui alle diverse fasi del processo devono essere svolte da soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

- Attività di controllo: la normativa interna di riferimento identifica i controlli che devono essere svolti a cura di ciascuna Struttura interessata in ogni singola fase del processo:
  - verifica dei limiti di spesa e della pertinenza della stessa;
  - verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
  - verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti, ivi comprese le garanzie circa l'autenticità e la legittima provenienza dei beni forniti.

Per quanto concerne infine l'acquisizione di incarichi professionali e consulenze che comportano un rapporto diretto con la Pubblica Amministrazione (quali ad esempio spese legali per contenzioso, onorari a professionisti per pratiche edilizie, spese per consulenze propedeutiche all'acquisizione di contributi pubblici, ecc.) i Responsabili delle Strutture interessate dovranno:
- disporre che venga regolarmente tenuto in evidenza l'elenco dei professionisti/consulenti, l'oggetto dell'incarico ed il relativo corrispettivo;
- verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
  - documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nel processo di gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice di comportamento interno di Gruppo.
In particolare:

- la documentazione contrattuale che regola il conferimento di incarichi di fornitura/incarichi professionali deve contenere un'apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere, collaborare, dare causa alla realizzazione di comportamenti che possano risultare strumentali alla commissione di fattispecie di reato

considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della Banca che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi;
- minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore o utilizzino i servizi di concorrenti della Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.9. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

Si precisa che, ai fini del presente protocollo, valgono le seguenti definizioni:

- per omaggi si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della Banca;
- per spese di rappresentanza si intendono le spese sostenute dalla Banca nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Banca (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza ed ospitalità, ecc.);
- per iniziative di beneficenza si intendono le elargizioni in denaro che la Banca destina esclusivamente ad Enti senza fini di lucro;
- per sponsorizzazioni si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della Banca attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: società o gruppi sportivi che svolgono attività anche dilettantistica, Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero costituire una delle modalità strumentali attraverso cui commettere i reati di "corruzione"[1] e "corruzione in atti giudiziari".

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione al fine di favorire interessi della Banca ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

I processi di gestione degli omaggi e delle spese di rappresentanza hanno ad oggetto i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi, quali, ad esempio, clienti, fornitori, Enti della Pubblica Amministrazione, istituzioni pubbliche o altre organizzazioni.
Tali beni sono acquisiti sulla base delle regole operative sancite dalla normativa interna in materia di spesa e dal protocollo "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali".

I processi di gestione delle spese per beneficenze e per sponsorizzazioni si articolano nelle seguenti fasi:

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di due diligence[1] della Banca;
- esame/valutazione dell'iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell'accordo/ contratto;
- erogazione delle elargizioni da parte della Banca.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti che costituisce parte integrante e sostanziale del presente protocollo.

[1] Ricerca di informazioni rilevanti sull'Ente richiedente quali, a titolo esemplificativo e non esaustivo denominazione, natura giuridica e data di costituzione, dati anagrafici sulla sede legale e operativa (se diversa da quella legale) ed eventuale sito web, legale rappresentante, notizie sull'ente e sulle sue linee strategiche, sulla dimensione (numero dipendenti e/o collaboratori, numero di soci), sui principali progetti realizzati negli ultimi due anni nel settore di riferimento dell'iniziativa proposta, sintesi delle informazioni finanziarie relative ai bilanci approvati negli ultimi due anni, ecc..

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti:
  - per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
  - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
  - per quanto attiene gli omaggi e le spese di rappresentanza destinati, seppure in modo non esclusivo, ad esponenti della Pubblica Amministrazione, le procedure aziendali stabiliscono idonei limiti quantitativi rapportati al valore di tali omaggi/spese.

- Segregazione dei compiti: tra i differenti soggetti coinvolti nei processi. In particolare:
  - le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

- Attività di controllo:
  - la normativa interna definisce i limiti oltre ai quali le erogazioni per beneficenze e sponsorizzazioni devono essere precedute da un'attività di due diligence da parte della Struttura interessata, avente ad oggetto:
    - analisi e verifica del tipo di organizzazione e della finalità per la quale è costituita;
    - tutte le erogazioni devono essere verificate ed approvate del Responsabile della Struttura interessata;
    - le erogazioni complessive sono stabilite annualmente e devono trovare capienza in apposito budget deliberato dagli Organi competenti, all'interno del quale è fissato un limite massimo di importo e di numero di erogazioni

annuali per destinatario, salvo espresse deroghe formalizzate ai livelli competenti;

- per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa;

Inoltre i Responsabili delle Strutture interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo della Banca (quali biro, oggetti per scrivania, ecc...), nonché l'omaggistica standard predisposta dalle Strutture Centrali (ad esempio, in occasione di fine anno);
- verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le Strutture interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni.

Principi di comportamento

Premesso che le spese per omaggi sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo. In particolare:

- la Banca può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che non contrastino i principi etici conformi a quelli della Banca;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di Enti coinvolti in note vicende giudiziarie, pratiche non rispettose dei diritti umani, vivisezionistiche o antiambientali. Non possono inoltre essere oggetto di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club (ad esempio Lions, Rotary, ecc.), associazioni e gruppi ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico;
- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo;
- promettere o versare somme di denaro, promettere o concedere beni in natura o altri benefici a Enti esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della Banca, anche a seguito di illecite pressioni. Il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso;
- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.10. Gestione del processo di selezione e assunzione del personale

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione del processo di selezione e assunzione del personale.

Ai sensi della citata normativa, il processo in oggetto potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "corruzione"[1] o di "corruzione in atti giudiziari"
Una gestione non trasparente del processo di selezione e assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per la Banca.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Il processo di selezione e assunzione si articola nelle seguenti fasi:

- Selezione del personale:
  - analisi e richiesta di nuove assunzioni;
  - definizione del profilo del candidato;

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

- reclutamento dei candidati;
- effettuazione del processo selettivo;
- individuazione dei candidati.

- Formalizzazione dell'assunzione.

Qualora il processo riguardi personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro.

Resta nelle competenze delle Strutture aziendali specificatamente facoltizzate l'istruttoria relativa alla selezione ed assunzione di personale specialistico altamente qualificato ovvero di figure destinate a posizioni di vertice (cosiddetta "assunzione a chiamata").
Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti:
  - accentramento del processo di selezione e assunzione del personale in capo alla Struttura competente che riceve le richieste formali di nuovo personale da parte delle Strutture interessate e le valuta in coerenza con il budget ed i piani interni di sviluppo;
  - autorizzazione all'assunzione concessa soltanto dal personale espressamente facoltizzato secondo il vigente sistema dei poteri e delle deleghe;
  - l'assunzione dei candidati individuati come idonei e per i quali è stata fornita autorizzazione all'inserimento viene effettuata dalle Unità Organizzative competenti per Struttura.

- Segregazione dei compiti tra i diversi soggetti coinvolti nel processo. In particolare l'approvazione finale dell'assunzione è demandata a strutture diverse, commisurate all'importanza della posizione ricercata all'interno dell'organizzazione aziendale.

- Attività di controllo:

- compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica per garantire la raccolta omogenea delle informazioni sui candidati.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta (tra cui quella standard ad esempio testi, application form, contratto di lavoro, ecc.) anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché eventualmente le eventuali previsioni del Codice Etico e del Codice di comportamento interno di Gruppo.

In particolare:

- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.11. Gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico

Premessa

La gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico riguarda qualunque tipologia di attività svolta dalle strutture della Banca finalizzata alla valorizzazione ed ottimizzazione del patrimonio immobiliare di Gruppo - di proprietà ed in locazione - nonché alla valorizzazione, valutazione degli interventi e gestione dei beni mobili della Banca aventi valore artistico.
Ai sensi del D. Lgs. n. 231/2001, il processo in oggetto potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "corruzione"[1] e "corruzione in atti giudiziari".
Una gestione non trasparente del processo relativo alla gestione di beni immobili e mobili aventi valore artistico potrebbe, infatti, consentire la commissione di tali reati, attraverso il riconoscimento / concessione di vantaggi ad esponenti della Pubblica Amministrazione al fine di favorire interessi della Banca.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

L'attività di gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico della Banca si articola nei seguenti processi:

[1] Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore è penalmente sanzionata non solo allorché abbia quali destinatari i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando: i) si realizzi verso quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) sia posta in essere nei confronti di quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica)
.

- pianificazione degli atti dispositivi;
- gestione amministrativa e contabile degli immobili;
- gestione dei contratti di locazione;
- gestione delle spese di proprietà e degli oneri fiscali.

Gestione patrimonio immobiliare:

- individuazione e selezione delle opportunità di investimento /disinvestimento;
- acquisizione e vendita degli immobili;
- ottimizzazione del patrimonio immobiliare corrente;
- pianificazione immobiliare di lungo periodo.

Gestione patrimonio artistico:

- gestione contratti locazione/comodato dei beni aventi valore artistico;
- gestione beni aventi valore artistico.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti:
  - tutti i soggetti che intervengono nella gestione dei rapporti pre-contrattuali devono essere individuati e autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
  - tutte le deliberazioni relative alle compravendite ed alle locazioni spettano esclusivamente a soggetti muniti di idonei poteri in base al vigente sistema dei poteri e delle deleghe che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

- Segregazione delle funzioni: tra i differenti soggetti coinvolti nel processo. In particolare:

- le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

- Attività di controllo:
  - verifica della congruità del canone di locazione passiva e attiva per tutte le nuove locazioni e le rinegoziazioni di locazioni con riferimento alle condizioni espresse dal mercato o in conformità a quanto stabilito all'interno di una gara pubblica;
  - effettuazione delle attività di due diligence sulla controparte;
  - verifica della congruità del prezzo di compravendita dell'immobile / bene mobile avente valore artistico rispetto al valore di mercato, anche attraverso l'acquisizione di perizie redatte da esperti indipendenti ogni qualvolta la controparte sia una Pubblica Amministrazione o un esponente della medesima;
  - verifica puntuale di tutti i dati contenuti nei contratti di compravendita e, in particolare, verifica di coerenza tra compromesso / preliminare e contratto definitivo;
  - redazione e aggiornamento dell'anagrafe delle locazioni in essere, con indicazione di dettaglio delle nuove locazioni e di quelle oggetto di rinnovo nel periodo di riferimento;
  - redazione e aggiornamento dell'anagrafe dei beni mobili aventi valore artistico.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante inerente agli atti dispositivi (compravendite, locazioni, comodati) deve risultare da apposita documentazione scritta;
  - ogni atto dispositivo (compravendite, locazioni, comodati) è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture a qualsiasi titolo coinvolte nella gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico della Banca, sono tenute ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice di comportamento interno di Gruppo.
In particolare:

- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nel processo di gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano risultare strumentali alla commissione di fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o concedere beni immobili e mobili aventi valore artistico a Enti della Pubblica Amministrazione, istituzioni pubbliche o a soggetti da questi ultimi indicati a condizioni diverse da quelle di mercato;
- procedere all'autorizzazione al pagamento di fatture passive a fronte di acquisizioni / locazioni di beni immobili e mobili aventi valore artistico in assenza di un'attenta e puntuale verifica dell'importo da liquidare;

- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice di Comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.3 Area sensibile concernente i reati di falsità in monete (e valori)

7.3.1 Fattispecie di reato

L'art. 25-bis del Decreto contempla una serie di reati previsti dal codice penale a tutela della fede pubblica, ossia dell'affidamento sociale nella genuinità ed integrità di alcuni specifici simboli, essenziale ai fini di un rapido e certo svolgimento del traffico economico. Le condotte punite hanno ad oggetto monete – a cui sono equiparate le carte di pubblico credito, vale a dire le banconote e le carte e cedole al portatore emesse da Governi o da Istituti a ciò autorizzati – valori di bollo, carte filigranate e strumenti od oggetti destinati al falso nummario[1].
In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate.

Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
Alterazione di monete (art. 454 c.p.)
Si ha contraffazione di monete nell'ipotesi in cui un soggetto fabbrichi ex novo una moneta falsa, mentre sussiste la diversa fattispecie dell'alterazione nel caso di monete vere cui sia stata data l'apparenza di un valore superiore a quello reale.
In entrambe le fattispecie, è punito sia il soggetto che ponga in essere la contraffazione o l'alterazione, sia colui che, in concerto con chi abbia proceduto alla contraffazione o alterazione, o con un suo intermediario, introduca nel territorio dello Stato, detenga o metta in circolazione in qualsiasi modo le monete così contraffatte o alterate, sia, infine, colui che, al fine di metterle in circolazione, se le procuri presso il soggetto che le ha contraffatte o alterate, o presso un suo intermediario.
Remota appare la possibilità che soggetti interni ad una banca pongano in essere, autonomamente o in concorso di terzi, nell'interesse della banca stessa, fatti di alterazione o contraffazione; i maggiori rischi sono individuabili nelle ipotesi di messa in circolazione delle monete falsificate e di ricezione delle stesse al fine della messa in circolazione.

Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
L'ipotesi contemplata dall'art. 455 c.p., residuale rispetto a quelle disciplinate dalle due disposizioni precedenti, presuppone comunque la consapevolezza o il sospetto ab origine, nel soggetto che

[1] La L. n. 99/2009 ha modificato l'art. 25-bis, aggiungendo ai reati in tema di falso nummario i reati in tema di contraffazione di marchi, segni distintivi, brevetti e modelli (artt. 473 e 474 c.p.), per i quali si rimanda al Capitolo 7.10.

pone in essere la condotta, della non autenticità delle monete, pur in assenza di qualunque accordo con il soggetto che abbia proceduto alla loro falsificazione.
Nella fattispecie di cui all'art. 457 c.p., al contrario, l'elemento essenziale e distintivo è la buona fede iniziale del soggetto che pone in essere la condotta criminosa; buona fede che viene meno soltanto al momento della spendita o, più in generale, della messa in circolazione della moneta contraffatta o alterata.
Potrebbe quindi essere chiamato a rispondere del reato in oggetto l'operatore bancario che utilizzi per operazioni di sportello banconote contraffatte, anche se ricevute in buona fede, nell'intento di evitare alla banca i pregiudizi o, semplicemente, i fastidi derivanti dal rilevare e denunciare la falsità.

Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
Dato il carattere peculiare dell'oggetto materiale dei reati in esame, si ritiene invero assai remota la sussistenza di profili di rischio per gli operatori bancari in ordine a tali fattispecie.

7.3.2. Attività aziendali sensibili

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i reati di falsità in monete è la:

- Gestione dei valori.

Si riporta di seguito il protocollo che detta i principi di controllo ed i principi di comportamento applicabili a detta attività e che si completa con la normativa aziendale di dettaglio che regolamenta l'attività medesima.

7.3.2.1 Gestione dei valori

Premessa

La gestione dei valori riguarda qualsiasi attività inerente alla trattazione di valori di qualsiasi natura con particolare riferimento a banconote, monete, valori di bollo aventi corso legale nello Stato e all'estero.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "falsificazione di monete, spendita e introduzione nello Stato, previo concerto di monete falsificate" (art. 453 c.p.), "alterazione di monete" (art. 454 c.p.), "spendita e introduzione nello Stato, senza concerto, di monete falsificate" (art. 455 c.p.), "spendita di monete falsificate ricevute in buona fede" (art. 457 c.p.).

Ancorché l'attività tradizionale della Banca sia propriamente incentrata sulla gestione dei valori appare remota la possibilità che operatori interni della Banca pongano in essere, autonomamente ovvero in concorso con terzi, nell'interesse della stessa, fatti di alterazione o contraffazione di valori.

Maggiori rischi si possono, invece, rinvenire in relazione alla messa in circolazione di valori falsificati e/o contraffatti posto che potrebbe sussistere la responsabilità amministrativa della Banca nel caso in cui, anche in assenza di concerto con gli autori della falsificazione, un operatore bancario, dubitando della autenticità di taluni valori al momento della ricezione, pur senza avere conoscenza certa della loro falsità, li mettesse in circolazione nell'intento di evitare alla Banca pregiudizi od anche solo gli inconvenienti derivanti dalla rilevazione e dalla denunzia della falsità dei valori alle Autorità competenti.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo si articola nelle seguenti attività:

- movimentazione dei valori (operazioni di sportello, cassa continua, gestione ATM, rimessa valori alle Filiali e versamenti in Banca d'Italia, contazione esterna);
- monitoraggio ed esame degli stessi;
- gestione dei valori ed in particolare delle banconote sospette di falsità (ritiro delle banconote, compilazione verbale, trasmissione del verbale e della banconota alle Autorità competenti ed archiviazione della documentazione).

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti, nell'ambito di ciascuna fase operativa del processo. In particolare:
  - tutti i soggetti che intervengono nel processo di movimentazione di valori devono essere individuati e autorizzati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
  - la stipula di rapporti contrattuali con intermediari addetti alla lavorazione dei valori deve essere autorizzata da soggetti a ciò facoltizzati in base al vigente sistema dei poteri e delle deleghe.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo.

- Attività di controllo: la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna Struttura/Punto Operativo interessata nello svolgimento delle attività di trattazione dei valori inerenti all'esecuzione del processo oggetto del presente protocollo. In particolare:
  - sotto la responsabilità del Responsabile della Struttura/Direttore del Punto Operativo, si riscontrano con periodicità semestrale i valori in carico a tutti gli operatori (controllo da non far coincidere con i passaggi di consegna);
  - con riferimento alla cassa continua/raccolta valori tramite intermediari, l'apertura del mezzo corazzato, il riscontro dei contenitori e dei valori deve avvenire con il concorso di due addetti senza soluzione di continuità;

- con riferimento alle attività di gestione delle apparecchiature ATM, l'apertura del mezzo corazzato, il caricamento delle banconote, il riscontro dei valori, il recupero delle carte catturate e la quadratura deve avvenire con il concorso di due addetti senza soluzione di continuità;
- il Responsabile della Struttura/Direttore del Punto Operativo, o addetto designato, procede almeno una volta al mese alla verifica a campione del contenuto quali/quantitativo delle mazzette oggetto di rimessa, annotando i controlli effettuati e le relative risultanze.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - la realizzazione delle operazioni nella esecuzione degli adempimenti di cui alla messa in circolazione di valori prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle operazioni effettuate;
  - al fine di consentire la ricostruzione delle responsabilità, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei valori, inclusa quella rimessa alla Banca d'Italia con riferimento alla trasmissione di banconote sospette di falsità.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei valori, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare tutti i soggetti che, nell'espletamento delle attività di propria competenza, a qualunque titolo si trovino a dover trattare valori:

- devono essere appositamente incaricati;
- sono tenuti ad operare con onestà, integrità, correttezza e buona fede;
- sono tenuti a prestare particolare attenzione in relazione alle negoziazioni con clientela non sufficientemente conosciuta ovvero avente ad oggetto importi di rilevante entità;
- sono tenuti ad effettuare uno scrupoloso controllo sui valori ricevuti, al fine di individuare, ove presente, quelli sospetti di falsità. L'attività di identificazione può avvenire anche attraverso l'utilizzo di apparecchiature di selezione e accettazione delle banconote, atte a verificare sia l'autenticità sia l'idoneità alla circolazione delle banconote oppure a verificarne

esclusivamente l'autenticità, oppure mediante controlli di autenticità da parte di personale addestrato, attraverso accertamenti manuali e senza l'ausilio di dispositivi di selezione e accettazione;

- sono tenuti, in presenza di banconote sospette di falsità, a predisporre tempestivamente un verbale di ritiro delle banconote sospette di falsità ed a farne segnalazione alle competenti Autorità (UCAMP, Banca d'Italia) con le modalità ed entro i termini prescritti dalla normativa interna;
- custodire le banconote sospette di falsità per le quali è stato redatto il verbale in idonei mezziforti nel periodo intercorrente tra la data di accertamento/ritiro del valore a quella di inoltro alla Banca d'Italia;
- immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque tentativo di messa in circolazione di banconote o valori sospetti di falsità da parte della clientela o di terzi del quale il personale risulti destinatario o semplicemente a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso;

Inoltre,

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei valori, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a fornitori di servizi eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di fornitori di servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- mettere in circolazione, in concorso o meno con terzi, valori falsi. L'addetto che riceva in buona fede una banconota ed abbia, successivamente, dei dubbi sulla sua legittimità non deve tentare a sua volta di metterla nuovamente in circolazione ovvero restituire la banconota sospetta di falsità all'esibitore, tagliarla a metà o distruggerla;
- contravvenire a quanto previsto dalla normativa vigente in materia di ritiro dalla circolazione e trasmissione alla Banca d'Italia delle banconote denominate in euro sospette di falsità.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.4 Area sensibile concernente i reati societari

7.4.1 Fattispecie di reato

Premessa

L'art. 25-ter del D. Lgs. n. 231/2001 contempla la maggior parte dei reati societari non specificamente riferibili all'esercizio della specifica attività bancaria e pertanto sono qualificabili come reati generali.

