Banca Profilo

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del D.Lgs. n.231/2001

Aggiornamenti al documento

Edizione	Descrizione
Aprile 2008	Prima versione del Modello approvata dal Consiglio di Amministrazione del 24/4/2008
Dicembre 2011	Nuova impostazione del Modello e aggiornamento dei reati e dei presidi approvato dal Consiglio di Amministrazione del 15/12/2011
Giugno 2013	Aggiornamento dei reati e dei presidi. Approvato dal Consiglio di Amministrazione del 20/6/2013
Gennaio 2014	Approvato dal Consiglio di Amministrazione del 30/1/2014
Novembre 2015	Approvato dal Consiglio di Amministrazione del 5/11/2015
Dicembre 2016	Approvato dal Consiglio di Amministrazione del 15/12/2016
Settembre 2017	Approvato dal Consiglio di Amministrazione 14/9/2017
Ottobre 2018	Approvato dal Consiglio di Amministrazione 11/10/2018
Gennaio 2019	Approvato dal Consiglio di Amministrazione del 24/1/2019
Dicembre 2019	Approvato dal Consiglio di Amministrazione del 12/12/2019
Febbraio 2020	Modificato da parte dell'Amministratore Delegato e Direttore Generale in virtù della delega del Consiglio di Amministrazione del 12/12/2019
Dicembre 2020	Approvato dal Consiglio di Amministrazione del 17/12/2020
Febbraio 2022	Approvato dal Consiglio di Amministrazione del 10/2/2022
Ottobre 2022	Approvato dal Consiglio di Amministrazione del 20/10/2022
Dicembre 2024	Approvato dal Consiglio di Amministrazione del 19/12/2024

Indice e sommario

Premessa

DESCRIZIONE DELLA REALTÀ AZIENDALE, DEL MODELLO DI GOVERNANCE E DELL'ASSETTO ORGANIZZATIVO GENERALE DELLA SOCIETÀ

Descrizione della Società

Banca Profilo S.p.A. (di seguito anche la "**Banca**") è una società quotata, costituita nel 1988 in forma di Società per Azioni, con Sede legale a Milano, in Via Cerva 28.

La Banca appartiene al Gruppo bancario Banca Profilo e dal 2009 è indirettamente controllata dal Fondo Sator Private Equity Fund "A" L.P. che, attraverso la Capogruppo Arepo BP, detiene oltre il 60% di **Banca Profilo**, società quotata in Borsa dal 1999 con circa il 34% del capitale sul mercato.

Il Gruppo bancario Banca Profilo è costituito dalla Capogruppo (Arepo BP) e da società controllate ai sensi dell'art. 2359 del Codice Civile. In particolare, Arepo BP controlla **Banca Profilo** che, a sua volta, controlla le seguenti Società:

- Arepo Fiduciaria S.r.l. ("**Arepo Fiduciaria**");
- Profilo Real Estate S.r.l. ("**Profilo RE**").

Le suddette Società fanno parte del Gruppo bancario Banca Profilo.

Il *core business* della **Banca** ha ad oggetto l'attività bancaria, ossia la raccolta del risparmio tra il pubblico e l'esercizio del credito nelle sue varie forme. In particolare, la Banca offre servizi specialistici per la gestione del patrimonio di clienti privati e istituzionali e per le esigenze finanziarie delle imprese.

Essa, da statuto, può inoltre compiere, con l'osservanza delle disposizioni vigenti, tutte le operazioni e i servizi di intermediazione mobiliare, bancari e finanziari consentiti, ed emettere obbligazioni conformemente alle vigenti disposizioni normative.

Arepo BP, *holding* di partecipazioni, svolge in qualità di Capogruppo l'attività di direzione e coordinamento del Gruppo bancario Banca Profilo ai sensi dell'art. 61 T.U. 385/1993 ed emana disposizioni alle componenti del Gruppo per l'esecuzione delle istruzioni impartite dalla Banca d'Italia nell'interesse della stabilità del Gruppo.