I reati societari considerati hanno ad oggetto differenti ambiti di interesse tra i quali assumono particolare rilevanza la formazione del bilancio, le comunicazioni esterne, talune operazioni sul capitale, l'impedito controllo e l'ostacolo all'esercizio delle funzioni di vigilanza, fattispecie accomunate dalla finalità di tutelare la trasparenza nei documenti contabili e nella gestione societaria e la corretta informazione ai soci, ai terzi ed al mercato in generale.

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili ed ai controlli delle Autorità di Vigilanza, si rileva che la Banca – anche in quanto appartenente al gruppo bancario Intesa Sanpaolo, società quotata - si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione nonché una serie di obblighi ed adempimenti in relazione ai rapporti con le Autorità, con la conseguenza che le modalità di gestione del rischio dei reati qui considerati risultano replicare comportamenti già consolidati nella prassi bancaria o, comunque, derivanti dall'applicazione delle norme primarie e regolamentari vigenti.

Si elencano qui di seguito le fattispecie contemplate dall'art. 25-ter del Decreto.

False comunicazioni sociali (art. 2621 c.c.)

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

Questi reati si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci ai creditori o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della Società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;

- le informazioni false o omesse devono essere rilevanti - vale a dire devono essere superiori a certe soglie prefissate dalla legge - e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. Qualora le alterazioni siano inferiori alle soglie rilevanti, sono comunque applicate nei confronti delle persone fisiche che hanno posto in essere la condotta sanzioni amministrative pecuniarie e sanzioni interdittive;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- il reato di cui all'articolo 2622 c.c. richiede l'ulteriore circostanza che le informazioni, false od omesse, abbiano provocato un danno patrimoniale alla società, ai soci o ai creditori. Inoltre, esso è punibile solo a querela della parte lesa, salvo che si tratti di società quotate;
- la Legge n. 262/2005 ("Legge sul Risparmio") ha esteso il novero dei soggetti che possono compiere i reati di cui agli artt. 2621 e 2622 c.c. ai "dirigenti preposti alla redazione dei documenti contabili societari" ed ha altresì inasprito le pene detentive previste per il reato di cui all'art. 2622 c.c. nel caso in cui il fatto sanzionato abbia cagionato un grave nocumento ai risparmiatori.

Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 27 D. Lgs. n. 39/2010)

Il Decreto Legislativo n. 39/2010, che ha riordinato la disciplina della revisione legale dei conti, ha abrogato, a decorrere dal 7 aprile 2010, l'art. 2624 del codice civile, concernente il reato di falsità nelle relazioni o nelle comunicazioni delle società di revisione, sostituendolo con la nuova fattispecie prevista dall'art. 27 del D. Lgs. stesso.

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, circa la situazione economica, patrimoniale o finanziaria della società sottoposta a revisione, al fine di conseguire per sé o per altri un ingiusto profitto, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni.

L'illecito è più severamente sanzionato se: la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni; concerne la revisione di determinati enti qualificati dal predetto Decreto "di interesse pubblico" (tra cui le società quotate, gli emittenti di strumenti finanziari diffusi tra il pubblico in maniera rilevante, le banche, alcune imprese di assicurazione, le SIM, le SGR, le SICAV, gli intermediari finanziari di cui all'art. 107 T.U.B.); è commesso per denaro o altra utilità; è commesso in concorso con gli esponenti della società sottoposta a revisione.

Soggetti attivi sono in primis i responsabili della società di revisione (reato proprio). Peraltro l'art. 27 prevede ora espressamente la punibilità di chi dà o promette il denaro o l'utilità e dei direttori

generali, dei componenti l'organo amministrativo e dell'organo di controllo degli enti di interesse pubblico, che abbiano concorso a commettere il fatto.
Poiché l'art. 25-ter del D. Lgs. n. 231/2001, che richiama l'art. 2624 del codice civile, non è stato conseguentemente modificato sostituendo il richiamo alla norma abrogata con quello alla nuova disposizione, si pongono seri dubbi sulla permanente configurabilità della responsabilità degli enti per le condotte in questione.

Impedito controllo (art. 2625 comma 2 c.c. . e art. 29 D. Lgs. n. 39/2010)

Il reato di cui all'art. 2625 comma 2 del codice civile si verifica nell'ipotesi in cui gli amministratori impediscano od ostacolino, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri Organi societari procurando un danno ai soci. Il reato è punito a querela della persona offesa e la pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.
L'art. 2625 c.c. contemplava anche il reato di impedito controllo degli amministratori nei confronti della società di revisione. Tale reato è stato espunto dall'art. 2625 c.c. dal D. Lgs. n. 39/2010, che ha riordinato la disciplina della revisione legale dei conti, ed è ora punito ai sensi dell'art. 29 di tale decreto, in vigore dal 7 aprile 2010, che prevede la procedibilità d'ufficio e sanzioni più gravi se viene procurato un danno ai soci e a terzi, o nel caso di revisione legale di enti di interesse pubblico.
Poiché l'art. 25-ter del D. Lgs. n. 231/2001 non è stato conseguentemente modificato con l'inserimento di un richiamo anche al citato art. 29, si pongono seri dubbi sulla permanente configurabilità della responsabilità degli enti per le condotte in questione concernenti l'attività di revisione.

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

La condotta tipica prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche mediante il compimento di operazioni simulate, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

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

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.
Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

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

Il reato in questione si perfeziona con l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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

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

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

Questo reato si perfeziona quando l'amministratore di una società con titoli quotati in un mercato regolamentato italiano o dell'Unione Europea o diffusi in misura rilevante tra il pubblico, ovvero soggetta a vigilanza ai sensi del Testo Unico Bancario, del Testo Unico dell'Intermediazione Finanziaria o delle norme disciplinanti le attività assicurative o le forme pensionistiche complementari, non comunica, nelle forme e nei termini previsti dall'art. 2391 c.c, all'organo al quale partecipa ovvero alla società e comunque al Collegio Sindacale, l'interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società in questione, ovvero se si tratta di amministratore delegato non si astiene dall'operazione cagionando in tal modo un danno alla società o a terzi.

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

Tale reato si perfeziona nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

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

Il reato si perfeziona con la ripartizione da parte dei liquidatori di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Illecita influenza sull'assemblea (art. 2636 c.c.)
La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Aggiotaggio (art. 2637 c.c.)
La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)
Il reato in questione si realizza nel caso in cui, col fine specifico di ostacolare l'attività delle autorità pubbliche di vigilanza, si espongano in occasione di comunicazioni ad esse dovute in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero si occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che si era tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi.
Il reato si perfeziona altresì mediante qualsiasi condotta attiva od omissiva che in concreto determini un ostacolo allo svolgimento delle funzioni demandate alle Autorità di Vigilanza.
La pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

Falso in prospetto (art. 173-bis D. Lgs. n. 58/1998**)**
La legge 262/2005 (cosiddetta "Legge sul Risparmio") ha abrogato l'art. 2623 c.c., concernente il falso in prospetto, sostituendolo con una nuova fattispecie inserita all'interno del corpo normativo del Testo Unico delle disposizioni in materia di intermediazione finanziaria di cui al D. Lgs. n. 58/1998 (di seguito T.U.F.).
Il nuovo art. 173-bis del T.U.F punisce la condotta di chi espone false informazioni od occulta dati o notizie nei prospetti richiesti ai fini della sollecitazione al pubblico risparmio o dell'ammissione

alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio.
Affinché tale condotta integri gli estremi del reato, è indispensabile che il soggetto che la pone in essere agisca con l'intenzione di ingannare i destinatari dei prospetti, al fine di conseguire un ingiusto profitto, per sé o per altri. Occorre altresì che le informazioni false od omesse siano idonee ad indurre in errore i loro destinatari.
Poiché la Legge sul Risparmio non è intervenuta sul testo dell'art. 25-ter del D. Lgs. n. 231/2001, sostituendo espressamente il richiamo all'art. 2623 c.c. in esso contenuto con quello all'art. 173-bis del T.U.F., si pongono seri dubbi sulla configurabilità della responsabilità amministrativa degli Enti a fronte della commissione del reato punito da tale nuova fattispecie.

7.4.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati societari sono le seguenti:

- Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione;
- Gestione dell'informativa periodica;
- Gestione dei rapporti con le Autorità di Vigilanza.

Si riportano di seguito, per le prime due sopraelencate attività sensibili, i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili a dette attività e che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime. Quanto all'attività indicata all'ultimo punto si rimanda al protocollo per la "Gestione dei rapporti con le Autorità di Vigilanza", avente la specifica finalità di prevenire, oltre al reato di corruzione, anche il reato societario di cui all'art. 2638 c.c..

7.4.2.1. Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione

Premessa

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli Organi e le Strutture della Banca coinvolte nella gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione in essere in occasione di verifiche e di controlli svolte da tali Organi, in ottemperanza alle prescrizioni di legge.

Ai sensi del D. Lgs. n. 231/2001, il processo in oggetto potrebbe presentare potenzialmente occasioni per la commissione del reato di "impedito controllo", ai sensi dell'art. 2625 del codice civile nonché dei reati di cui all'art. 27 del D. Lgs. n. 39/2010 (per quanto concerne la fattispecie di false relazioni o comunicazioni da parte dei responsabili della revisione, commessa in concorso con gli organi della società sottoposta a revisione) e all'art. 29 del medesimo Decreto (concernente la fattispecie di impedimento od ostacolo alle attività di revisione legale), che potrebbero anch'essi rilevare ai fini della responsabilità degli enti qualora fossero superate le riserve espresse al riguardo nel precedente paragrafo 7.4.1..

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti in oggetto.

Descrizione del Processo

Nell'ambito dell'attività di verifica propria del Collegio Sindacale e della Società di Revisione, la gestione dei rapporti con tali soggetti si articola nelle seguenti attività:

- comunicazione delle informazioni periodiche previste;
- comunicazione di informazioni e di dati societari e messa a disposizione della documentazione, sulla base delle richieste ricevute.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare, i rapporti con il Collegio Sindacale e la Società di Revisione, sono intrattenuti dal Responsabile della struttura di riferimento o dai soggetti dal medesimo appositamente incaricati.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Collegio Sindacale e la Società di Revisione al fine di garantire, per tutte le fasi del processo, un meccanismo di maker e checker.

- Partecipazione regolare e continua del Collegio Sindacale alle riunioni del Consiglio di Amministrazione, a garanzia della effettiva conoscenza da parte dell'Organo di Controllo in merito alle scelte strategiche della Banca.

- Tempestiva e completa evasione delle richieste di documentazione specifica avanzate dal Collegio Sindacale – per il tramite della Segreteria Generale della Banca - nell'espletamento della propria attività di vigilanza e controllo.

- Tempestiva e completa evasione, a cura delle strutture competenti, delle richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili: ciascuna Struttura ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori.

- Tempestiva e completa messa a disposizione della Società di Revisione, da parte delle strutture interessate, della documentazione disponibile relativa alle attività di controllo ed ai processi operativi seguiti, sui quali i revisori effettuano le proprie attività di verifica.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo del Collegio Sindacale;

- verifica e conservazione delle dichiarazioni di supporto per la predisposizione delle Representation Letter, con firma delle stesse da parte del Rappresentante Legale e del Direttore Generale, rilasciate alla Società di Revisione;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla gestione dei rapporti con il Collegio Sindacale e la Società di Revisione.

Principi di comportamento

Le Strutture e gli Organi della Banca, a qualsiasi titolo coinvolti nella gestione dei rapporti con il Collegio Sindacale e la Società di Revisione, sono tenute alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni ed agli eventuali adempimenti richiesti nel presente protocollo, in conformità alle disposizioni di legge esistenti in materia nonché alle eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare:

- devono essere puntualmente trasmesse le comunicazioni periodiche al Collegio Sindacale – per il tramite della Segreteria Generale della Banca - e alla Società di Revisione, e tempestivamente riscontrate le richieste/istanze pervenute dagli stessi;
- i membri del Consiglio di Amministrazione e i dipendenti che, a qualunque titolo, siano coinvolti in una richiesta di produzione di documenti o di informazioni da parte del Collegio Sindacale o da qualunque dei suoi membri – per il tramite della Segreteria Generale della Banca – nonché della Società di Revisione pongono in essere comportamenti improntati alla massima correttezza e trasparenza e non ostacolano in alcun modo le attività di controllo e/o di revisione;
- i dati ed i documenti devono essere resi disponibili in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete, fedeli e veritiere;
- ciascuna Struttura aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata ai membri del Collegio Sindacale e ai Revisori, nell'ambito della propria attività, ivi inclusa quella trasmessa in via elettronica.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre il Collegio Sindacale e la Società di Revisione in errore di valutazione tecnico-economica della documentazione presentata;
- promettere o dare somme di denaro o altre utilità a membri del Collegio Sindacale o della Società di Revisione con la finalità di promuovere o favorire interessi della Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.4.2.2. Gestione dell'informativa periodica

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Banca.

Ai sensi del D. Lgs. n. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare potenzialmente occasioni per la commissione del reato di "false comunicazioni sociali", così come disciplinato agli artt. 2621 e 2622 del Codice Civile.

La Capogruppo è sottoposta a precisi obblighi informativi di bilancio in qualità di società quotata sul mercato regolamentato italiano. Il processo di predisposizione dei documenti in oggetto è pertanto disciplinato da apposito regolamento approvato dal Consiglio di Gestione di Intesa Sanpaolo S.p.A. con parere favorevole del Consiglio di Sorveglianza, in risposta alle sollecitazioni provenienti dall'art. 154-bis del T.U.F., che ha qualificato normativamente la figura del "Dirigente Preposto alla redazione dei documenti contabili societari" prevedendo specifiche responsabilità funzionali a garantire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria del Gruppo.

Il Regolamento, denominato "Linee guida di governo amministrativo finanziario" e recepito con delibera del Consiglio di Amministrazione della Cassa di Risparmio del Veneto S.p.A., definisce i principi di riferimento, i ruoli e le responsabilità attribuite alle strutture della Banca in relazione al processo afferente il presente Protocollo, di cui deve intendersi parte integrante. Il Regolamento prevede, in particolare, che le procedure sensibili ai fini dell'informativa finanziaria siano oggetto di formalizzazione e di verifica, al fine di pervenire alla valutazione della loro adeguatezza richiesta dal citato art. 154-bis del T.U.F., garantendone l'affidabilità e, in particolare, il presidio dei sistemi di controllo interno funzionali alla formazione del bilancio e di ogni altra comunicazione di ordine finanziario a livello di Gruppo; tali procedure rappresentano pertanto le regole operative di dettaglio del presente protocollo.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Nell'ambito dei processi sensibili ai fini dell'informativa finanziaria, particolare rilievo assumono le attività strettamente funzionali alla produzione del bilancio d'esercizio, delle situazioni contabili infrannuali, e l'alimentazione del reporting package per il bilancio consolidato del Gruppo, la determinazione degli oneri fiscali e lo svolgimento degli adempimenti relativi alle imposte dirette ed indirette. Tali attività attengono ai seguenti processi aziendali:

- Gestione della contabilità e delle segnalazioni di vigilanza;
- Gestione del bilancio d'impresa e del reporting package per il bilancio consolidato del Gruppo;
- Gestione degli adempimenti fiscali.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

I documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Banca devono essere redatti in base alle specifiche procedure, prassi e logiche aziendali e di Gruppo in essere che:

- identificano con chiarezza e completezza le funzioni interessate nonché i dati e le notizie che le stesse devono fornire;
- identificano i criteri per le rilevazioni contabili dei fatti aziendali e per la valutazione delle singole poste;
- determinano le scadenze, gli argomenti oggetto di comunicazione e informativa, l'organizzazione dei relativi flussi e l'eventuale richiesta di rilascio di apposite attestazioni;
- prevedono la trasmissione di dati ed informazioni alla Struttura responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema;

- prevedono criteri e modalità per l'elaborazione dei dati della Banca necessari per la formazione del bilancio consolidato del Gruppo e la trasmissione degli stessi alla Controllante.

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Ruoli e responsabilità definiti:
  - ogni singola Struttura è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
  - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto, in particolare per quanto riguarda il passaggio a perdite;
  - sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
  - la verifica dell'adeguatezza dei processi sensibili ai fini della informativa contabile e finanziaria nonché dei relativi controlli è affidata ad una specifica struttura della funzione Amministrazione che rappresenta altresì l'interfaccia del Servizio di Governance Amministrativo Finanziaria della Capogruppo con il quale si coordina per la redazione dei documenti contabili e societari ed alla funzione di Internal Audit nell'ambito dello svolgimento della sua attività.

- Segregazione delle funzioni:
  - il processo di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Banca prevede il coinvolgimento di distinte Strutture, operanti nelle diverse fasi del processo in base ai principi riportati nel documento "Linee Guida di governo amministrativo finanziario".

- Attività di controllo:
  - le attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Banca sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali. Si riportano nel seguito i principali controlli svolti dalle singole Strutture:
    - verifiche, con cadenza periodica, dei saldi sulle ldei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;
    - verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le Unità interessate che hanno

alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
- esistenza di controlli maker e checker attraverso i quali la persona che esegue l'operazione è differente da quella che la autorizza, previo controllo di adeguatezza;
- produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
- analisi degli scostamenti, attraverso il confronto tra i dati contabili esposti nel periodo corrente e quelli relativi a periodi precedenti;
- controllo di merito in sede di accensione di nuovi conti ed aggiornamento del piano dei conti;
- quadratura della versione definitiva del bilancio con i dati contabili.

- La verifica dell'adeguatezza dei processi sensibili ai fini dell'informativa contabile e finanziaria e dell'effettiva applicazione dei relativi controlli è articolata nelle seguenti fasi:
  - verifica del disegno dei controlli;
  - test dell'effettiva applicazione dei controlli;
  - identificazione delle criticità e dei piani di azione correttivi;
  - monitoraggio sull'avanzamento e sull'efficacia delle azioni correttive intraprese.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - il processo decisionale, con riferimento alle attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Banca è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
  - tutte le scritture di rettifica effettuate dalle singole Strutture responsabili dei conti di propria competenza o dalla Struttura deputata alla gestione del Bilancio, sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati ed, analiticamente, lo sviluppo dei relativi calcoli;
  - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascuna Struttura coinvolta per le voci contabili di propria competenza;

- tutta la documentazione di supporto alla stesura del bilancio è archiviata presso la Struttura deputata alla gestione del Bilancio e/o presso le strutture coinvolte nel processo di redazione delle disclosures.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nelle attività di tenuta della contabilità e della successiva predisposizione/deposito delle comunicazioni sociali in merito alla situazione economico e patrimoniale della Banca (bilancio di esercizio, relazione sulla gestione, relazioni trimestrali e semestrali, ecc.) e del Gruppo (reporting package per il bilancio consolidato) sono tenute ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia, nonché le norme contenute nelle "Linee Guida di governo amministrativo finanziario" e nelle procedure che disciplinano le attività in questione, norme tutte improntate a principi di trasparenza, accuratezza e completezza delle informazioni contabili al fine di produrre situazioni economiche, patrimoniali e finanziarie veritiere e tempestive anche ai sensi ed ai fini di cui agli artt. 2621 e 2622 del Codice Civile. In particolare, le Strutture della Banca sono tenute a tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Banca;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Banca.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.5 Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona

7.5.1 Fattispecie di reato

Premessa

Attraverso ripetuti interventi legislativi sono state introdotte nel sistema della responsabilità amministrativa degli Enti varie categorie di illeciti, con la comune finalità di contrastare fenomeni di criminalità che destano particolare allarme a livello internazionale, specie in relazione a reati di matrice politico-terroristica, oppure commessi nei settori e con le forme tipiche della delinquenza organizzata, anche transnazionale, o particolarmente lesivi di fondamentali diritti umani.

Il settore bancario e, con esso, la politica del Gruppo Intesa Sanpaolo ha da sempre dedicato particolare attenzione ed impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo, impegno questo che la Banca assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti e del buon funzionamento del sistema nel suo complesso Inoltre, nell'esercizio dell'attività bancaria e finanziaria è di particolare evidenza il rischio di mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

Si fornisce qui di seguito una sintetica esposizione delle categorie di fattispecie in questione.

* * *

Delitti con finalità di terrorismo o di eversione dell'ordine democratico

L'art. 25-quater del Decreto dispone la punibilità dell'ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'ente stesso, delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale, dalle leggi speciali o in violazione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9.12.1999.

La norma non prevede un elenco di reati chiuso e tassativo, ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente[1]..

[1] L'art. 270-sexies c.p. considera connotate da finalità di terrorismo le condotte che possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto, o di

Si menzionano di seguito le principali fattispecie che possono venire in considerazione.

A) Delitti con finalità di terrorismo o eversione dell'ordine democratico previsti dal codice penale o da leggi penali speciali.

Si tratta dei delitti politici, cioè contro la personalità interna ed internazionale dello Stato, contro i diritti politici del cittadino, nonché contro gli Stati esteri, i loro Capi e i loro rappresentanti.

Le fattispecie di maggior rischio sono quelle concernenti la "**Partecipazione a prestiti a favore del nemico"** (art. 249 c.p.), il "**Sequestro di persona a scopo di terrorismo o di eversione"** (art. 289-bis c.p.) e il reato di cui all'art. 270-bis c.p., denominato "**Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico**". In particolare, tale ultima fattispecie punisce anche qualsiasi forma di finanziamento a favore di associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione.

Si richiama inoltre l'attenzione sui reati a danno del patrimonio, ed in particolare sulle fattispecie di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, beninteso qualora commessi strumentalmente al perseguimento di finalità di terrorismo o eversione dell'ordine democratico.

Accanto alle disposizioni del codice penale, vengono in considerazione i reati previsti in leggi speciali attinenti alle più varie materie (ad. es. in materia di armi, di stupefacenti, di tutela ambientale, ecc.) nonché tutta quella parte della legislazione italiana, emanata negli anni '70 e 80, volta a combattere il terrorismo(ad es. in tema di sicurezza della navigazione aerea e marittima, ecc.).

B) I delitti con finalità di terrorismo previsti dalla Convenzione di New York del 1999.

Il richiamo a tale disposizione tende chiaramente ad evitare possibili lacune nella disciplina, già generale e generica, dettata ed è dunque diretto a rafforzare e completare l'ambito di riferimento anche mediante il rinvio ad atti internazionali.

* * *

Delitti di criminalità organizzata

---

destabilizzare le strutture. strutture politiche fondamentali, costituzionali, economiche e sociali, nonché le altre condotte previste da convenzioni o da norme internazionali. Secondo la giurisprudenza (Cass. pen. n. 39504/2008) l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

L'art. 24-ter del Decreto, inserito dalla L. n. 94/2009, prevede innanzitutto un gruppo di reati inerenti alle varie forme di associazioni criminose, e cioè:

- Associazione per delinquere generica (art. 416 c.p., primi cinque commi);
- Associazione di tipo mafioso, anche straniera e scambio elettorale politico-mafioso (artt. 416-bis e 416-ter);
- Associazione per delinquere finalizzata alla commissione di delitti in tema di schiavitù, di tratta di persone e di immigrazione clandestina (art. 416 c.p., comma 6);
- Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990).

Con riferimento alle fattispecie di associazioni per delinquere sopra considerate, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente dell'ente potrebbe determinare la responsabilità amministrativa dell'ente stesso, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'ente medesimo. E' inoltre richiesto che il vincolo associativo si esplichi attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta cioè l'occasionale accordo per la commissione di uno o più delitti determinati. La giurisprudenza ritiene altresì possibile il concorso nel reato di associazione criminosa da parte di colui che, pur non partecipando all'associazione stessa, fornisca un apporto sostanziale, anche se episodico, alla sua sussistenza od al perseguimento dei suoi scopi.

L'associazione di tipo mafioso (art. 416-bis c.p.) si distingue dalla associazione per delinquere generica per il fatto che coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, oppure - anche non mediante la commissione di delitti, ma pur sempre con l'uso del metodo mafioso - per acquisire in modo diretto od indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

La norma si applica anche alla camorra e alle altre associazioni, comunque denominate, anche straniere, che presentino i connotati mafiosi predetti. Lo scambio elettorale politico-mafioso invece è commesso da chi ottiene una promessa di voti contro erogazione di denaro.

Gli altri due tipi di associazioni criminose sono invece caratterizzate dall'essere preordinate al fine della commissione degli specifici reati in esse considerati, vale a dire: dei reati in tema di schiavitù,

di tratta di persone e di immigrazione clandestina (puniti ai sensi degli artt. 600, 601 e 602 c.p. nonché dell'art. 12 comma 3-bis del D. Lgs. n. 286/1998) e dei reati di illecita produzione, traffico o detenzione di sostanze stupefacenti o psicotrope. Questi specifici reati-fine (eccetto quelli in materia di stupefacenti) costituiscono di per sé autonomi reati presupposto della responsabilità dell'ente, come meglio si dirà nel prosieguo a proposito dei reati contro la persona e dei reati transnazionali.

L'art. 24-ter prevede inoltre la generica categoria dei delitti di qualsivoglia tipo, commessi avvalendosi del metodo mafioso od al fine di favorire l'attività di una associazione mafiosa, fermo restando, per la responsabilità dell'ente, il requisito dell'interesse o del vantaggio del medesimo.
La prima circostanza si ritiene ricorra allorquando il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione, quale ad esempio la minaccia avvalendosi dello sfruttamento della "fama" di organizzazioni criminali operanti nell'ambito di un determinato territorio. L'ipotesi della commissione di un reato di qualsiasi tipo atto ad agevolare l'attività di una associazione mafiosa si verifica quando il soggetto abbia agito con tale scopo specifico e la sua condotta sia concretamente idonea a realizzare tale risultato, come ad esempio nel caso del reato di riciclaggio compiuto essendo a conoscenza della riferibilità dell'operazione ad una associazione mafiosa.
Infine, ai sensi del medesimo art. 24-ter, rilevano i seguenti reati, solitamente, anche se non necessariamente, realizzati nell'ambito di organizzazioni criminali.

Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.).
Il reato consiste nel sequestro di una persona con lo scopo di conseguire per sé o per altri un ingiusto profitto in cambio della liberazione. Il profitto potrebbe anche consistere in un vantaggio di natura non patrimoniale. In casi particolari potrebbero essere ritenuti corresponsabili del reato anche coloro che, pur non avendo partecipato al sequestro, si attivino per far sì che gli autori possano conseguire il riscatto, contribuendo al protrarsi delle trattative e conseguentemente, della privazione della libertà personale del sequestrato, o al conseguimento del profitto da parte dei sequestratori. Potrebbe invece integrare il reato di riciclaggio l'attività di chi interviene nel trasferimento, nella circolazione o nell'impiego di somme di denaro o di altri beni, essendo a conoscenza della provenienza dal reato in questione.

Delitti in tema di armi e di esplosivi (art. 407 comma 2, lettera a), n. 5).
Si tratta di fattispecie previste dalle leggi speciali vigenti in materia (in particolare dalla L. n. 110/1975 e dalla L. n. 895/1967), che puniscono le condotte di illegale fabbricazione, introduzione nello Stato, vendita, cessione, detenzione e porto abusivo di esplosivi, di armi da guerra e di armi

comuni da sparo, con esclusione di quelle da bersaglio da sala, o ad emissione di gas, o ad aria compressa. Anche in questo caso, come per il reato precedente, eventuali collusioni in qualsiasi forma degli operatori bancari con gli autori dei reati in questione o l'espletamento di attività, quali ad esempio la concessione di finanziamenti, con la consapevolezza di anche solo indirettamente favorirli, potrebbe comportare il concorso nei reati stessi o l'imputabilità per altri reati, quali ad esempio il riciclaggio.

* * *

Delitti transnazionali

La responsabilità degli Enti per tale categoria di reati è sancita dalla L. n. 146/2006, al fine di più efficacemente contrastare le organizzazioni criminali che agiscono a livello internazionale.
Si considera transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato e:

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

Si descrivono di seguito le fattispecie penali che, se integrate dagli elementi costitutivi dell'interesse o del vantaggio dell'ente e della transnazionalità (sui quali pure si ritiene debba sussistere la consapevolezza da parte del soggetto agente), possono dar luogo alla responsabilità dell'ente.

Associazioni per delinquere previste dagli artt. 416 e 416-bis c.p. ovvero finalizzate al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. n. 43/1973) o al traffico di stupefacenti (art. 74 D.P.R. n. 309/1990)

Per la definizione delle condotte di base dei reati associativi in questione si rimanda a quanto sopra osservato a proposito dei delitti di criminalità organizzata. Si ritiene che, ricorrendo le caratteristiche della transnazionalità, siano applicabili all'ente unicamente le sanzioni previste dalla L. n. 146/2006 e non anche quelle di cui all'art. 24-ter del Decreto.

Reati in tema di immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del D. Lgs. n. 286/1998)

La norma punisce le condotte consistenti nel trasportare illegalmente stranieri nel territorio dello Stato, nel promuovere, dirigere, organizzare o finanziare tale trasporto, oppure in altri atti diretti a procurare illegalmente l'ingresso di stranieri nel territorio italiano o di uno Stato diverso da quello di loro appartenenza o residenza permanente. E' però richiesto che ricorra almeno una delle cinque condizioni elencate dalla norma stessa [1].

Le medesime condotte sono punite più severamente se si verifichi la contemporanea presenza di almeno due delle cinque condizioni predette oppure se siano commesse con determinate finalità, quali: il reclutamento di persone destinate alla prostituzione; lo sfruttamento sessuale o lavorativo, lo sfruttamento di minori, o in genere, la finalità di trarre un profitto anche indiretto.

Infine, il comma 5 punisce il favoreggiamento della permanenza dello straniero al fine di trarre un ingiusto profitto dalla sua condizione di illegalità. Si deve ritenere che l'ingiusto profitto sussista quando l'equilibrio delle prestazioni sia fortemente alterato, quale conseguenza dello sfruttamento da parte del soggetto agente dello stato di clandestinità, da lui conosciuto.

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

Il reato è commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano chiamati a rendere dichiarazioni davanti all'autorità giudiziaria, utilizzabili in un procedimento penale, ed abbiano la facoltà di non rispondere.

Si precisa che tale reato può dar luogo alla responsabilità dell'ente anche se commesso senza le caratteristiche della transnazionalità, essendo richiamato, oltre che dalla Legge n.146/2006, anche dall'art. 25-novies del Decreto 2 .

Favoreggiamento personale (art. 378 c.p.)

[1] In sintesi: a) procurato ingresso o permanenza illegale di cinque o più persone; b) pericolo per l'incolumità delle persone trasportate; c) loro trattamento degradante; d) fatti commessi da tre o più persone concorrenti o con utilizzo di servizi di trasporto internazionali o di documenti falsi o illegalmente ottenuti; e) fatti commessi da chi è nella disponibilità di armi o di esplosivi.

[2] La L. n. 116/2009, che ha ratificato la Convenzione ONU contro la corruzione del 31.10.2003, ha introdotto nel D. Lgs. n. 231/2001 l'art. 25-novies, così numerato per palese refuso, essendo già presente nel Decreto un articolo con tale numerazione.

La condotta criminosa consiste nel prestare aiuto a taluno - dopo l'avvenuta commissione di un delitto per il quale la legge stabilisce l'ergastolo o la reclusione e fuori dei casi di concorso nel medesimo - ad eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa. Il reato sussiste anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto. La pena è aggravata quando il delitto commesso è quello di associazione mafiosa.

Si precisa che, per giurisprudenza maggioritaria, integrano il reato anche le false risposte, tese ai fini di cui sopra, alle richieste dell'Autorità Giudiziaria.

* * *

Delitti contro la persona

L'art. 25-quinquies del Decreto elenca talune fattispecie di reato poste a presidio della personalità individuale previste dal codice penale col fine di contrastare aspramente il fenomeno delle "nuove schiavitù" quali prostituzione, tratta degli esseri umani, sfruttamento dei minori, accattonaggio, attività strettamente collegate al proliferare della criminalità organizzata e delle "nuove mafie".

In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate: **"Riduzione o mantenimento in schiavitù" (art. 600 c.p)**, "**Prostituzione minorile" (art. 600-bis c.p.)**, "**Pornografia minorile" (art. 600-ter c.p.)**, **"Detenzione di materiale pornografico" (art. 600-quater c.p.)**, **"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.)**.

Infine, si ricorda che l'art. 25-quater 1 dispone la punibilità dell'ente nel caso di commissione del reato contro la persona di cui all'art. 583-bis c.p. (Pratiche di mutilazione degli organi genitali femminili).

Il rischio di responsabilità per i delitti in questione si può ritenere rilevante solo con riferimento all'ipotesi in cui un esponente o un dipendente della Banca agiscano in concorso con l'autore materiale del reato. La forma di concorso che presenta maggiori profili di rischio è quella connessa alla messa a disposizione di risorse finanziarie o economiche in favore di organizzazioni o di soggetti che pongano in essere reati dei tipi sopra menzionati.

7.5.2 Attività aziendali sensibili

Il rischio che siano posti in essere i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona riguarda principalmente, nell'ambito dell'attività bancaria, le attività di instaurazione dei rapporti

con la clientela, di trasferimento di fondi, l'operatività di "sportello" ed, in particolare, il processo di erogazione del credito, attività che, ai fini della prevenzione dei reati in questione, si devono basare sul fondamentale principio dell'adeguata conoscenza della clientela. Tale principio rappresenta uno dei fondamentali requisiti stabiliti dal D. Lgs. n. 231/2007 concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Le attività sopra individuate sono le medesime nelle quali è più alto il rischio che si verifichino anche reati di riciclaggio. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

Inoltre, per quanto concerne il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, si individua quale attività aziendale sensibile quella inerente alla gestione dei contenziosi e degli accordi transattivi.

Si rimanda pertanto ai protocolli previsti rispettivamente al Capitolo 7.2.2.6 per la "Gestione dei contenziosi e degli accordi transattivi" ed al Capitolo 7.6.2.1 per il "Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose".

7.6 Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

7.6.1 Fattispecie di reato

Premessa

Il D. Lgs. 21.11.2007, n. 231 (di seguito Decreto antiriciclaggio) ed il D. Lgs. 22.6.2007 n. 109, in attuazione di disposizioni comunitarie (Direttiva 2005/60/CE, c.d. "terza direttiva antiriciclaggio") hanno profondamente riordinato la normativa in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di contrasto al finanziamento del terrorismo.

L'art. 25-octies del D. Lgs. n. 231/2001, introdotto dal Decreto antiriciclaggio ha esteso la responsabilità dell'Ente ai reati di ricettazione, riciclaggio e impiego illecito a prescindere da fatto che siano commessi con finalità di terrorismo o di eversione dell'ordine democratico, in ordine alle quali si rimanda al Capitolo 7.5 ed anche qualora non presentino le caratteristiche di transnazionalità in precedenza previste[1].

La finalità del rafforzamento della disciplina della responsabilità amministrativa degli Enti consiste nel prevenire e reprimere più efficacemente il fenomeno dell'immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all'amministrazione della giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza, in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.

Su un piano diverso, ma pur sempre finalizzate al contrasto del riciclaggio e del finanziamento del terrorismo, si collocano le previsioni contenute nel Decreto antiriciclaggio di specifici adempimenti posti a carico delle banche e degli intermediari finanziari in genere (adeguata verifica della clientela; registrazione e conservazione della documentazione delle operazioni; segnalazione di operazioni sospette; comunicazioni delle violazioni dei divieti in tema di denaro contante e dei titoli

[1] Si ricorda che ai sensi dei commi 5 e 6 dell'art. 10 L. n. 146/2006, abrogati dal Decreto antiriciclaggio, il riciclaggio e l'impiego illecito costituivano reati presupposto della responsabilità degli Enti solo se ricorrevano le caratteristiche di transnazionalità previste dall'art. 3 della medesima legge.

al portatore; comunicazione da parte degli Organi di controllo dell'Ente delle infrazioni riscontrate). La violazione di detti obblighi è di per sé sanzionata, ma non comporta la responsabilità amministrativa dell'Ente ai sensi del D. Lgs. n. 231/2001, non essendo detti illeciti ricompresi nell'elencazione dei cosiddetti reati presupposto.
Il Decreto antiriciclaggio, con la previsione di sanzioni per le infrazioni di tali obblighi, ha inteso istituire una tutela preventiva, che prescinde dal ricorrere nelle concrete fattispecie di ipotesi di riciclaggio, ma che mira comunque ad assicurare il rispetto dei fondamentali principi della approfondita conoscenza della clientela e della tracciabilità delle transazioni, al fine di scongiurare anche il mero pericolo di inconsapevole coinvolgimento degli intermediari finanziari in fatti di ricettazione, riciclaggio e impiego illecito di capitali.

E' importante sottolineare che qualora l'operatore bancario contravvenisse a detti adempimenti nella consapevolezza della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato a rispondere per i predetti reati, e potrebbe quindi conseguirne anche la responsabilità amministrativa della Banca ai sensi del D. Lgs. n. 231/2001.

Si fornisce qui di seguito una sintetica descrizione degli elementi costitutivi dei reati in oggetto.

Ricettazione (art. 648 c.p.)
Commette il reato di ricettazione chiunque, allo scopo di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza delittuosa.
E' inoltre richiesta la conoscenza della provenienza delittuosa del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche - quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni - da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

Riciclaggio (art. 648-bis c.p.)
Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti

da un delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
La norma va interpretata come volta a punire coloro che - consapevoli della provenienza delittuosa di denaro, beni o altre utilità - compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati.
Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento. Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione. Con riferimento ai rapporti bancari, ad esempio, la semplice accettazione di un deposito potrebbe integrare la condotta di sostituzione tipica del riciclaggio (sostituzione del denaro contante con moneta scritturale, quale è il saldo di un rapporto di deposito).
Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave ed univoca.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio) c.p..
Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648-ter circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie. Peraltro, in considerazione della ampiezza della formulazione della fattispecie del reato di riciclaggio, risulta difficile immaginare condotte di impiego di beni di provenienza illecita che già non integrino di per sé il reato di cui all'art. 648-bis c.p..