Il modello di *Governance* della Banca

Il sistema di governo societario adottato dalla **Banca** è conforme alla normativa applicabile alle società quotate ed alla normativa bancaria e si ispira ai principi ed ai criteri del Codice di Autodisciplina per le società quotate promosso dalla Borsa Italiana.

Il modello di *Governance* della **Banca** e, in generale, tutto il suo sistema organizzativo, è pertanto strutturato in modo da assicurarle e garantire la massima efficienza ed efficacia operativa nel perseguimento dei propri scopi.

Banca Profilo ha, pertanto, adottato un modello di *governance* tradizionale fondato sull'interazione di due organi di nomina assembleare:

- Il Consiglio di Amministrazione;
- Il Collegio Sindacale.

La struttura di *corporate governance*, in linea con il modello di amministrazione e controllo tradizionale prescelto e in conformità con lo statuto, prevede dunque i seguenti Organi aziendali:

- Assemblea dei Soci, quale organo rappresentante l'universalità dei soci;
- Consiglio di Amministrazione, quale organo sul quale è incardinata la funzione di supervisione strategica;
- Presidente del Consiglio di Amministrazione, quale organo incaricato di garantire il buon funzionamento del Consiglio, favorire la dialettica endo-consiliare, l'effettivo bilanciamento dei poteri, l'assunzione di decisioni informate anche da parte degli Amministratori non esecutivi, in coerenza con i compiti in tema di organizzazione dei lavori del Consiglio di Amministrazione e di circolazione delle informazioni attribuiti dall'articolo 2381, comma 1 del Codice Civile;
- Collegio Sindacale, quale organo sul quale è incardinata la funzione di controllo e che ha la responsabilità di vigilare sulla funzionalità del complessivo sistema dei controlli interni e di accertare l'efficacia di tutte le strutture e funzioni coinvolte nel sistema dei controlli e l'adeguato coordinamento delle medesime;
- Comitato per le Remunerazioni, quale organo cui compete verificare, esaminare ed eventualmente formulare proposte in materia di remunerazione e di incentivazione;
- Comitato Controllo e Rischi, quale organo cui compete supportare le valutazioni e le decisioni del Consiglio di Amministrazione relative al sistema di controllo interno e di gestione dei rischi e le valutazioni relative al sistema di controllo interno e di gestione dei rischi e le valutazioni relative all'approvazione del bilancio individuale e consolidato. Ha inoltre compiti e poteri in materia di operazioni con parti correlate e/o soggetti ad esse connessi;
- Comitato Nomine, coinvolto nei processi (**i**) di nomina e cooptazione dei Consiglieri e dei responsabili delle Funzioni di Controllo, (**ii**) di verifica della sussistenza dei requisiti per l'assunzione della carica, (**iii**) di autovalutazione del Consiglio con riferimento all'individuazione del personale da utilizzare, (**iv**) di definizione dei piani di successione nelle posizioni di vertice dell'esecutivo o in altre posizioni, (**v**) di individuazione dell'obiettivo (*target*) in termini di quota di genere meno rappresentato;
- Amministratore Delegato, cui compete, unitamente al Direttore Generale, la funzione di gestione, sulla base delle deleghe attribuite dal Consiglio di Amministrazione. L'Amministratore Delegato svolge le funzioni di Amministratore Incaricato del sistema di controllo interno e di gestione dei rischi ai sensi del Codice;
- Direttore Generale, che rappresenta il vertice della struttura interna e, come tale, partecipa alla funzione di gestione;
- Dirigente preposto alla redazione dei documenti contabili societari ai sensi dell'articolo 154-bis del TUF, cui compete la definizione di procedure amministrative e contabili attendibili ed efficaci (in seguito anche Dirigente Preposto);
- Società di Revisione, cui compete la revisione legale dei conti.

Sistema delle Procure e delle Deleghe

La gestione di **Banca Profilo** S.p.A. è affidata al Consiglio di Amministrazione, composto da un Presidente del Consiglio, un Amministratore Delegato, un Vice Presidente del Consiglio e sei Consiglieri senza deleghe.