Considerazioni comuni ai tre reati.

Oggetto materiale.
L'oggetto materiale dei reati può essere costituito da qualsiasi entità economicamente apprezzabile e possibile oggetto di scambio, quale il denaro, i titoli di credito, i mezzi di pagamento, i diritti di credito, i preziosi, i beni materiali ed immateriali in genere. Deve però trattarsi di bene o utilità proveniente da delitto, vale a dire esso ne deve costituire il prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato), il profitto (lucro o vantaggio economico ricavato dal reato) o il prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato). Oltre che dai delitti tipicamente orientati alla creazione di capitali illeciti (ad

es.: concussione, corruzione, appropriazione indebita, traffico di armi o di stupefacenti, usura, frodi comunitarie, etc.) anche i reati in materia fiscale potrebbero dar luogo a proventi oggetto di riciclaggio.

Condotta ed elemento soggettivo.
Si deve evidenziare che nel sistema giuridico italiano non costituisce reato di ricettazione, riciclaggio o impiego illecito la condotta, corrispondente ad una delle tre fattispecie in esame, se posta in essere dal medesimo autore del reato di provenienza del bene (cosiddetto "autoriciclaggio"), in quanto considerata un "normale" sviluppo del crimine precedente, per conseguirne i vantaggi o metterne al sicuro i risultati; a titolo di riciclaggio/ricettazione/impiego illecito può essere perseguito solo il terzo estraneo al delitto d'origine, che cooperi per tali fini con il reo. Peraltro, il terzo risponderebbe non di riciclaggio, ma a titolo di concorso nel delitto di provenienza del bene se avesse promesso il suo aiuto nel riciclare i proventi del reato ancor prima della commissione dello stesso, rafforzando così il proposito criminoso del reo.
Con specifico riguardo all'attività bancaria e finanziaria, ai fini dell'individuazione della tipologia delle operazioni con le quali può concretarsi il riciclaggio, va innanzitutto ricordato che il Decreto antiriciclaggio definisce "operazione" la trasmissione o la movimentazione di mezzi di pagamento". Inoltre, il medesimo Decreto all'art. 2 contiene un' elencazione amplissima di condotte qualificabili come riciclaggio per i soli fini del Decreto, vale a dire, essenzialmente, per l'individuazione delle ipotesi che fanno sorgere l'obbligo di segnalazione delle operazioni sospette. Tra queste può ricomprendersi anche l'autoriciclaggio che, come detto, ai sensi della disciplina penale italiana non costituisce reato. Sempre nell'ambito della predetta elencazione, alcune di tali condotte, oltre che rilevare per i fini del Decreto antiriciclaggio, concernono comportamenti che potrebbero integrare quantomeno gli estremi del concorso nei reati in esame, e pertanto, se posti in essere da dipendenti o da soggetti apicali, anche detti comportamenti potrebbero far sorgere la responsabilità amministrativa dell'ente stesso. Infine, l'elencazione in discorso è atta a ricomprendere anche condotte tipiche di altri reati, quali il favoreggiamento personale (art. 378 c.p.) che, se connotato dai requisiti della transnazionalità (al riguardo si rimanda al Capitolo 7.5), può costituire reato presupposto della responsabilità amministrativa degli Enti.

Circa l'elemento soggettivo, come già accennato, i reati in esame devono essere caratterizzati dalla consapevolezza della provenienza delittuosa del bene. Secondo una interpretazione particolarmente rigorosa, sarebbe sufficiente anche l'aver agito nel dubbio della provenienza illecita, accettandone il rischio (cosiddetto dolo indiretto od eventuale). Con riferimento all'operatività bancaria ed agli indici di anomalia delle operazioni contenuti nel "Decalogo" della Banca d'Italia, va osservato che la ricorrenza di taluno di essi in determinate situazioni concrete

potrebbe essere ritenuto, accedendo alla particolarmente rigorosa interpretazione di cui sopra, come una circostanza oggettiva grave ed univoca atta far sorgere il dubbio della provenienza illecita del bene.

7.6.2 Attività aziendali sensibili

Il rischio che si verifichino i reati di riciclaggio nel contesto bancario appare, invero, più marcato, quale rischio tipico del circuito bancario e finanziario, essenzialmente con riferimento ai rapporti con la clientela, ed in particolare concerne:

- l'instaurazione e la gestione dei rapporti continuativi con la clientela[1];
- il trasferimento di fondi;
- l'operatività di sportello.

Meno rilevante appare laddove si abbia riguardo all'impresa bancaria come "società", con riferimento a quelle aree in cui la banca, a prescindere dallo svolgimento delle attività tipiche, compie operazioni strumentali, acquista partecipazioni o movimenta il proprio patrimonio, e ciò in ragione della sviluppata articolazione dei presidi di controllo e delle procedure già imposti dalla normativa di settore.

L'attività di prevenzione si basa sulla approfondita conoscenza della clientela e delle controparti e sulla osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose. Tale protocollo si completa con la normativa aziendale di dettaglio che regolamenta l'attività medesima. Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili - quali la Gestione dei contenziosi e degli accordi transattivi (Capitolo 7.2.2.6), la Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali (Capitolo 7.2.2.8); la Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni (Capitolo 7.2.2.9); la Gestione del patrimonio immobiliare e dei beni mobili aventi valore artistico (Capitolo 7.2.2.11) e la Gestione dei valori (Capitolo 7.3.2.1) - sono previsti alcuni principi di controllo e di comportamento ispirati al medesimo criterio dell'attenta valutazione di fornitori, consulenti e controparti contrattuali in genere, principi che esplicano la loro efficacia preventiva anche in relazione ai reati sopra illustrati.

[1] Per rapporto continuativo ai sensi dell'art. 1, comma 1 lettera s) del D. Lgs. n. 231/2007 si intende ogni rapporto di durata rientrante nell'esercizio dell'attività istituzionale della Banca, che dia luogo a più operazioni di versamento, prelievo o trasferimento di mezzi di pagamento e che non si esaurisce in una sola operazione.

7.6.2.1. Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose

Premessa

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di controllo e di comportamento per il contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose. Si intendono qui richiamate le vigenti disposizioni aziendali, ed in particolare le "Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi".

Il presente protocollo si applica a tutte le strutture della Banca coinvolte nelle attività sensibili sopra individuate nonché nelle attività di presidio dei rischi connessi alla normativa antiriciclaggio.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività, tracciabilità e riservatezza nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Ai fini del contrasto finanziario al terrorismo, al riciclaggio dei proventi di attività criminose, si rimanda ai seguenti ambiti di operatività:

- identificazione e conoscenza della clientela e dei soggetti per conto dei quali i clienti operano, valutandone il profilo di rischio e cioè la probabilità di esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo tramite una apposita procedura di profilatura[5]. La valutazione della sussistenza di tale rischio si basa sulla stessa conoscenza dei clienti e tiene conto, in particolare, di aspetti oggettivi (attività svolte dai clienti, le operazioni da essi

[5] Effettuata secondo le disposizioni previste dall'art. 20 del D. Lgs. n. 231/2007.

compiute e degli strumenti utilizzati[1]) e di aspetti soggettivi (soggetti sottoposti ad obblighi rafforzati di adeguata verifica; soggetti insediati in Paesi/centri caratterizzati da regimi fiscali o antiriciclaggio privilegiati quali quelli individuati dal GAFI come "non cooperativi", etc.). Con riguardo alle caratteristiche soggettive della clientela, particolare attenzione deve essere posta ai soggetti (persone fisiche e giuridiche) "black listed" ovvero ricompresi nelle liste UE, OFAC, ABI-UIF;

- apertura di nuovi rapporti continuativi e aggiornamento/revisione delle informazioni sui clienti esistenti, finalizzati al rispetto del principio della "know your customer rule";
- concessione e gestione delle linee di credito alla clientela (processo del credito);
- monitoraggio operatività e costante valutazione dei rischi di riciclaggio di denaro proveniente da attività illecite o di finanziamento del terrorismo secondo tempistiche e modalità stabilite con riferimento al profilo di rischio assegnato;
- valutazione operatività disposta dalla clientela riguardante soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- assolvimento degli obblighi normativi in materia di registrazione dei rapporti continuativi e delle operazioni disposte dalla clientela e conservazione delle relative informazioni;
- reporting esterno indirizzato alle Autorità di Vigilanza[2] e processi di reporting interno ad esso finalizzate.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti. Tale normativa costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:

- Responsabilità definite:

[1] ad esempio interposizione di soggetti terzi, impiego di strumenti societari, associativi o fiduciari suscettibili di limitare la trasparenza della proprietà e della gestione; utilizzo di denaro contante o di strumenti al portatore.

2 Tali comunicazioni comprendono:

- invio all'UIF delle segnalazioni di operazioni sospette ai sensi degli artt. 41 e 42 D. Lgs. n. 231/2007;
- invio all'UIF delle segnalazioni di blocco o congelamento dei fondi ai sensi del D. Lgs. n. 109/2007;
- invio al MEF delle infrazioni relative alle limitazioni all'uso del contante e dei titoli al portatore ai sensi dell'art. 51 del D. Lgs. n. 231/2007;
- invio all'Autorità di Vigilanza e al MEF delle comunicazioni ai sensi dell'art. 52 del D. Lgs. n. 231/2007.

- la normativa interna individua i soggetti e le Strutture responsabili dell'attivazione/gestione dell'iter dei processi sopra descritti e dei relativi processi di controllo interno;

- Segregazione dei compiti:
  - relativamente ai rapporti continuativi inerenti alla erogazione del credito, esistenza di una segregazione tra i soggetti incaricati della fase istruttoria rispetto ai soggetti facoltizzati alla delibera del finanziamento, fatte salve le eccezioni espressamente previste dalla normativa interna tempo per tempo vigente;
  - nelle situazioni individuate dalle disposizioni di legge e dalla normativa interna che impongono obblighi rafforzati di adeguata verifica della clientela (presenza di un rischio più elevato e altre ipotesi previste dall'art. 28 del Decreto antiriciclaggio), subordinazione dell'apertura di nuovi rapporti, del mantenimento di rapporti preesistenti e dell'esecuzione delle operazioni al rilascio di una autorizzazione da parte di una Struttura diversa da quella operativa;
  - in relazione alle attività di monitoraggio dell'operatività volte ad individuare operazioni potenzialmente sospette, esistenza di una segregazione in base alla quale:
    - gli operatori di Filiale o delle altre Strutture operative monitorano le operazioni relative alla loro area di competenza, segnalando i movimenti anomali al direttore di Filiale o al gestore della relazione col cliente per gli opportuni approfondimenti e/o segnalazioni;
    - il direttore della Filiale o il gestore della relazione col cliente, sulla scorta delle informazioni in proprio possesso, ovvero di segnalazioni pervenute dagli operatori o dalla procedura Gianos (operazioni "inattese"), provvede, se l'operazione risulta sospetta, alla segnalazione della stessa al Responsabile Delegato per la segnalazione delle operazioni sospette;
    - il Responsabile Delegato effettua l'analisi della segnalazione e svolge autonomamente le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno delle segnalazioni alla competente Autorità.

- Attività di controllo: il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:
  - nell'ambito di una puntuale profilatura della clientela verifica, all'atto dell'accensione del rapporto, da parte del Responsabile di ogni Struttura operativa, della correttezza e completezza dei dati censiti in anagrafe, nonché in merito alle informazioni acquisite in relazione alla attività economica svolta; tali informazioni devono essere aggiornate, di

volta in volta, in relazione alle motivazioni economiche sottostanti alle operazioni richieste o eseguite;

- verifica, in occasione della profilatura del cliente e nel continuo, dell'eventuale presenza del nominativo nelle versioni aggiornate delle liste antiterrorismo;
- verifica, nell'ambito della concessione e gestione delle linee di credito alla clientela, della coerenza tra il finanziamento richiesto ed il profilo economico-finanziario del cliente, per una valutazione circa la (potenziale) esposizione a fenomeni di riciclaggio, di finanziamento al terrorismo;
- monitoraggio nel medio-lungo periodo da parte delle Strutture operative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
- monitoraggio e presidio da parte delle Strutture preposte al controllo interno della puntuale esecuzione delle attività delle Strutture operative in merito alla:
  - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
  - valutazione delle operazioni rilevate dalla procedura Gianos (o da altre procedure informatiche in uso);
  - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
  - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
  - registrazione dei rapporti e delle operazioni in AUI e conservazione dei documenti e delle informazioni;
- tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati con modalità che consentano la registrazione procedurale nell'Archivio Unico Informatico con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati. A tale fine è indispensabile procedere alle attività di "integrazione" e "sistemazione" delle operazioni o dei rapporti in stato di "sospeso" entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
- presidio sulla corretta esecuzione degli adempimenti prescritti anche con riferimento alle attività svolte dalle filiali estere;

- adozione di sistemi di controllo informatici atti ad impedire l'operatività riguardanti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi).

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto, in particolare:
    - conservazione riservata e ordinata,, a cura del direttore di Filiale o del gestore della relazione col cliente, di tutta la documentazione relativa alla identificazione e alla profilatura della clientela;
  - archiviazione sistematica di tutta la documentazione relativa all'operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti, presso le strutture operative di competenza;
  - conservazione di traccia completa delle decisioni e delle motivazioni addotte che dovessero portare all'eventuale modifica del profilo del cliente e alla conseguente decisione circa l'inoltro o meno di una segnalazione di operazione sospetta alle Autorità di Vigilanza competenti.

- Riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi, alla profilatura dei clienti ed ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche.

- Formazione: è prevista la sistematica erogazione di attività formative specificamente dedicate ai profili di rischio legati alla normativa antiriciclaggio.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nelle attività di contrasto finanziario al terrorismo, al riciclaggio dei proventi di attività criminose sono tenute ad osservare le modalità

esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare, le Strutture competenti sono tenute a:

- assicurare lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/antiriciclaggio e comunque in tutte le attività che si basano sulla "adeguata conoscenza della clientela";
- verificare e garantire l'aggiornamento/manutenzione/diffusione delle liste interne di soggetti/Paesi/merci interessati da provvedimenti restrittivi emanati da UE, OFAC, ABI-UIF;
- dettagliare nell'ambito di regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal presente protocollo;
- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative ovvero diverse società del Gruppo, collaborare tra loro e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza del cliente e delle sue abitudini operative;
- nei rapporti instaurati con corrispondenti estere, acquisire la documentazione con cui la banca terza dichiari di adempiere agli obblighi antiriciclaggio e/o agli obblighi previsti da normative emanate da altri Stati (in particolare dagli Stati Uniti d'America);
- assicurare con continuità e sistematicità la formazione e l'addestramento del personale sulla normativa antiriciclaggio ed embarghi e sulle finalità dalla stesse perseguite;
- diffondere a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento ed i relativi aggiornamenti.

Inoltre, gli operatori, attenendosi a quanto prescritto nelle procedure aziendali, devono:

- all'atto dell'accensione di rapporti continuativi o del compimento di operazioni oltre la soglia di legge, anche se frazionate:
  - procedere all'identificazione della clientela e verificare l'eventuale presenza del nominativo nelle versioni aggiornate delle liste antiterrorismo;
  - verificare la sussistenza di eventuali titolari effettivi, acquisire informazioni sullo scopo e sulla natura del rapporto o dell'operazione e, qualora il cliente sia una società o un Ente, verificare la sussistenza dei poteri di rappresentanza e la struttura di proprietà e di controllo del cliente;
  - procedere alla profilatura della clientela;
- mantenere aggiornati tutti i dati relativi ai rapporti continuativi al fine di consentire una costante valutazione del profilo economico e finanziario del cliente;

- rinnovare l'adeguata verifica e all'aggiornamento della profilatura della clientela quando, indipendentemente da qualsiasi soglia di importo o di esenzione applicabile, vi sia il sospetto di riciclaggio, di finanziamento del terrorismo o sorgano dubbi sulla veridicità o sull'adeguatezza dei dati identificativi già acquisiti;
- dare avvio all'iter di segnalazione quando sanno o sospettano che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo;
- valutare se dare avvio all'iter di segnalazione in presenza di indici di anomalia anche se non rilevati dalle procedure informatiche, o nei casi in cui risulti impossibile rispettare gli obblighi di adeguata verifica;
- bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi) o per le quali sussista comunque il sospetto di una relazione con il riciclaggio o con il finanziamento del terrorismo;
- inoltrare le comunicazioni delle infrazioni delle disposizioni in tema di limitazioni all'uso del contante e dei titoli al portatore rilevabili nell'operatività della clientela;
- rispettare rigorosamente le procedure interne in tema di registrazione dei rapporti e delle operazioni in AUI e di conservazione della documentazione.

Tutti i dipendenti della Banca, siano essi addetti alle Strutture centrali o territoriali, devono partecipare fattivamente al processo di analisi della clientela e della relativa attività per l'individuazione e la segnalazione di operazioni sospette.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio, con il finanziamento del terrorismo;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;

- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
- mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.7 Area sensibile concernente i reati ed illeciti amministrativi riconducibili ad abusi di mercato

7.7.1 Fattispecie di reato

Premessa

La Legge n. 62/2005 ha introdotto, agli articoli 184 e 185 del D. Lgs. n. 58/1998 (Testo Unico delle disposizioni in materia di intermediazione finanziaria, di seguito T.U.F.), i reati di "abuso di informazioni privilegiate" e di "manipolazione di mercato", oltre a due corrispondenti fattispecie di illecito amministrativo, disciplinate agli artt. 187-bis e 187 ter del T.U.F. medesimo.

La responsabilità amministrativa dell'Ente a fronte delle fattispecie penali di cui agli artt. 184 e 185 del T.U.F è sancita dall'art. 25-sexies del D. Lgs. n. 231/2001. Si rammenta altresì che tra i reati societari che possono dar luogo alla responsabilità degli Enti vi è anche il reato di aggiotaggio (vedi supra paragrafo 7.4.1) riconducibile, al tempo stesso, alla materia degli abusi di mercato in senso lato riferiti, in particolare, agli strumenti finanziari non quotati o per i quali non é stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato.

Per quanto invece concerne gli illeciti amministrativi di cui agli artt. 187-bis e 187-ter, la responsabilità dell'Ente discende dalla previsione contenuta nell'art. 187-quinquies del T.U.F., il quale rimanda ai medesimi principi, condizioni ed esenzioni del D. Lgs. n. 231/2001, ponendo però sempre a carico dell'Ente, a propria discolpa, la prova secondo cui l'autore dell'illecito ha agito esclusivamente nell'interesse proprio o di un terzo.

Le predette norme mirano a garantire l'integrità, la trasparenza, la correttezza e l'efficienza dei mercati finanziari in ottemperanza al principio per cui tutti gli investitori debbono operare in condizioni di uguaglianza sotto il profilo dell'accesso all'informazione, della conoscenza del meccanismo di fissazione del prezzo e della conoscenza delle origini delle informazioni pubbliche.

Va precisato che ai sensi dell'art. 182 del T.U.F. le condotte sanzionate sono punite secondo la legge italiana anche se commesse all'estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano in un sistema multilaterale di negoziazione italiano per i quali l'ammissione é stata richiesta o autorizzata dall'emittente. Nel caso in cui i fatti siano commessi in Italia, le medesime condotte sono sanzionate se riferite a strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altri Paesi dell'Unione europea oppure a strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano.

I maggiori rischi in relazione alla commissione degli illeciti si possono ipotizzare nei seguenti casi: operazioni simulate, altri artifici o abuso di informazioni privilegiate per conto della Banca o a

favore di clienti della stessa ove sussista un interesse o vantaggio della Banca medesima, nonché diffusione di notizie false o fuorvianti, soprattutto in correlazione ad operazioni effettuate sul mercato, prima o dopo tale diffusione.
In presenza di operazioni richieste dai clienti che facciano sospettare la commissione di uno degli illeciti di "Abuso di informazione privilegiata" o di "Manipolazione del mercato", esiste unicamente (ai sensi dell'art. 187-nonies T.U.F.) un obbligo di segnalazione in capo all'intermediario; tuttavia non può escludersi che, in astratto, si possa configurare un coinvolgimento della Banca nell'illecito commesso dal cliente in relazione alle concrete modalità di svolgimento delle attività da parte della Banca.

Si fornisce qui di seguito una descrizione delle fattispecie sopra indicate.

Abuso di informazioni privilegiate (art. 184 T.U.F.)
La fattispecie penale si realizza quando un soggetto acquista, vende o compie altre operazioni per conto proprio o di terzi su strumenti finanziari utilizzando informazioni privilegiate di cui sia venuto in possesso in ragione della sua qualità di membro degli organi di amministrazione, direzione o controllo dell'emittente ovvero (ii) della partecipazione al capitale dell'emittente ovvero (iii) dell'esercizio di un'attività lavorativa, professionale ovvero di una funzione o di un ufficio. Può, inoltre, essere commesso da chi sia entrato in possesso di informazioni privilegiate in conseguenza della preparazione o commissione di un reato (es. intrusione in un sistema informatico ed estrazione di informazioni privilegiate).
La fattispecie si realizza altresì quando detti soggetti comunicano dette informazioni privilegiate al di fuori dell'esercizio del proprio lavoro o professione ed anche quando raccomandano o inducono altri soggetti, sulla scorta delle informazioni privilegiate di cui sono in possesso, a compiere talune delle operazioni sopradescritte.
Per informazione privilegiata, ai sensi dell'art. 181, comma 1 del T.U.F. si intende quella "di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari".
Nell'ambito dell'operatività bancaria, si riscontrano numerose fattispecie nelle quali possono profilarsi elementi di rischio, e che possono comportare la responsabilità della Banca nel caso in cui il reato sia commesso nell'interesse, esclusivo o concorrente, dell'Ente stesso (ad esempio, in relazione alle attività di proprietary trading allorché chi dispone o esegue l'operazione abusi di un'informazione privilegiata riguardante un determinato emittente cui ha accesso la Banca nello

svolgimento della propria attività, stante la pluralità di rapporti intrattenuti con l'emittente, ovvero in relazione al fenomeno del front running[1]).

Manipolazione del mercato (art. 185 T.U.F.)

La fattispecie penale si realizza quando qualcuno diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari indicati dall'art. 182 T.U.F. illustrato in premessa.

Sanzioni amministrative: abuso di informazioni privilegiate e manipolazione del mercato (art. 187-bis e art. 187-ter T.U.F.)

Come sopra illustrato, sono state introdotte specifiche sanzioni amministrative che sanzionano le medesime condotte materiali che formano oggetto delle fattispecie penali (artt. 184 e 185 T.U.F.): si precisa al riguardo che, mentre per l'illecito penale è necessario il dolo, per l'illecito amministrativo è sufficiente la colpa.

Va, in particolare, precisato che la condotta che integra l'illecito amministrativo di manipolazione del mercato ha una estensione più ampia rispetto alla fattispecie penale col medesimo nome, posto che il reato prevede la diffusione di notizie false o il compimento di operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, mentre l'illecito amministrativo contempla diverse condotte quali: la diffusione, tramite mezzi di informazione, compreso internet o ogni altro mezzo, di informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti; il compimento di operazioni idonee a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari ovvero a fissare in modo anomalo o artificioso il prezzo di tali strumenti ovvero che utilizzano artifizi od ogni altro tipo di inganno o di espediente; altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

7.7.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati ed illeciti amministrativi riconducibili ad abusi di mercato sono le seguenti:

[1] Modalità operativa con la quale si abusa dell'informazione privilegiata concernente gli ordini del cliente in attesa di esecuzione a vantaggio dello stesso intermediario ovvero a vantaggio di un altro cliente ed anche nell'interesse o a vantaggio dello stesso intermediario.

- Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
- Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato.

Si riportano di seguito, per ognuna delle sopraelencate attività sensibili, i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili a dette attività e che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime.

7.7.2.1. Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Premessa

Il presente protocollo si applica a tutti i componenti gli Organi Sociali ed ai dipendenti della Banca che abbiano accesso ad informazioni privilegiate, nell'accezione di cui alla vigente normativa di legge e regolamentare ovvero che gestiscano le comunicazioni della Banca al mercato ed, in genere, all'esterno, intendendosi con tale espressione la distribuzione di ricerche e raccomandazioni nonché qualsiasi diffusione di notizie, dati o informazioni nell'ambito dei rapporti di business, delle attività di marketing o promozionali, dei rapporti con i mezzi di informazione, oltre che le comunicazioni di carattere obbligatorio c.d. price sensitive.
Il processo di gestione e di trattamento delle informazioni privilegiate potrebbe presentare potenzialmente occasioni per la commissione del reato di abuso di informazioni privilegiate ovvero della connessa fattispecie di illecito amministrativo, rispettivamente previsti dagli artt. 184 e 187-bis del T.U.F..
Una corretta gestione del processo in oggetto consente anche la prevenzione dei reati di aggiotaggio e di manipolazione del mercato nonché dell'omologo illecito amministrativo - rispettivamente disciplinati dall'art. 2637 del codice civile, e dagli artt. 185 e 187-ter del T.U.F.– relativamente alle condotte di cosiddetta "manipolazione informativa", presidiando il potenziale rischio di "diffusione di informazioni, voci o notizie false o fuorvianti".
Per quanto attiene alla prevenzione delle condotte di cosiddetta "manipolazione operativa" si fa riferimento al protocollo per la "Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato".

Secondo le indicazioni della Consob, per la Banca, in quanto soggetto controllato da emittente quotato, rilevano le informazioni che possono essere considerate di carattere privilegiato per la controllante quotata alla luce della significatività della controllata.
In relazione a quanto sopra si dà atto che le informazioni relative alla Banca non sono di norma tali in termini di significatività da riverberare effetti idonei ad influenzare il corso dei titoli della Capogruppo. La Banca, inoltre, nella prestazione dei propri servizi, può entrare in possesso di informazioni privilegiate relative a società clienti.
Atteso quanto sopra, al fine di assicurare un'adeguata sensibilizzazione di tutto il personale, si riportano nel seguito i principi di controllo e di comportamento adottati dalla Capogruppo e condivisi dalla Banca, volti a garantire il rispetto della normativa primaria e secondaria vigente in

materia ed i principi di riservatezza delle informazioni trattate e di segretezza nel trattamento delle informazioni non di pubblico dominio.

Obiettivo delle regole sancite dal presente documento, in ottemperanza ai dettami della normativa vigente, è quello di garantire:

- che la circolazione delle informazioni nel contesto aziendale possa svolgersi senza pregiudizio del carattere privilegiato o confidenziale delle informazioni stesse ed evitare che dette informazioni siano condivise con soggetti non autorizzati nonché di assicurare che la divulgazione al mercato delle informazioni privilegiate avvenga in modo tempestivo, in forma completa e comunque in modo tale da evitare asimmetrie informative fra il pubblico;
- le comunicazioni della Banca al mercato ed, in genere, all'esterno trovino adeguata disciplina e una precisa individuazione dei soggetti abilitati ad effettuarle, affinché le stesse siano tali da evitare la divulgazione di informazioni o notizie false o fuorvianti, sia con riferimento alla Banca, sia con riferimento a società terze.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione e diffusione delle informazioni privilegiate di cui le strutture della Banca vengono a conoscenza è articolato sulla base delle specifiche responsabilità operative indicate nell'ambito del sistema di attribuzione dei ruoli e delle mission, definito dalla Banca.

In ragione dell'attività lavorativa e delle funzioni svolte nell'ambito dell'operatività aziendale, le strutture della Banca possono trattare informazioni privilegiate aventi ad oggetto:

- la Banca stessa, la sua Capogruppo e le società appartenenti al Gruppo e gli strumenti finanziari emessi;
- le società clienti e gli strumenti finanziari da queste emessi (ad es. in sede di prestazione di servizi di finanza aziendale alle società quotate clienti della Banca;
- l'informazione trasmessa da un cliente e/o concernente gli ordini del cliente in attesa di esecuzione, che ha carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

L'informazione privilegiata può nascere da una decisione interna alla Banca (ad esempio le iniziative strategiche, gli accordi e le operazioni straordinarie) oppure derivare dall'accertamento di eventi o circostanze oggettive aventi un riflesso sull'attività dell'impresa (ad esempio situazioni contabili di periodo, notizie sul management) oppure derivare dalle attività svolte in nome o per conto di società terze.

Presso la Capogruppo è istituito dalla medesima, ai sensi dell'art. 115-bis del T.U.F., il Registro delle persone aventi accesso a tali informazioni.

Il processo di divulgazione al mercato delle informazioni price sensitive per il Gruppo, ossia che si riferiscano ad eventi che accadono nella sfera di attività della Capogruppo e/o delle Società Controllate che abbiano effetti rilevanti sull'andamento economico-patrimoniale del Gruppo, si articola nelle seguenti fasi:

- individuazione delle informazioni privilegiate;
- predisposizione ed approvazione del comunicato da diffondere al mercato;
- attestazione da parte del Dirigente Preposto della Capogruppo, ai sensi dell'art.154-bis del T.U.F., qualora le comunicazioni abbiano direttamente per oggetto informazioni economico – finanziarie consuntive della Capogruppo Intesa Sanpaolo S.p.A. e del Gruppo;
- diffusione delle informazioni.

I criteri per l'individuazione delle informazioni privilegiate e le modalità operative per la gestione delle medesime sono disciplinati nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Il processo di diffusione di ricerche e raccomandazioni si articola nelle seguenti fasi:

- produzione delle raccomandazioni;
- verifica del rispetto degli standard adottati;
- diffusione delle raccomandazioni.

In relazione agli obblighi di correttezza e trasparenza nella divulgazione di notizie, dati e informazioni al fine di prevenire forme di manipolazione informativa, la Banca adotta specifiche procedure interne volte a disciplinare tali aspetti.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:

- istituzione del Registro delle persone che hanno accesso alle informazioni privilegiate ai sensi dell'art. 115-bis del T.U.F.: la normativa interna delinea il processo per l'alimentazione e la gestione del Registro, nonché le funzioni aziendali tempo per tempo responsabili della gestione medesima. Tali funzioni aziendali, ognuna per quanto di rispettiva competenza, hanno la responsabilità dell'adempimento degli obblighi informativi nei confronti dei soggetti iscritti nel Registro e ottemperano alle richieste di accesso formulate dalle Autorità competenti;
- implementazione di sistemi di sicurezza logica e fisica e di altre procedure rispondenti alle migliori prassi, a garanzia della corretta gestione delle informazioni;
- separazione organizzativa e logistica tra le Strutture che hanno a disposizione delle informazioni privilegiate e quelle che operano sui mercati sulla base di informazioni di pubblico dominio o che intraprendono attività di gestione di investimenti;
- istituzione di procedure di watch e restricted list, finalizzate al monitoraggio di situazioni "sensibili" (watch list) al rischio di conflitti di interesse tra la Banca e la clientela di riferimento od il mercato in genere, nonché alla gestione e al monitoraggio delle informazioni privilegiate tra le Strutture soggette a separazione ed all'eventuale imposizione di ulteriori e specifiche restrizioni operative (restricted list);
- implementazione di misure procedurali e organizzative per la prevenzione degli illeciti in tema di abusi di mercato;
- attività di compliance clearing, svolta dalle competenti Strutture della Banca, sulle informazioni concernenti i prodotti distribuiti dalla Banca e sui messaggi promozionali;
- istituzione di Strutture dedicate alla supervisione delle attività in tema di comunicazione e di relazioni esterne.

Il tutto come meglio individuato e disciplinato nelle policy e nei regolamenti interni tempo per tempo vigenti.

Con particolare riferimento agli aspetti connessi alla diffusione al mercato dell'informazione privilegiata il relativo iter procedurale, che coinvolge strutture della Capogruppo e della Banca, è il seguente:

- in presenza di eventi "price sensitive" sottoposti a deliberazione del Consiglio di Gestione e/o del Consiglio di Sorveglianza della Capogruppo, le relative comunicazioni al mercato sono approvate dal Consiglio deliberante;

- in tutti gli altri casi in cui si sia in presenza di eventi potenzialmente rilevanti ai fini degli obblighi di comunicazione, il Consigliere Delegato della Capogruppo valuta, con il supporto della competente funzione di Investor Relations della Capogruppo, la "price sensitivity", delle informazioni da divulgare. Il testo del relativo comunicato stampa è approvato dal Consigliere Delegato della Capogruppo;
- qualora le comunicazioni abbiano direttamente per oggetto informazioni economico – finanziarie consuntive della Capogruppo Intesa Sanpaolo S.p.A. e del Gruppo, il Dirigente Preposto della Capogruppo appone l'attestazione prevista ai sensi dell'art. 154-bis del T.U.F.;
- il Presidente del Consiglio di Gestione della Capogruppo autorizza la diffusione al mercato dei comunicati approvati dal Consiglio di Gestione della Capogruppo. Il Presidente del Consiglio di Sorveglianza della Capogruppo autorizza la diffusione al mercato dei comunicati approvati dal Consiglio di Sorveglianza della Capogruppo. Il Consigliere Delegato della Capogruppo informa - nell'ambito delle rispettive competenze - il Presidente del Consiglio di Gestione della Capogruppo e il Presidente del Consiglio di Sorveglianza della Capogruppo in merito ai comunicati sottoposti alla propria approvazione;
- qualora le informazioni price sensitive si riferiscano ad eventi che accadono nella sfera di attività della Cassa di Risparmio del Veneto S.p.A., il Consiglio di Amministrazione e/o la Direzione Generale hanno la responsabilità dell'individuazione e della segnalazione delle circostanze ed avvenimenti a tal fine rilevanti, con l'onere di contattare tempestivamente le funzioni di Investor Relations e di Relazioni Esterne della Capogruppo per il corretto adempimento degli obblighi di comunicazione al mercato;
- la funzione di Investor Relations della Capogruppo predispone i comunicati stampa relativi ad informazioni price sensitive per il Gruppo, ossia che si riferiscano ad eventi che accadono nella sfera di attività della Capogruppo e/o delle Società Controllate che abbiano effetti rilevanti sull'andamento economico-patrimoniale del Gruppo, da inoltrare - previa autorizzazione degli organismi aziendali competenti e tramite la funzione di Relazioni Esterne della Capogruppo - alle Autorità di Vigilanza competenti in materia, via N.I.S., e alla stampa;
- la funzione di Investor Relations della Capogruppo ha la responsabilità della gestione dei rapporti con gli analisti finanziari e gli investitori istituzionali al fine della divulgazione di informazioni rilevanti assicurandone l'omogeneità anche nelle ipotesi in cui la diffusione all'esterno avvenga tramite internet;
- la responsabilità della gestione dei rapporti con le agenzie di rating al fine della divulgazione di informazioni rilevanti è riservata ad una specifica funzione aziendale della Capogruppo.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nelle attività di gestione e divulgazione delle informazioni privilegiate, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.

In particolare:

- è fatto obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la Banca, la Capogruppo o le altre Società del Gruppo e gli strumenti finanziari delle stesse, sia riguardanti Società terze in rapporto d'affari con la Banca e gli strumenti finanziari di queste ultime nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- è vietato compiere operazioni su strumenti finanziari della Capogruppo o di Società del Gruppo e di Società terze in rapporto d'affari con la Banca stessa, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse. Tale divieto si applica a qualsiasi tipo di operazione in strumenti finanziari (ad esempio: azioni, obbligazioni, warrant, covered warrant, opzioni, futures);
- é vietato compiere operazioni che anticipino le operazioni della clientela sugli stessi strumenti, considerandosi a tal fine informazione privilegiata anche l'informazione concernente gli ordini del cliente in attesa di esecuzione. Tale previsione implica anche il divieto di trasmettere a terzi informazioni sugli ordini o sulle informazioni ricevute dalla clientela;
- è possibile diffondere le informazioni privilegiate nell'ambito delle Strutture ed uffici della Banca solo nei riguardi di coloro che abbiano effettiva necessità di conoscerle per motivi attinenti al normale esercizio del lavoro e nel rispetto delle misure di separazione previste, evidenziando la natura riservata delle informazioni e procedendo a rendere nota tale diffusione al fine della iscrizione dei soggetti interessati nel Registro delle persone aventi accesso ad informazioni privilegiate. Inoltre, qualora l'iscritto nel Registro dovesse comunicare involontariamente un'informazione privilegiata ad un soggetto che non possa legittimamente accedervi, dovrà comunicare tale circostanza alla Struttura che gestisce il Registro per l'adozione dei provvedimenti necessari;
- è vietato comunicare le medesime informazioni a terzi per ragioni diverse da quelle di ufficio (a titolo esemplificativo e non esaustivo: clienti, emittenti di titoli pubblicamente

contrattati,ecc.) ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate;

- qualora dette informazioni debbano essere comunicate a terzi (consulenti e/o professionisti esterni) per ragioni di ufficio, è fatto obbligo di iscrivere costoro nel Registro delle persone aventi accesso ad informazioni privilegiate. Nel caso in cui detti soggetti non siano istituzionalmente tenuti ad un obbligo di riservatezza legale, regolamentare o statutario è necessario formalizzare un accordo di confidentiality, che imponga il reciproco dovere di riservatezza circa le informazioni scambiate;
- è vietato discutere informazioni privilegiate in luoghi pubblici o in locali in cui siano presenti estranei o comunque soggetti che non hanno necessità di conoscere tali informazioni. A titolo esemplificativo: si deve evitare di discutere tali informazioni in open space che ospitano strutture diverse, ascensori, corridoi, aree di ristoro, mense aziendali, ristoranti, treni, aerei, aeroporti, autobus e, in generale, in luoghi accessibili ad un pubblico indistinto; si deve porre particolare attenzione nell'uso di telefoni cellulari e di telefoni "viva voce";
- fatto salvo quanto previsto in materia di comunicazione al pubblico di informazioni privilegiate relative alla Banca, è vietato comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della Banca. Qualora fosse richiesto un commento su specifiche operazioni relative a tali emittenti, ci si dovrà limitare a commentare i fatti già resi pubblici dall'emittente in base all'art. 114 del TUF; in ogni caso sono previsti obblighi di consultazione con le funzioni aziendali che sono legittimamente in possesso delle informazioni privilegiate in modo che queste possano verificare che non siano anche involontariamente divulgate informazioni soggette a riservatezza;
- è vietato diffondere sia ad altro personale sia all'esterno della Banca, attraverso qualsiasi canale informativo, compreso internet, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla Banca o al Gruppo e/o ai relativi strumenti finanziari nonché in relazione a Società terze in rapporto d'affari con la Banca o il Gruppo e ai relativi strumenti finanziari;
- è vietato produrre e diffondere studi e ricerche o altre comunicazioni di marketing in violazione delle norme, interne ed esterne, specificamente dettate per tale attività e, in particolare, senza garantire un'informazione chiara, corretta e non fuorviante e senza comunicare nei modi richiesti dalla normativa gli interessi rilevanti e/o i conflitti eventualmente sussistenti;
- è fatto obbligo, secondo quanto stabilito dalle norme interne in tema di sicurezza fisica e logica di custodire accuratamente documenti contenenti informazioni confidenziali e

riservate, di assicurarsi che le proprie password rimangano segrete e che il proprio computer sia adeguatamente protetto attraverso il blocco temporaneo dello stesso nei momenti in cui ci si allontana dalla propria postazione. Si evidenzia inoltre che:

- l'attività di produzione dei documenti (quali, ad esempio, stampa e fotocopiatura di documenti) contenenti informazioni privilegiate deve essere presidiata da personale a ciò abilitato;
- i documenti in oggetto devono essere classificati come "confidenziali", "riservati" o, ove possibile, utilizzando nomi in codice per salvaguardare la natura dell'informazione in essi contenuta; l'accesso a informazioni confidenziali e riservate, quando elaborate/trattate/trasmesse/archiviate in formato elettronico, deve essere regolato tramite inserimento di password o, per le Strutture che ne siano fornite, mediante l'apposito applicativo di crittografia;
- i supporti recanti informazioni confidenziali e riservate devono essere custoditi in locali ad accesso fisico controllato, ovvero riposti in archivi custoditi o protetti al termine del loro utilizzo e non devono mai essere lasciati incustoditi, particolarmente quando portati all'esterno delle sedi di lavoro;
- la distruzione dei supporti recanti informazioni confidenziali e riservate deve avvenire a cura degli stessi soggetti che ne dispongono, con le modalità più idonee ad evitare ogni improprio recupero del contenuto informativo.