Al Presidente e all'Amministratore Delegato sono riservate la rappresentanza della **Banca** e determinati poteri meglio individuati in visura, cui si fa integrale rinvio.

Il Consiglio è investito dei più ampi poteri per la gestione ordinaria e straordinaria della **Banca** con facoltà di compiere tutti gli atti che ritiene opportuni per il raggiungimento e l'attuazione dello scopo sociale, esclusi soltanto quelli che la legge in modo tassativo riserva all''Assemblea. Sono pertanto di competenza del Consiglio di Amministrazione le delibere aventi ad oggetto:

a. la fusione nei casi previsti dagli artt. 2505 e 2505-*bis* c.c.;
b. l'istituzione o la soppressione di sedi secondarie;
c. l'indicazione di quali amministratori abbiano la rappresentanza della Banca;
d. la riduzione del capitale in caso di recesso del socio;
e. l'adeguamento dello statuto sociale a disposizioni normative;
f. il trasferimento della sede sociale in altro comune del territorio nazionale.

Sono riservate all'esclusiva competenza del Consiglio le decisioni concernenti:

- le linee e le operazioni strategiche e i piani industriali e finanziari;
- la determinazione degli indirizzi generali di gestione;
- l'approvazione e la modifica per quanto attiene all'assetto organizzativo e di governo societario;
- l'approvazione dei sistemi contabili e di rendicontazione;
- la supervisione del processo di informazione al pubblico e di comunicazione della banca;
- la verifica dell'attività di gestione svolta dagli organi delegati;
- la nomina e revoca del Direttore Generale e dei Dirigenti con poteri di firma e l'attribuzione dei relativi poteri;
- l'assunzione di partecipazioni, fatto salvo il disposto dell'art. 2361, c. 2 c.c., la cessione di partecipazioni;
- l'acquisto e la vendita di immobili;
- l'istituzione, il trasferimento e la soppressione di filiali, succursali, agenzie, dipendenze, uffici e recapiti;
- la promozione di azioni giudiziarie e amministrative in ogni ordine e grado di giurisdizione e sede fatte salve le azioni concernenti il recupero dei crediti, le rinunzie e le transazioni;
- l'approvazione e la modifica dei principali regolamenti interni;
- la costituzione di comitati interni agli organi aziendali;

- la nomina e la revoca del responsabile della funzione di revisione interna, del responsabile della funzione di conformità del responsabile della funzione di gestione del rischio, del responsabile della funzione antiriciclaggio, del delegato aziendale *ex* D.Lgs. 231/2007, art. 42, dei membri dell'Organismo di Vigilanza ai sensi del D.Lgs. 231/01;
- la definizione delle linee generali, degli indirizzi, delle politiche, dei processi, dei modelli, dei piani e dei programmi nelle materie tempo per tempo riservate alla competenza dell'organo con funzione di supervisione strategica dalla normativa primaria e secondaria.

Il Consiglio di Amministrazione può delegare proprie attribuzioni ad un Amministratore Delegato, determinando i limiti della delega, e conferire singoli incarichi a consiglieri. All'Amministratore Delegato è incaricato di sovrintendere alla gestione corrente e di curare l'esecuzione delle delibere del Consiglio.

L'Amministratore Delegato cura che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa e riferisce, con periodicità almeno trimestrale al Consiglio di Amministrazione sul generale andamento della gestione e sulla sua prevedibile evoluzione, nonché sulle operazioni di maggior rilievo economico, finanziario e patrimoniale effettuate dalla **Banca** e dalle sue controllate.

Non possono essere delegate le attribuzioni indicate negli artt. 2423, 2443, 2446, 2447, 2501-*ter* e 2506-bis del Codice Civile, nonché quelle indicate nell'art. 19, comma terzo, dello Statuto.

In casi urgenti, anche collegati all'attuazione del piano di risanamento del Gruppo bancario Banca Profilo, l'Amministratore Delegato, con il parere favorevole del presidente del Consiglio di Amministrazione, può assumere decisioni di competenza del Consiglio, fatta eccezione per le materie riservate alla esclusiva competenza del Consiglio di Amministrazione dalla legge o dallo Statuto. Le decisioni assunte dovranno essere riportate a conoscenza del Consiglio di Amministrazione nella prima riunione successiva.