Inoltre:

- con particolare riferimento all'attività di emissione di comunicati ufficiali al mercato, si precisa che essi devono essere redatti nel rispetto delle norme legali e regolamentari e, comunque, dei requisiti di correttezza, chiarezza, e parità di accesso all'informazione, dove:
  - per correttezza si intende un'informazione esaustiva e non fuorviante, in relazione alle legittime richieste di dati e notizie provenienti dal mercato;
  - la chiarezza attiene alle forme con cui l'informazione è comunicata al mercato e ne comporta la completezza e l'intelligibilità in funzione dei diversi destinatari;
  - per parità di accesso si intende l'inammissibilità di ogni forma di comunicazione selettiva di informazioni che possano avere rilevanza per la valutazione degli strumenti finanziari;
- con riferimento all'attività di divulgazione di informazioni privilegiate alle Autorità di Vigilanza, questa deve essere effettuata in modo completo, tempestivo e adeguato, nel rispetto delle norme e dei regolamenti in materia. Prima di tale comunicazione nessuna dichiarazione riguardante le informazioni privilegiate può essere rilasciata verso l'esterno.

Ove ritenuto opportuno, la Banca può stabilire regole comportamentali e/o divieti per i dipendenti che, in ragione del ruolo, della funzione o dell'attività svolta, sono particolarmente esposti al rischio di abuso di informazione privilegiata.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.7.2.2. Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione delle operazioni di mercato su strumenti finanziari.

Il processo di gestione delle operazioni di mercato presenta potenzialmente occasioni per la commissione dei reati di aggiotaggio e di manipolazione del mercato o del corrispondente illecito amministrativo previsti rispettivamente dall'art. 2637 del codice civile dagli artt.185 e 187-ter del T.U.F., con riferimento alle condotte di c.d. "manipolazione operativa" da dette norme previste.
Per quanto attiene la prevenzione delle fattispecie – penale e amministrativa - della cosiddetta "manipolazione informativa" - che può consistere nella diffusione di informazioni, voci o notizie false o fuorvianti - si fa riferimento al protocollo per la "Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di Abusi di mercato", dove sono definiti i principi di controllo e di comportamento da osservare nel processo di gestione delle informazioni privilegiate di cui le Strutture operative della Banca potrebbero entrare in possesso in ragione dell'esecuzione dei compiti ad esse assegnati ovvero in relazione alle comunicazioni della Banca al mercato ed, in genere, all'esterno.

Obiettivo delle regole sancite dal presente documento, in ottemperanza ai dettami della normativa vigente, è quello di garantire che nella esecuzione delle operazioni di negoziazione e regolamento sul mercato – ovvero nelle modalità di inoltro degli ordini a soggetti terzi per la loro esecuzione - non siano poste in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari ovvero non siano poste in essere operazioni o altri artifizi idonei a fornire indicazioni false e fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Si dà atto che in base all'attuale assetto organizzativo della Banca, le attività inerenti alla gestione delle operazioni di mercato sono demandate operativamente alle competenti Strutture di Capogruppo e/o di altre Società del Gruppo sulla scorta dei relativi contratti di outsourcing. Ciononostante, anche al fine di assicurare un'adeguata sensibilizzazione di tutto il personale, si riportano nel seguito i principi di controllo e di comportamento, applicati dalla Capogruppo e condivisi dalla Banca, volti a garantire il rispetto della normativa vigente e dei principi di

trasparenza, correttezza, oggettività, e tracciabilità per la corretta attuazione del processo sottodescritto.

Descrizione del processo

Il processo di gestione delle operazioni di mercato, ai fini del presente protocollo, riguarda l'attività di trading, sia per conto proprio che di terzi concernente gli strumenti finanziari di cui all'art. 182 del T.U.F..
Con riferimento al trading per conto proprio della Banca il processo ricomprende principalmente le seguenti attività:

- definizione delle linee guida complessive di gestione del portafoglio titoli di proprietà;
- elaborazione di strategie di investimento sulla base di analisi e proposte sottoposte all'approvazione dei competenti organi;
- esecuzione delle operazioni di negoziazione per la gestione dei portafogli titoli:
- svolgimento degli adempimenti di carattere amministrativo/normativo connessi alla esecuzione delle operazioni di negoziazione.

In relazione alle attività della Banca di trading per conto terzi (esecuzione di ordini per conto dei clienti e ricezione e trasmissione di ordini) o per le attività di negoziazione per conto proprio concluse in contropartita diretta con la clientela è presente una procedura automatica di selezione delle operazioni sospette per consentire una successiva analisi delle stesse. Qualora al momento dell'acquisizione dell'ordine, vi sia la consapevolezza o il motivato sospetto che l'esecuzione sia strumentale al compimento di un reato o di un illecito amministrativo o alla realizzazione del profitto che ne deriva, deve essere altresì valutato se rifiutare o sospendere l'operazione.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti e in particolare approvazione da parte degli Organi competenti in base al vigente sistema dei poteri e delle deleghe:
  - delle linee guida per la gestione del portafoglio titoli immobilizzati e non immobilizzati della Banca;

- del perimetro operativo per l'effettuazione delle operazioni di negoziazione sui mercati in termini di compravendita di strumenti finanziari;
- delle delibere volte all'autorizzazione degli investimenti/disinvestimenti partecipativi;
- di limiti operativi in funzione dell'anzianità e del grado del personale interessato.

- Separatezza organizzativa tra le Strutture che hanno a disposizione delle informazioni privilegiate e quelle che operano sui mercati sulla base di informazioni di pubblico dominio o che intraprendono attività di gestione di investimenti.

- Attività di controllo sulle operazioni di compravendita titoli eseguite sui mercati attraverso un sistema di controlli differenziato che tenga conto delle diverse tipologie di strumenti finanziari trattati e della specificità del mercato di riferimento.

- Sottoposizione delle attività relative alla prestazione di servizi di investimento a monitoraggio da parte di funzioni di controllo di secondo livello della Banca, con particolare riferimento alla funzione Compliance che svolge, per gli aspetti di competenza, un'attività di validazione preventiva e verifica costante della idoneità delle procedure interne in materia di prestazione dei servizi di investimento, anche sotto il profilo della conformità ai dettati normativi di riferimento avvalendosi altresì delle risultanze della Direzione Centrale Internal Auditing.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: in particolare, le operazioni di compravendita di strumenti finanziari sono gestite attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli delle transazioni effettuate.

- Principi generali di gestione dell'operatività contenuti nella normativa interna di dettaglio che disciplina, in particolare, i seguenti aspetti:
  - definizione intermediari abilitati ad operare con la Banca, modalità di negoziazione e conclusione delle operazioni (quotazione e esecuzione), orari di negoziazione, late deals, pagamenti "brucianti" a fronte di operazioni in derivati OTC, iter autorizzativi nuovi prodotti, accesso alle sale trading, traders autorizzati, errori dispute e reclami.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione di patrimoni dei clienti ovvero in attività di trading, per conto proprio o di terzi, attraverso la negoziazione ed il regolamento di operazioni sui mercati, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.

In particolare è fatto divieto di:

- porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari;
- compiere operazioni o impartire ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- compiere operazioni o ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;
- compiere operazioni od ordini di compravendita che utilizzano artifizi od ogni altro tipo di inganno o di espediente;
- utilizzare altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Sono vietati i seguenti comportamenti, concernenti strumenti finanziari di cui all'art. 182 del T.U.F., salvo che nei casi e con le procedure previste dalla vigente normativa:

- eseguire operazioni o impartire ordini di compravendita che rappresentano una quota significativa del volume giornaliero degli scambi dello strumento finanziario pertinente nel mercato interessato, in particolare quando tali ordini o operazioni conducono ad una significativa variazione del prezzo dello strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita avendo una significativa posizione in acquisto o in vendita su uno strumento finanziario che conducono a significative variazioni del prezzo dello strumento finanziario o dello strumento derivato collegato o dell'attività sottostante;
- eseguire operazioni che non determinano alcuna variazione nella proprietà ovvero non comportano alcun trasferimento effettivo della proprietà di uno strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita che prevedono inversioni di posizione in acquisto o in vendita nel breve periodo e rappresentano una quota significativa

del volume giornaliero di scambi dello strumento finanziario nel mercato interessato e possono associarsi a significative variazioni del prezzo di uno strumento finanziario;

- eseguire operazioni o impartire ordini di compravendita concentrati in un breve lasso di tempo nel corso della sessione di negoziazione che conducano a una variazione del prezzo che successivamente si inverte;
- impartire ordini di compravendita che modificano la rappresentazione dei migliori prezzi delle proposte di acquisto o di vendita di uno strumento finanziario o, più in generale, modificano la rappresentazione del book di negoziazione a disposizione dei partecipanti al mercato, e sono revocati prima della loro esecuzione;
- eseguire operazioni o impartire ordini nei momenti o intorno ai momenti utili per il calcolo dei prezzi delle aste di apertura o di chiusura, dei prezzi di controllo, dei prezzi di riferimento, dei prezzi di regolamento o di valutazione di strumenti finanziari, conducendo a variazioni di tali prezzi;
- eseguire operazioni o impartire ordini di compravendita facendo precedere o seguire dette operazioni dalla diffusione, anche per il tramite di persone collegate, di informazioni false o fuorvianti;
- eseguire operazioni o impartire ordini di compravendita prima o dopo avere elaborato o diffuso, anche per il tramite di persone collegate, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.8 Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro

7.8.1 Fattispecie di reato

La Legge 3 agosto 2007 n. 123 ha inserito nel D. Lgs. n. 231/2001 l'art. 25-septies che aggiunge all'elenco degli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Successivamente, , è stato emanato il c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D. Lgs. 9 aprile 2008 n. 81 come modificato dal D. Lgs. 3 agosto 2009 n.106) che ha profondamente riordinato le molteplici fonti normative previgenti in materia. Per quanto concerne la responsabilità amministrativa degli Enti, l'art. 300 ha modificato l'art. 25-septies del D. Lgs. n. 231/2001 lasciando nella sostanza immutata l'individuazione delle fattispecie penali che costituiscono reati presupposto; l'art. 30 inoltre ha esplicitato le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.
Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.
Si fornisce qui di seguito una sintetica descrizione dei reati sopra menzionati.

Omicidio colposo (art. 589 c.p.)
Lesioni personali colpose gravi o gravissime (art. 590 comma 3 c.p.)
Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima.
Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.
Ai sensi del predetto art. 25-septies del Decreto, entrambe le condotte devono essere caratterizzate dalla violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.

Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro a seguito dell'abrogazione da parte del medesimo Testo Unico di varie leggi speciali previgenti, tra le quali, fondamentalmente: il D.P.R. 27.4.1955 n. 547 in tema di prevenzione degli infortuni; il D.P.R. 19.3.1956 n. 303 che disciplinava l'igiene del lavoro; il D. Lgs. 19.9.1994 n. 626 che conteneva norme generali sulla tutela della salute e della sicurezza dei lavoratori; il D. Lgs. 14.8.1996 n. 494 in tema di sicurezza dei cantieri.

A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del codice civile, in forza della quale il datore di lavoro deve adottare le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.

Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

7.8.2 Attività aziendali sensibili

La tutela della salute e della sicurezza sul lavoro è materia che pervade ogni ambito ed attività aziendale.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di salute e sicurezza sul lavoro. Tale protocollo si completa con la normativa aziendale di dettaglio vigente in argomento.

7.8.2.1 Gestione dei rischi in materia di salute e sicurezza sul lavoro

Premessa

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D. Lgs. N.81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico,compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

In ottemperanza a quanto disposto dalla predetta normativa,la Banca adotta e tiene aggiornato il "Documento di Valutazione dei Rischi", che contiene:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, dei rappresentanti dei lavoratori per la sicurezza e dei medici competenti che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Tale Documento è redatto in conformità alla normativa nazionale ed alle linee guida nazionali ed Europee (ISPESL, INAIL, UNI-EN-ISO, Agenzia Europea per la Salute e Sicurezza).

Il "Sistema di Gestione Aziendale per la Prevenzione e Protezione" delineato nel documento sopra citato prende come riferimento sistemi di qualità ed, in particolare, quelli ricavabili dalla BS 8800 (Guide to Occupational Health and Safety Management Systems) e dalla OHSAS 18001:1999 Occupational Health and Safety Assessment Series. Inoltre la Banca ha scelto di certificare in qualità i processi gestiti dalla funzione di Prevenzione e Protezione secondo la normativa ISO 9001

ed. 2000. L'azienda si è dotata, in relazione alla natura e dimensioni dell'organizzazione ed al tipo di attività svolta, di un'articolazione di funzioni che assicura le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

Le Strutture aziendali incaricate della gestione della documentazione inerente la materia, quali autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo "Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione".

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi. Le linee d'azione generali della Banca devono essere orientate verso un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un "sistema di prevenzione e protezione". Tutte le Strutture della Banca devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

- identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);
- valutazione dei rischi;
- individuazione e predisposizione delle misure di prevenzione e di protezione;
- definizione di un piano di intervento con l'identificazione delle strutture competenti all'attuazione di detti interventi;
- realizzazione degli interventi pianificati nell'ambito di un programma;

- verifica sull'attuazione e controllo sull'efficacia delle misure adottate.

Con specifico riferimento alla gestione dei cantieri (artt. 88 e seguenti del Testo Unico) che è nella responsabilità del "Committente", il processo prevede le seguenti fasi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto / subappalto e dei lavoratori autonomi;
- pianificazione delle fasi di lavorazione e loro valutazione con particolare riferimento alle interazioni delle attività interferenti anche al contorno del cantiere ed alla eventuale compresenza di attività della Banca;
- designazioni figure di legge (es. Responsabile dei lavori; Coordinatore per la progettazione e per l'esecuzione dei lavori) e predisposizioni dei piani di sicurezza e coordinamento nonché dei documenti di valutazione dei rischi interferenziali;
- esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla pubblica amministrazione;
- coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere.

Nei cantieri temporanei o mobili allestiti in unità operative ove sono presenti collaboratori della Banca i rischi derivanti da interferenze tra le due attività sono gestiti dal Committente individuando le specifiche misure di prevenzione, protezione ed emergenza a tutela della salute e sicurezza dei collaboratori, dei clienti e delle imprese appaltatrici e lavoratori autonomi. Tali misure sono indicate nel Piano di Sicurezza e Coordinamento o nel Documento unico di valutazione dei rischi interferenziali (in relazione al rispettivo campo di applicazione) elaborato a cura dei soggetti individuati dal Committente, che può avvalersi anche del supporto della struttura di Prevenzione e Protezione del Datore di Lavoro della Banca.

Con specifico riferimento alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione (art. 26 del Testo Unico) che è nella responsabilità sia del Datore di Lavoro che del Committente, il processo prevede le seguenti fasi:

- verifica, con le modalità previste dalla normativa vigente, dell'idoneità tecnico professionale delle imprese (comprese le eventuali subappaltatrici) e dei lavoratori autonomi;
- informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, nonché ove previsto dalla normativa, predisposizione del Documento di Valutazione dei Rischi Interferenziali (DUVRI), da inviare all'offerente ai fini della formulazione dell'offerta e parte integrante del contratto, contenente le misure idonee per

eliminare o ridurre i rischi relativi alle interferenze delle attività connesse all'esecuzione del contratto;

- redazione della lettera di invito/bando, ove prevista;
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio / fornitura offerti nonché contenente dichiarazione di presa di visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- aggiudicazione del servizio e stipula del contratto;
- esecuzione del servizio / fornitura da parte dell'aggiudicatario e cooperazione e coordinamento con la controparte per la prevenzione dei rischi propri dell'attività oggetto del contratto nonché per gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, anche mediante reciproca informazione al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva ed i rischi insiti nell'eventuale compresenza di personale, collaboratori e clienti della Banca;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.

Le modalità operative per la gestione del processo e l'individuazione delle strutture/figure che hanno le responsabilità delle diversi fasi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito del processo:
  - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità e procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, sono state individuate le figure aziendali che rivestono il ruolo rispettivamente di "Datore di Lavoro" e "Committente". Tali figure possono impartire disposizioni in materia alle Strutture aziendali e godono della più ampia autonomia organizzativa nonché dei più ampi poteri di spesa anche con facoltà di delega e subdelega ai sensi dell'art. 16 comma 3-bis del Testo Unico;

- è prevista un'articolazione di distinte funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- tutti i soggetti/figure aziendali che intervengono nelle fasi del processo sopra descritto devono essere individuati e autorizzati con espressa previsione della normativa interna o tramite delega interna, da conferirsi e conservarsi a cura del Datore di Lavoro/Committente, ovvero a cura dei soggetti da costoro facoltizzati.

- Segregazione dei compiti tra i differenti soggetti/figure aziendali coinvolte nel processo di gestione dei rischi in materia di salute e sicurezza sul lavoro. In particolare:
  - le strutture operative che hanno il compito di realizzare e di gestire gli interventi (di natura immobiliare, informatica, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), sono distinte e separate dalla Struttura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
  - le strutture competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
  - i Rappresentanti dei Lavoratori per la Sicurezza collaborano attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.
- Attività di controllo:
  - le strutture competenti devono attivare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione nonché l'efficacia delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, deve contemplare:
    - aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa[1], di sorveglianza sanitaria, di informazione e formazione dei lavoratori, di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori);
    - modalità di esecuzione delle verifiche, modalità di rendicontazione;

    Il piano aziendale deve altresì assicurare:
    - il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
    - l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti persone, società ecc.) da parte delle competenti strutture;

[1] Quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza

- il rispetto del processo e degli adempimenti tecnici ed amministrativi previsti dalle normative interne e di legge.

Deve inoltre prevedere un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del piano devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

- le Strutture competenti devono controllare che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. Tali Strutture si avvalgono, laddove occorra, della collaborazione della Struttura deputata alla gestione delle risorse umane, nonché delle strutture di gestione e realizzazione di interventi immobiliari, di progettazione e gestione dei processi lavorativi, della sicurezza fisica e dei sistemi informativi;
- i Rappresentanti dei Lavoratori per la Sicurezza, nel rispetto delle norme di legge in materia, possono accedere alla documentazione aziendale inerente la valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. I medesimi Rappresentanti possono accedere ai luoghi di lavoro e formulare osservazioni in occasione di visite e verifiche da parte delle Autorità competenti;
- tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente ed il Responsabile del Servizio Prevenzione e Protezione visitano i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti;
- figure specialistiche di alta professionalità e con i titoli ed i requisiti previsti dalle norme specifiche, contribuiscono alla valutazione ed alla elaborazione di misure di tutela nel caso di rischi specifici (ad es.amianto, radon, elevato rischio di incendio) nonché nei cantieri temporanei e mobili (Responsabili dei lavori, Coordinatori per la Sicurezza, Progettisti, Direttori dei lavori, ecc.);
  - le competenti Strutture individuate dal Datore di Lavoro/Committente provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare;
  - qualora la documentazione prevista dal Testo Unico sia tenuta su supporto informatico, la competente Struttura verifica che le modalità di memorizzazioni dei dati e di accesso al sistema di gestione della predetta documentazione assicurino quanto previsto dall'art. 53 del Testo Unico;

- il Datore di Lavoro ed il Committente, ciascuno negli ambiti di competenza, vigilano ai sensi del comma 3-bis dell'art. 18 del Testo Unico in ordine all'adempimento degli obblighi in materia che la legge attribuisce a preposti, lavoratori, medici competenti, progettisti, fabbricanti, fornitori, installatori attraverso il piano aziendale di controllo sistematico sopra indicato.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - l'impiego di sistemi per la gestione informatica dei dati e delle documentazione prescritta dal Testo Unico deve avvenire nel rispetto dell'art. 53 del medesimo;
  - ciascuna Struttura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, deve dotarsi di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
  - ciascuna Struttura di volta in volta interessata è responsabile altresì dell'acquisizione di documentazioni e certificazioni obbligatorie di legge e della relativa conservazione e archiviazione;
  - la gestione dei diversi contesti di rischio prevede l'utilizzo di specifici sistemi informativi che consentano l'accesso in rete a tutte le Strutture interessate ed autorizzate alla valutazione dei rischi delle unità operative e che contengano, ad esempio, la documentazione tecnica di impianti, macchine, luoghi di lavoro, ecc., le liste degli esposti a specifici rischi, la documentazione sanitaria (con il rispetto dei requisiti di riservatezza previsti dalla normativa), le attività di formazione ed informazione, le attività di eliminazione/riduzione dei rischi, l'attività ispettiva interna ed esterna, le informazioni in tema di infortuni e segnalazioni di rischio, la modulistica per la gestione dei monitoraggi ambientali e della cartella sanitaria, ecc..

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, come pure tutti i dipendenti, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare, tutte le Strutture/figure sono tenute - nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, etc.) in occasione di accertamenti/procedimenti ispettivi;
- provvedere, nell' ambito dei contratti di appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate ad operare e ad elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese compresi gli eventuali lavoratori autonomi, evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nell'ambito dei contratti di appalti di forniture, di servizi o d'opere nonché di quelli regolati dal D. Lgs. n. 276/2003 e successive modifiche ed integrazioni, nonché nei confronti dei soggetti beneficiari di iniziative di tirocinio e dei terzi in genere che dovessero trovarsi nei luoghi di lavoro.
- assicurarsi che, nell'impiego di sistemi di elaborazione automatica dei dati, le modalità di memorizzazione dei dati e di accesso al sistema di gestione della documentazione prescritta garantiscano quanto previsto dall'art. 53 del Testo Unico.

Parimenti, tutti i dipendenti sono tenuti a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Strutture aziendali e dalle Autorità competenti;

- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti (anche omissivi) che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.9 Area sensibile concernente i reati informatici

7.9.1 Fattispecie di reato

Premessa

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, fatta a Budapest il 23 novembre 2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.

La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D. Lgs. n. 231/2001 l'art. 24 bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli Enti.

La citata legge ha modificato anche il codice di procedura penale, essenzialmente al fine di agevolare e regolamentare le indagini e le operazioni di perquisizione e di sequestro dei dati informatici, imponendo all'Autorità procedente di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali ed ad impedirne l'alterazione. E' stata altresì disposta l'integrazione dell'art. 132 del Codice della privacy (D. Lgs. n. 196/2003) che consente ora alle competenti Autorità di ordinare ai fornitori e agli operatori di servizi informatici o telematici di conservare per un periodo complessivamente non superiore a sei mesi i dati relativi al traffico telematico.

Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso la Capogruppo stessa sulla scorta dei relativi contratti di outsourcing.

Si illustrano qui di seguito i reati presupposto elencati dall'art. 24-bis del D. Lgs. n. 231/2001.

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

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Banca (o anche di terzi concesse in licenza alla Banca), mediante l'utilizzo delle credenziali di altri colleghi abilitati.

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

Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

La condotta punita dall'art. 617-quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware). L'impedimento od interruzione delle comunicazioni (c.d. "Denial of service") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fasulle.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro Ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall' installazione non autorizzata di un software da parte di un dipendente.

L'art. 617-quinquies punisce il solo fatto della istallazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

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.)

L'art. 635-bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.

Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.

L'art. 635-ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di

pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.
Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615-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.)
L' art. 635-quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

L'art. 635-quinquies c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.
In questa previsione, a differenza di quanto previsto all'art. 635-ter, non vi è più alcun riferimento all'utilizzo da parte di Enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di Enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema.

E' da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.
Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p..

Detenzione o 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.)
L'art. 615-quater punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo.
L'art. 615-quinquies punisce chiunque si procura, produce, riproduce importa, diffonde, comunica consegna o mette a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento.
Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche.
La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

Falsità nei documenti informatici (art. 491-bis c.p.)
L'art. 491-bis c.p. dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche[1].

Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione.

Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.).

Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Tra i reati richiamati dall'art. 491 bis, sono punibili a querela della persona offesa la falsità in scrittura privata (art. 485 c.p.) e, se riguardano una scrittura privata, l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato[2]. Il soggetto attivo del reato

[1] Si rammenta al riguardo che, ai sensi del Codice dell'amministrazione digitale (cfr.art. 1, lettera p) del D. Lgs. n. 82/2005), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:

- se non è sottoscritto con una firma elettronica (art. 1, lettera q), non può avere alcuna efficacia probatoria, ma può al limite, a discrezione del Giudice, soddisfare il requisito legale della forma scritta (art. 20, c. 1 bis);
- anche quando sia firmato con una firma elettronica "semplice" (cioè non qualificata) può non avere efficacia probatoria (il giudice dovrà infatti tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento informatico);
- il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata ha l'efficacia prevista dall'articolo 2702 del codice civile (al pari della scrittura privata), fa cioé piena prova, fino a querela di falso, se colui contro il quale è prodotto ne riconosce la sottoscrizione.

[2] Per certificato qualificato si intende, ai sensi dell'art. 1 lettere e) ed f) del D. Lgs. n. 82/2005, l'attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare le firme elettroniche, che sia conforme ai requisiti stabiliti dall'allegato I della direttiva 1999/93/CE, rilasciato da certificatori - vale a dire i soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi con quest'ultime - che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

può essere evidentemente soltanto un soggetto “certificatore qualificato” , che esercita particolari funzioni di certificazione per la firma elettronica qualificata.
A tale specifico proposito si osserva che la Banca riveste la qualifica di “certificatore qualificato” e che quindi tale disposizione è di immediato interesse per la stessa. Si tenga comunque presente che – per assumere rilevanza penale – la violazione degli obblighi per il rilascio di un certificato qualificato deve essere assistita dal dolo specifico sopra evidenziato (perseguimento di un ingiusto profitto / danno altrui).

* * *

Più in generale può osservarsi che molte fattispecie di reati informatici in concreto potrebbero non presentare il requisito della commissione nell’interesse o a vantaggio della Banca, indispensabile affinché possa conseguire la responsabilità amministrativa della stessa. Per altro verso si ricorda che qualora fossero integrati tutti gli elementi previsti dal D. Lgs. n. 231/2001 la responsabilità della Banca potrebbe sorgere, secondo la previsione contenuta nell’art. 8 del Decreto, anche quando l’autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt’altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati e dell’evanescenza del cyberspazio, che rendono assai difficile anche l’individuazione del luogo ove il reato stesso possa ritenersi consumato.

Va infine ricordato che anche l’art. 640-ter c.p., che punisce il delitto di frode informatica perpetrata ai danni dello Stato o di altro Ente pubblico, costituisce reato presupposto della responsabilità amministrativa degli Enti; al riguardo si rimanda al Capitolo 7.2.1.

7.9.2 Attività aziendali sensibili

Le attività della Banca nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell’informazione.
La Banca ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni di Vigilanza ed al Codice della privacy, per prevenire e controllare i rischi in tema di tecnologia dell’informazione (IT), a tutela del proprio patrimonio informativo e dei dati personali della clientela e dei terzi.
Il reato di cui all’art. 640-quinquies c.p. concerne specificamente l’attività della Banca nella prestazione del servizio di certificatore qualificato.

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti è la:

- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.

Si riporta di seguito il protocollo che detta i principi di controllo ed i principi di comportamento applicabili a detta attività e che si completa con la normativa aziendale di dettaglio che regolamenta l'attività medesima.

7.9.2.1. Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo

Premessa

Il presente protocollo si applica a tutte le Strutture della Banca coinvolte nella gestione e nell'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.
In particolare, si applica a:

- tutte le Strutture della Banca coinvolte nella gestione e l'utilizzo dei sistemi informativi che si interconnettono/utilizzano software della Pubblica Amministrazione ovvero delle Autorità di Vigilanza;
- tutte le Strutture deputate alla progettazione, alla realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- tutte le Strutture che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del Patrimonio Informativo di Gruppo nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al Patrimonio Informativo del Gruppo;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della Banca e trattano i dati del Patrimonio Informativo di Gruppo.

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero presentare potenzialmente occasioni per la commissione dei delitti informatici contemplati dall'art. 24 bis, nonché del reato di frode informatica ai danni dello Stato o di altro Ente pubblico previsto dall'art. 640-ter del codice penale e richiamato dall'art. 24 del Decreto. Inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi ad oggetto le opere del'ingegno protette[1].

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo sono conformi a quelli adottati dalla Capogruppo / altre società del Gruppo e pertanto risultano applicati anche a presidio di tutte le attività accentrate presso i predetti outsourcer sulla scorta dei relativi contratti.

[1] Per la descrizione delle relative condotte si veda il Capitolo 7.10.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi della Banca.
Tra i sistemi informativi utilizzati dalla Banca vi sono altresì hardware e software per l'espletamento di adempimenti verso la Pubblica Amministrazione che prevedano il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi.
Si rendono quindi necessarie una efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo in coerenza con la normativa vigente.

Alla luce delle considerazioni che precedono, di seguito si declinano i processi sui quali si basa il presidio posto in essere sulla gestione e sull'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo della Banca.

Il processo di gestione della sicurezza informatica si articola nelle seguenti fasi:

- analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
- gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
- gestione normativa e architettura di sicurezza informatica;
- monitoraggio eventi sicurezza informatica e gestione crisi di sicurezza informazioni;
- progettazione e realizzazione soluzioni di sicurezza informatica.

Il processo di prevenzione frodi si articola nelle seguenti fasi:

- identificazione delle misure atte al rafforzamento della prevenzione;
- monitoraggio dell'evoluzione delle frodi informatiche, anche per quanto riguarda eventuali aspetti di sicurezza fisica correlati;
- presidio delle attività necessarie all'intercettazione e alla soluzione delle minacce verso gli asset aziendali;
- gestione delle comunicazioni con le Forze dell'Ordine.

Il processo di gestione della sicurezza fisica si articola nelle seguenti fasi:

- gestione protezione di aree e locali ove si svolge l'attività;
- gestione sicurezza fisica dei sistemi periferici (ambienti di filiali, sede centrale, altre reti).

Il processo relativo al servizio di certificazione di firma elettronica si articola nelle seguenti fasi:

- apertura del contratto;
- registrazione del titolare;
- gestione del certificato (sospensione, riattivazione, revoca, rinnovo e sblocco PIN).

Il processo relativo alla progettazione, sviluppo e attivazione dei servizi ICT si articola nelle seguenti fasi:

- progettazione, realizzazione e gestione delle soluzioni applicative e delle infrastrutture tecnologiche di Gruppo;

Il processo di gestione e supporto ICT si articola nelle seguenti fasi:

- erogazione dei servizi ICT;
- monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;
- assistenza agli utenti attraverso attività di Help desk e problem solving.

Le modalità operative per la gestione dei processi descritti sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Fatti salvi i requisiti di sicurezza propri del software della Pubblica Amministrazione o delle Autorità di Vigilanza utilizzato dalla Banca, il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica dei processi sopra descritti. In particolare:
  - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso"in ragione delle funzioni svolte all'interno della Banca;
  - le variazioni al contenuto dei profili sono eseguite dalle Strutture della Banca deputate al presidio della sicurezza logica, su richiesta delle Strutture interessate. La Struttura

richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte;

- ogni utente ha associato un solo profilo abilitativo in relazione al proprio ruolo aziendale nel rispetto del principio del minimo privilegio. In caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato;

- Segregazione dei compiti:
  - sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni; in particolare:
    - sono attribuite precise responsabilità in modo che siano presidiati gli ambiti di indirizzo e governo della sicurezza, di progettazione, di implementazione, di esercizio e di controllo delle contromisure adottate per la tutela del Patrimonio Informativo aziendale;
    - sono attribuite precise responsabilità per la gestione degli aspetti di sicurezza alle funzioni organizzative che sviluppano e gestiscono sistemi informativi;
    - sono definite le responsabilità ed i meccanismi atti a garantire la gestione di eventi di sicurezza anomali e delle situazioni di emergenza e crisi;
    - sono attribuite precise responsabilità della predisposizione, validazione, emanazione e aggiornamento delle norme di sicurezza a funzioni aziendali distinte da quelle incaricate della gestione;
  - le attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono organizzativamente demandate a strutture differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;
  - sono attribuite precise responsabilità per garantire che il processo di sviluppo e manutenzione delle applicazioni, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un opportuno iter autorizzativo.

- Attività di controllo: le attività di gestione ed utilizzo dei sistemi informativi della Banca e del Patrimonio Informativo di Gruppo sono soggette ad una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e

infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza. Le attività di controllo costituiscono valido presidio anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.

I controlli previsti, declinati dalle relative policy interne, si basano sulla definizione di specifiche attività finalizzate alla gestione nel tempo anche degli aspetti inerenti alla protezione del Patrimonio Informativo del Gruppo, quali:

- la definizione degli obiettivi e delle strategie di sicurezza;
- la definizione di una metodologia di analisi dei rischi ai quali è soggetto il patrimonio informativo da applicare a processi ed asset aziendali, stimando la criticità delle informazioni in relazione ai criteri di riservatezza, integrità e disponibilità;
- l'individuazione delle contromisure adeguate, con riferimento ai livelli di rischio rilevati, verificando e controllando il corretto mantenimento dei livelli di sicurezza stabiliti;
- l'adeguata formazione del personale sugli aspetti di sicurezza per sviluppare una maggiore sensibilità;
- la predisposizione e l'aggiornamento delle norme di sicurezza, al fine di garantirne nel tempo l'applicabilità, l'adeguatezza e l'efficacia;
- i controlli sulla corretta applicazione ed il rispetto della normativa definita.

Le principali attività di controllo, tempo per tempo effettuate, e specificamente dettagliate nella normativa interna di riferimento, sono le seguenti:

Con riferimento alla sicurezza fisica:

- protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi.

Con riferimento alla sicurezza logica:

- identificazione e autenticazione dei codici identificativi degli utenti;
- autorizzazione relativa agli accessi alle informazioni richiesti;
- previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse.

Con riferimento all'esercizio ed alla gestione di applicazioni, sistemi e reti:

- previsione di una separazione degli ambienti (sviluppo, collaudo e produzione) nei quali i sistemi e le applicazioni sono installati, gestiti e manutenuti in modo tale da garantire nel tempo la loro integrità e disponibilità;
- predisposizione e protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività;
- previsione di misure per le applicazioni in produzione in termini di installazione, gestione dell'esercizio e delle emergenze, protezione del codice, che assicurino il mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni trattate;
- attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti;
- pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
- gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità tramite la regolamentazione ed il controllo sull'utilizzo degli strumenti, delle apparecchiature e di ogni asset informativo in dotazione nonché mediante la definizione di modalità di custodia, riutilizzo, riproduzione, distruzione e trasporto fisico dei supporti rimuovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;
- monitoraggio di applicazioni e sistemi, tramite la definizione di efficaci criteri di raccolta e di analisi dei dati relativi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
- prevenzione da software dannoso tramite sia opportuni strumenti ed infrastrutture adeguate (tra cui i sistemi antivirus) sia l'individuazione di responsabilità e procedure per le fasi di installazione, verifica di nuovi rilasci, aggiornamenti e modalità di intervento nel caso si riscontrasse la presenza di software potenzialmente dannoso;
- formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica e siti web;
- adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati a supporto e garantire la corretta e sicura circolazione delle informazioni;
- previsione di specifiche procedure per le fasi di progettazione, sviluppo e cambiamento dei sistemi e delle reti, definendo i criteri di accettazione delle soluzioni;

- previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali.

Con riferimento allo sviluppo ed alla manutenzione delle applicazioni:

- individuazione di opportune contromisure ed adeguati controlli per la protezione delle informazioni gestite dalle applicazioni, che soddisfino i requisiti di riservatezza, integrità e disponibilità delle informazioni trattate, in funzione degli ambiti e delle modalità di utilizzo, dell'integrazione con i sistemi esistenti e del rispetto delle disposizioni di Legge e della normativa interna;
- previsione di adeguati controlli di sicurezza nel processo di sviluppo delle applicazioni, al fine di garantirne il corretto funzionamento anche con riferimento agli accessi alle sole persone autorizzate, mediante strumenti, esterni all'applicazione, per l'identificazione, l'autenticazione e l'autorizzazione.

Con riferimento alla gestione degli incidenti di sicurezza:

- previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette al fine di minimizzare il danno generato e prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
  - tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione (sistema di log files);
  - tutti i transiti in ingresso e in uscita degli accessi alle zone riservate, del solo personale che ne abbia effettiva necessità previa debita autorizzazione, sono rilevati tramite appositi meccanismi di tracciatura;
  - è prevista la tracciatura delle attività effettuate sui dati, compatibili con le leggi vigenti al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Struttura è responsabile dell'archiviazione e della

conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo di Gruppo sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice interno di comportamento di Gruppo.
In particolare:

- le Strutture coinvolte nei processi devono predisporre e mantenere il censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici software in uso;
- i soggetti coinvolti nel processo devono essere appositamente incaricati;
- ogni dipendente/amministratore del sistema è tenuto alla segnalazione all'Alta Direzione aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente ed attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Banca dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del Patrimonio Informativo di Gruppo nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

Con riferimento alla specifica attività di “certificatore qualificato”

- ogni dipendente è responsabile, al momento della sottoscrizione del contratto e della consegna del dispositivo utilizzabile per l’apposizione della firma elettronica, di accertare l’identità del cliente attraverso l’esibizione di un documento d’identità legalmente riconosciuto ed in corso di validità e, nel caso in cui l'interlocutore agisca per conto di terzi, di accertare che abbia i poteri di rappresentanza necessari;
- l’operatore deve assicurare la corretta e tempestiva esecuzione delle operazioni inerenti al certificato (sospensione, riattivazione, revoca, rinnovo e sblocco PIN).