Il Consiglio può nominare un Direttore Generale determinandone i poteri. Il Direttore Generale, ove diverso dall'Amministratore Delegato, riferisce all'Amministratore Delegato. Il Consiglio di Amministrazione può inoltre nominare dei Vice Direttori Generali che riferiscono al Direttore Generale, determinandone i relativi poteri.

Il Consiglio può altresì attribuire la firma sociale a dirigenti, funzionari e dipendenti con determinazione dei relativi poteri, dei limiti e delle modalità di esercizio. Il Consiglio può inoltre conferire mandati e procure anche a persone estranee alla Banca per il compimento di singoli atti e categorie di atti.
In base a tale sistema di procure, all'interno di Banca Profilo S.p.A. vi sono 17 procuratori che rappresentano la Banca negli ambiti identificati in visura, come da procure per categorie di atti depositate a Registro Imprese.

Rappresentanza legale della Banca

La rappresentanza legale della **Banca**, di fronte ai terzi ed in giudizio, e la firma sociale spettano al Presidente. In caso di assenza o impedimento, il Presidente è sostituito dal o da uno dei Vice Presidenti e, in mancanza, dall'Amministratore Delegato o dal Consigliere in sede più anziano nella carica. Di fronte ai terzi la firma di chi sostituisce il Presidente costituisce prova dell'assenza o dell'impedimento di questi.

All'Amministratore Delegato e al Direttore Generale, ove nominati, spettano la rappresentanza e la firma sociale nei limiti delle attribuzioni delegate e dei poteri ad essi conferiti dal Consiglio di Amministrazione.

In linea generale, il Presidente ha dunque il potere di nominare un difensore di fiducia per la Banca nell'ipotesi in cui sia indagata/imputata ai sensi del D.Lgs. 231/2001 per un reato presupposto commesso da un soggetto apicale o da soggetti sottoposti.

Tuttavia, l'art. 39 del D.Lgs. 231/2001 prevede che "*l'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo*".

La norma, quindi, prevede un divieto assoluto e generale di rappresentanza nell'ipotesi in cui il legale rappresentante della Banca abbia commesso il reato presupposto da cui è poi derivata la responsabilità dell'ente.

Pertanto, al fine di gestire correttamente il conflitto di interesse del proprio legale rappresentante indagato per il reato presupposto, il Consiglio di Amministrazione della Banca provvede a conferire procura speciale ad un soggetto diverso dal legale rappresentante affinché rappresenti la Banca in giudizio, in qualsiasi sede e grado ed innanzi a qualsiasi autorità giudicante, anche amministrativa, con espressa facoltà di nominare avvocati e consulenti tecnici a difesa della stessa.

Il Modello di Organizzazione, Gestione e Controllo della Banca

Il presente documento descrive il **Modello di Organizzazione, Gestione e Controllo** (di seguito, il "**Modello**") adottato da **Banca Profilo** ai sensi degli artt. 6 e 7 del Decreto Legislativo n. 231 dell'8 giugno 2001 (di seguito anche il **"Decreto"** o il "**D.Lgs. 231/2001**") e in ottemperanza alla "Direttiva in materia di responsabilità amministrativa degli Enti" della Capogruppo Arepo BP S.p.A. (di seguito la "**Direttiva**").

Sebbene l'adozione di un **Modello** sia prevista dal Decreto come facoltativa e non obbligatoria, la Banca - sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, nonché delle aspettative dei propri azionisti e del lavoro dei propri Dipendenti - ha ritenuto conforme alle proprie politiche aziendali procedere alla redazione del presente **Modello**.

Il **Modello** identifica l'insieme delle regole organizzative, operative e di comportamento - in funzione delle specifiche attività svolte dalla Banca - idonee a prevenire il rischio connesso al compimento dei reati previsti dal Decreto, nonché ad evitare che venga riconosciuta in capo alla Banca una responsabilità amministrativa conseguente alla commissione degli illeciti ad opera dei destinatari del presente **Modello** (cfr. il successivo paragrafo "Destinatari").