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

- introdursi abusivamente direttamente o per interposta persona in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all’accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Banca e del Gruppo, o a parti di esse, non possedendo le credenziali d’accesso o mediante l’utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc…) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l’integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre, o diffondere abusivamente codici d’accesso o comunque mezzi idonei all’accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri,

apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;

- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:
  - diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;
  - abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
  - detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;
  - riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costitutore;
  - rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
  - importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.10 Area sensibile concernente i reati contro l'industria ed il commercio ed i reati in materia di violazione del diritto d'autore

7.10.1 Fattispecie di reato

Premessa

La L. 23.7.2009 n. 99 – Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in tema di energia – in un più ampio quadro di iniziative di rilancio dell'economia e di tutela del "Made in Italy", dei consumatori e della concorrenza, ha attratto nell'ambito della responsabilità da reato degli Enti numerose norme penali, alcune delle quali dalla stessa legge emanate o riformulate. In particolare, nel testo novellato del D. Lgs. n. 231/2001, gli artt. 25-bis e 25-bis.1 richiamano fattispecie previste dal codice penale in tema di industria e di commercio[1], mentre l'art. 25-novies[2] - al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno[3] e i gravi danni economici arrecati agli autori e all'industria connessa – rimanda a reati contemplati dalla legge sul diritto d'autore (L. n. 633/1941). Si descrivono qui di seguito gli illeciti in questione.

Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni di prodotti industriali (art. 473 c.p.)

La norma punisce le condotte di chi, pur potendo accertare l'altrui appartenenza di marchi e di altri segni distintivi di prodotti industriali, ne compie la contraffazione, o altera gli originali, ovvero fa uso dei marchi falsi senza aver partecipato alla falsificazione[4].

Integrano la contraffazione le ipotesi consistenti nella riproduzione identica o nell'imitazione degli elementi essenziali del segno identificativo, in modo tale che ad una prima percezione possa

[1] A seguito della modifica apportata dalla L. n. 99/2009, l'art. 25-bis del D. Lgs. n. 231/2001 - che in precedenza riguardava i soli ai reati di falsità in materia di monete e di valori di bollo - concerne anche i delitti previsti dagli articoli 473 e 474 c.p., i quali hanno in comune con i primi il bene giuridico principalmente tutelato e cioè la fede pubblica, intesa quale affidamento che la generalità dei cittadini ripone nella veridicità di determinati oggetti, segni o attestazioni.

[2] La L. n. 116/2009 ha inserito nel D. Lgs. n. 231/2001 un secondo art. 25-novies, così numerato per palese refuso, concernente il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria.

[3] Ai sensi dell'art. 1 della L. n. 633/1941 sono tutelate le opere dell'ingegno di carattere creativo che appartengono alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì protetti come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

[4] Per "fare uso" dei marchi falsi dovrebbero intendersi condotte residuali, quali ad esempio l'apposizione su propri prodotti di marchi falsificati da terzi. Si deve trattare cioè di condotte diverse sia dalla messa in circolazione di prodotti recanti marchi falsi previste nell'art. 474 c.p., sia dalle condotte più propriamente realizzative della contraffazione, quale ad esempio la riproduzione del marchio altrui nelle comunicazioni pubblicitarie, nella corrispondenza commerciale, nei siti internet, ecc..

apparire autentico. Si tratta di quelle falsificazioni materiali idonee a ledere la pubblica fiducia circa la provenienza di prodotti o servizi dall'impresa che è titolare, licenziataria o cessionaria del marchio registrato. Secondo la giurisprudenza è tutelato anche il marchio non ancora registrato, per il quale sia già stata presentata la relativa domanda, in quanto essa lo rende formalmente conoscibile. E' richiesto il dolo, che potrebbe sussistere anche qualora il soggetto agente, pur non essendo certo dell'esistenza di altrui registrazioni (o domande di registrazione), possa dubitarne e ciononostante non proceda a verifiche.

Il secondo comma sanziona le condotte di contraffazione, nonché di uso da parte di chi non ha partecipato alla falsificazione, di brevetti, disegni e modelli industriali altrui[1]. Anche questa disposizione intende contrastare i falsi materiali che, nella fattispecie, potrebbero colpire i documenti comprovanti la concessione dei brevetti o le registrazioni dei modelli. La violazione dei diritti di esclusivo sfruttamento economico del brevetto è invece sanzionata dall'art. 517-ter c.p..

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

L'art. 474 c.p. punisce le condotte di coloro che, estranei ai reati di cui all'art. 473 c.p., introducono in Italia prodotti industriali recanti marchi o segni distintivi contraffatti o alterati, oppure detengono per la vendita, mettono in vendita o comunque in circolazione prodotti contraffatti, sempre che non siano già punibili per l'introduzione in Italia. E' sempre richiesto il fine di trarre profitto.

Il detentore potrebbe essere punito, oltre che per il reato in questione, anche a titolo di ricettazione, qualora fosse a conoscenza fin dal momento dell'acquisto della falsità dei segni distintivi apposti ai prodotti dal suo fornitore o da altri. Si ricorda che, ai sensi dell'art. 25-octies del Decreto, anche il reato di ricettazione può dar luogo alla responsabilità amministrativa degli Enti.

Turbata libertà dell'industria e del commercio (art. 513 c.p.)

Il reato, perseguibile a querela, consiste nel compiere atti di violenza sulle cose o nell'utilizzare mezzi fraudolenti al fine di ostacolare od impedire il regolare svolgimento di un'attività commerciale od industriale, sempre che non siano integrati reati più gravi (ad es. incendio, oppure uno dei reati informatici previsti dall'art. 24-bis del Decreto). Ad esempio, si è ritenuto sussistere il reato nel caso di inserimento nel codice sorgente del proprio sito internet - in modo da renderlo maggiormente visibile ai motori di ricerca - di parole chiave riferibili all'impresa o ai prodotti del concorrente, al fine di dirottare i suoi potenziali clienti.

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)

[1] Il Codice della proprietà industriale (D. Lgs. n. 30/2005), all'art. 2 recita: "*La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori.*".

Commette questo delitto l'imprenditore che compie atti di concorrenza con violenza o minaccia. La norma, introdotta nel codice penale dalla legge antimafia "Rognoni – La Torre" n. 646/1982, trova applicazione anche al di fuori della criminalità mafiosa ed intende contrastare gli atti diretti a impedire o limitare l'intervento sul mercato di operatori concorrenti. Il reato sussiste anche quando la violenza o la minaccia sia posta in essere da terzi per conto dell'imprenditore, oppure non sia direttamente rivolta al concorrente, ma ai suoi potenziali clienti. Potrebbe ad esempio ravvisarsi il reato nelle ipotesi di: minaccia di arrecare un danno ingiusto diretta ai partecipanti a una gara pubblica al fine di conoscere le loro offerte e formularne più basse; minaccia, nel rapporto con un proprio cliente, di applicare condizioni peggiorative o di revocare i crediti concessi, ovvero, nel rapporto con un proprio fornitore, di non effettuare altri ordini nel caso in cui il cliente/fornitore ricorra ai servizi di/fornisca un determinato concorrente.

Frodi contro le industrie nazionali (art. 514 c.p.)

Il delitto incrimina chiunque cagioni un danno contro l'industria nazionale, ponendo in circolazione od in commercio prodotti industriali con marchi o segni distintivi contraffatti. Le dimensioni del danno devono essere tali da colpire non singole imprese, ma l'economia industriale italiana.

Frode nell'esercizio del commercio (art. 515 c.p.)

L'illecito, sempre che non sussistano gli estremi della truffa, consiste nella consegna all'acquirente da parte di chi esercita un'attività commerciale di una cosa mobile per un altra, o che, pur essendo della stessa specie, per origine, provenienza, qualità o quantità, sia diversa da quella pattuita.

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

Il reato è commesso di chi pone in vendita o in commercio sostanze alimentari non genuine, vale a dire sostanze, cibi e bevande che, pur non pericolosi per la salute, siano stati alterati con aggiunta o sottrazione di elementi, od abbiano composizione diversa da quella prescritta.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

Il delitto consiste nel mettere in vendita o comunque in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi[1] atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. E' sufficiente che i segni distintivi, anche in relazione alle altre circostanze del caso concreto (prezzi dei prodotti, loro caratteristiche, modalità della vendita) possano ingenerare nel comune consumatore confusione con i prodotti affini (ma diversi per origine, provenienza o qualità) contrassegnati dal marchio genuino. La norma tutela

[1] L'art. 181-bis, comma 8, della L. n. 633/1941 dispone che ai fini della legge penale il contrassegno SIAE è considerato segno distintivo di opera dell'ingegno.

l'onestà nel commercio e si applica sussidiariamente, quando non ricorrano gli estremi delle più gravi incriminazioni degli artt. 473 e 474 c.p.. In essa ricadono casi quali la contraffazione e l'utilizzo di marchi non registrati, l'uso di recipienti o di confezioni con marchi originali, ma contenenti prodotti diversi, l'uso da parte del legittimo titolare del proprio marchio per contraddistinguere prodotti con standard qualitativi diversi da quelli originariamente contrassegnati dal marchio (il caso non ricorre se la produzione sia commissionata ad altra azienda, ma il committente controlli il rispetto delle proprie specifiche qualitative).

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)

Il reato consta di due diverse fattispecie. La prima, perseguibile a querela, punisce chiunque, potendo conoscere dell'esistenza di brevetti o di registrazioni altrui, fabbrica o utilizza ai fini della produzione industriale oggetti o altri beni, usurpando un titolo di proprietà industriale o in violazione dello stesso. Qualora sussista la falsificazione dei marchi o un'altra delle condotte previste dagli artt. 473 e 474 c.p., l'usurpatore potrebbe rispondere anche di tali reati.

La seconda fattispecie concerne la condotta di chi, al fine di trarne profitto, introduce in Italia, detiene per la vendita, pone in vendita o mette comunque in circolazione beni fabbricati in violazione dei titoli di proprietà industriale. Se le merci sono contraddistinte da segni falsificati si applica anche l'art. 474, comma 2, c.p..

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

Le condotte punite consistono nell'apporre a prodotti agroalimentari false o alterate indicazioni geografiche o denominazioni d'origine[1] nonché, ai fini di trarne profitto, nell'introdurre in Italia, detenere per la vendita, porre in vendita o mettere comunque in circolazione i medesimi prodotti con indicazioni o denominazioni contraffatte.

Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941)

Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941)

Commette il primo delitto in esame chiunque, senza averne il diritto, a qualsiasi scopo ed in qualsiasi forma, mette a disposizione del pubblico un'opera dell'ingegno protetta o parte di essa,

[1] Ai sensi dell'art. 29 del D. Lgs. n. 30/2005 sono protette: "*le indicazioni geografiche e le denominazioni di origine che identificano un paese, una regione o una località, quando siano adottate per designare un prodotto che ne è originario e le cui qualità, reputazione o caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico d'origine, comprensivo dei fattori naturali, umani e di tradizione*".

immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere. In alcuni particolari casi - per finalità culturali o di libera espressione ed informazione e con determinate limitazioni - è consentita la comunicazione al pubblico di opere altrui[1].

Il secondo delitto in oggetto consiste nell'abusivo utilizzo dell'opera dell'ingegno altrui (mediante riproduzione, trascrizione, diffusione in qualsiasi forma, commercializzazione, immissione in reti telematiche, rappresentazione o esecuzione in pubblico, elaborazioni creative, quali le traduzioni, i compendi, ecc.) aggravato dalla lesione dei diritti morali dell'autore. Alla condotta di per sé già abusiva deve cioè aggiungersi anche la violazione del divieto di pubblicazione imposto dall'autore, o l'usurpazione della paternità dell'opera (c.d. plagio), ovvero la sua deformazione, mutilazione, o altra modificazione che offenda l'onore o la reputazione dell'autore.

Entrambe le incriminazioni si applicano in via residuale, quando non risulti presente il dolo specifico del fine di trarre un profitto od un lucro, che deve invece caratterizzare le condotte, in parte identiche, più severamente sanzionate dagli artt. 171-bis e 171-ter.

Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941)

Il primo comma della norma, con riferimento ai programmi per elaboratore[2], punisce le condotte di abusiva duplicazione, nonché di importazione, distribuzione, vendita, detenzione a scopo commerciale od imprenditoriale (quindi anche per uso limitato all'ambito della propria impresa), concessione in locazione, quando hanno per oggetto programmi contenuti in supporti privi del contrassegno della Società italiana degli autori ed editori (SIAE). Costituiscono inoltre reato l' approntamento, la detenzione o il traffico di qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione da utilizzi abusivi dei programmi.

Il secondo comma, con riferimento alla tutela dei diritti dell'autore di una banca di dati[3], punisce la riproduzione - permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma - su supporti non contrassegnati dalla SIAE, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o la dimostrazione in pubblico non autorizzate

[1] Si veda ad es. l'art. 65 della L. n. 633/1941, secondo il quale gli articoli di attualità pubblicati nelle riviste e nei giornali possono essere utilizzati da terzi, se la riproduzione non è stata espressamente riservata, purché si indichino la fonte, la data e l'autore.

[2] Ai sensi dell'art. 2, n. 8, della L. n. 633/1941 sono tutelati i programmi per elaboratore in qualsiasi forma espressi purché originali, quale risultato di creazione intellettuale dell'autore. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. Gli artt. 64-bis, 64-ter e 64-quater della citata legge disciplinano l'estensione dei diritti che competono all'autore del programma e i casi di libera utilizzazione dello stesso, vale a dire le ipotesi in cui sono consentite riproduzioni od interventi sul programma anche senza specifica autorizzazione del titolare dei diritti.

[3] Ai sensi dell'art. 2, n. 9, della L. n. 633/1941, le banche di dati consistono in raccolte di opere, dati od altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici od in altro modo. Resta ovviamente salva la distinta tutela riconosciuta ai diritti d'autore eventualmente esistenti sulle opere dell'ingegno inserite nella banca dati. Gli artt. 64-quinquies e 64-sexies della legge disciplinano l'estensione dei diritti dell'autore della banca di dati nonché i casi di libera utilizzazione della stessa.

dal titolare del diritto d'autore. Sono altresì sanzionate le condotte di estrazione e di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati, in violazione del divieto imposto dal costitutore[1] della medesima banca dati. Per estrazione deve intendersi il trasferimento di dati permanente o temporaneo su un altro supporto con qualsiasi mezzo o in qualsivoglia forma e per reimpiego qualsivoglia forma di messa a disposizione del pubblico dei dati mediante distribuzione di copie, noleggio, trasmissione con qualsiasi mezzo e in qualsiasi forma.
Tutte le predette condotte devono essere caratterizzate dal dolo specifico del fine di trarne profitto, vale a dire di conseguire un vantaggio, che può consistere anche solo in un risparmio di spesa.

Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941)

La norma elenca una nutrita casistica di condotte illecite - se commesse per uso non personale e col fine di lucro - aventi ad oggetto: opere destinate al circuito televisivo, cinematografico, della vendita o del noleggio; supporti di qualunque tipo contenenti opere musicali, cinematografiche, audiovisive, loro fonogrammi, videogrammi o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche, didattiche, musicali, multimediali. Sono infatti punite:

- le condotte di abusiva integrale o parziale duplicazione, riproduzione, diffusione in pubblico con qualsiasi procedimento;
- le condotte, poste in essere da chi non ha partecipato all'abusiva duplicazione o riproduzione, di introduzione in Italia, detenzione per la vendita o distribuzione, messa in commercio, cessione a qualsiasi titolo, proiezione in pubblico o trasmissione televisiva o radiofonica, far ascoltare in pubblico le duplicazioni o riproduzioni abusive;
- le medesime condotte elencate al punto che precede (salvo l'introduzione in Italia e il far ascoltare in pubblico) riferite a supporti di qualunque tipo, anche se non frutto di abusiva duplicazione o riproduzione, privi del prescritto contrassegno SIAE o con contrassegno falso.

Sono altresì sanzionate le condotte abusive concernenti, in sintesi: la diffusione di servizi ricevuti con decodificatori di trasmissioni criptate; i traffici di dispositivi che consentano l'accesso abusivo a detti servizi o di prodotti diretti ad eludere le misure tecnologiche di contrasto agli utilizzi abusivi delle opere protette; la rimozione o l'alterazione delle informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse

[1] I diritti del costitutore sono regolati dagli artt. 102-bis e 102-ter della L. n. 633/1941. Per costitutore si intende colui che effettua investimenti rilevanti per la creazione, la verifica o la presentazione di una banca di dati ed al quale compete, indipendentemente dalla tutela che spetta al suo autore in ordine ai criteri creativi secondo i quali il materiale è stato scelto ed organizzato, il diritto di vietare le operazioni di estrazione o di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati. Per le banche di dati messe a disposizione del pubblico, ad esempio mediante libero accesso on line, gli utenti, anche senza espressa autorizzazione del costitutore, possono effettuare estrazioni o reimpieghi di parti non sostanziali, valutate in termini qualitativi e quantitativi, per qualsivoglia fine, salvo che l'estrazione od il reimpiego siano stati espressamente vietati o limitati dal costitutore.

gravanti, ovvero l'importazione o la messa in circolazione di opere dalle quali siano state rimosse od alterate le predette informazioni.

Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941)

Commettono il reato i produttori od importatori di supporti contenenti software destinati al commercio che omettono di comunicare alla SIAE i dati necessari all'identificazione dei supporti per i quali vogliano avvalersi dell'esenzione dall'obbligo di apposizione del contrassegno SIAE[1].
E' altresì punita la falsa attestazione di assolvimento degli obblighi di legge rilasciata alla SIAE per l'ottenimento dei contrassegni da apporre ai supporti contenenti software od opere audiovisive.

Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941)

Il delitto è commesso da chiunque, per fini fraudolenti produce, importa, promuove, installa, pone in vendita, modifica o utilizza anche per solo uso personale, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

7.10.2 Attività aziendali sensibili

Con riferimento all'operatività bancaria, i rischi di commissione dei reati contro l'industria ed il commercio ed in materia di violazione del diritto d'autore più verosimilmente possono presentarsi:

- nei rapporti con la clientela, con riguardo alla concessione di finanziamenti o alla prestazione di servizi a favore di soggetti coinvolti nelle attività illecite in questione;
- nella partecipazione a gare pubbliche, con particolare riferimento a comportamenti illeciti nei confronti dei partecipanti;
- nell'approvvigionamento o nell'utilizzo di prodotti, software, banche dati ed altre opere dell'ingegno, strumentali all'attività della Banca o destinati ad omaggi per la clientela.

Meno rilevante appare il rischio con riferimento alle attività di ideazione e di lancio di nuovi prodotti, di gestione del naming e dei marchi del Gruppo, della comunicazione esterna o pubblicitaria e delle iniziative di marketing, nonché con riferimento alle attività di gestione dei rapporti con la clientela, nell'ottica della lealtà della concorrenza e della correttezza e trasparenza delle pratiche

[1] L'art. 181-bis, comma 3, della L. n. 633/1941 dispone che, fermo restando il rispetto dei diritti tutelati dalla legge, possono essere privi del contrassegno SIAE i supporti contenenti software da utilizzarsi esclusivamente tramite elaboratore elettronico, che non contengano opere audiovisive intere non realizzate espressamente per il programma per elaboratore, ovvero riproduzioni di parti eccedenti il 50% di preesistenti opere audiovisive, che diano luogo a concorrenza nell'utilizzazione economica delle stesse.

commerciali, e ciò in ragione della sviluppata articolazione dei presidi di controllo e delle procedure già imposti dalla normativa di settore.

Si rimanda pertanto ai protocolli previsti:

- al Capitolo 7.6.2.1 per il “Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose”;
- al Capitolo 7.2.2.8 per la ”Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali”;
- al Capitolo 7.2.2.9 per la “Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni”;
- al Capitolo 7.9.2.1 per la “Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo”;
- al Capitolo 7.2.2.1 per la “Stipula dei rapporti contrattuali con la Pubblica Amministrazione”,

  i quali contengono processi, principi di controllo e principi di comportamento diretti a prevenire anche la commissione dei reati di cui al presente Capitolo.