Alla luce di quanto indicato, si precisa che sono parte integrante del presente **Modello** le disposizioni interne della Banca tempo per tempo vigenti, ovvero:

- lo Statuto;
- la Carta dei Principi Codice di Comportamento;
- le Policy e i Regolamenti;
- il Manuale delle Procedure Aziendali;

- gli Ordini di Servizio;
- ogni altra disposizione interna a contenuto normativo e/o precettivo;

in quanto rappresentano parti sostanziali del sistema dei controlli e dei presidi predisposti dalla Banca, funzionali anche al raggiungimento degli scopi che si prefissa il **Modello** stesso.

Il **Modello**, infatti, si integra con l'intero *corpus* normativo interno che disciplina in via generale il presidio delle varie attività in capo alle unità organizzative della Banca, dettagliando l'articolazione dei poteri e delle deleghe interne nonché i presidi di controllo, fatto salvo quanto ulteriormente definito nelle singole schede di dettaglio contenute nel **Modello** stesso.

Le disposizione interne della Banca sono espressione del modello di *governance* aziendale sopra descritto; in particolare il documento **Poteri Delegati** definisce i criteri generali di esercizio dei poteri di gestione e di rappresentanza che il Consiglio di Amministrazione conferisce all'Amministratore Delegato e Direttore Generale, ai Dirigenti, Quadri Direttivi e Dipendenti, singolarmente o per il tramite di Comitati, fissandone i limiti e le modalità di esercizio secondo quanto previsto dall'art. 22 dello Statuto della Banca e definendo i principi generali applicabili ai diversi livelli delle strutture interne in termini di:

- firma sociale e *sub*-delega: il conferimento della rappresentanza legale della Banca, in giudizio e di fronte ai terzi;
- separazione tra funzione istruttoria e decisoria: le modalità e i ruoli di istruttoria circa i poteri decisori assegnati;
- sconfinamenti: le modalità e le motivazioni per il superamento dei limiti all'assunzione dei rischi;
- assorbimento gerarchico e supplenza: le modalità di assorbimento dei poteri, di gestione e di rappresentanza, conferiti, anche in caso di assenza o impedimento temporaneo.

Per ogni ambito di *business*, di controllo e operativo della Banca è presente una norma interna di rango superiore che trova declinazione operativa nel Manuale delle Procedure Aziendali che, in aggiunta ai meccanismi operativi di funzionamento delle diverse attività, declina i presidi di controllo in relazione alla gestione dei Rischi Operativi e di quelli relativi ai Processi sensibili ai fini dell'informativa contabile e finanziaria (*ex* Legge 262/05).

Il presente **Modello** si compone di tre Parti:

- **Parte Generale**: contiene i principi generali del **Decreto**, le modalità di adozione, integrazione e modifica del **Modello**, il sistema di formazione e diffusione del **Modello** ai Destinatari, i flussi informativi tra le Funzioni della **Banca** e l'Organismo di Vigilanza, nonché il Sistema Disciplinare in materia adottato dalla Banca;
- **Parte Speciale**: sono identificati, per ogni fattispecie di illecito trattato nel **Decreto** e rilevante per la **Banca**, le misure e i presidi predisposti dalla **Banca** al fine di prevenire la commissione di detti illeciti;
- **Allegati**: il **Modello** è completato da un **Allegato**, contenente l'elenco di tutte le fattispecie di reati previsti dal **Decreto**, che ne costituiscono parte integrante.

Quadro Normativo e Regolamentare

I riferimenti normativi a cui la **Banca** si è attenuta nella predisposizione del presente documento sono di seguito indicati:

- D.Lgs. 231/2001 e successive modificazioni ed integrazioni, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300";
- Relazione ministeriale accompagnatoria al D.Lgs. n.231/2001;
- D.Lgs. 58/1998 e successive modificazioni, "Testo Unico della Finanza";
- D.Lgs. 152/2006 e successive modificazioni, "Norme in materia ambientale";
- D.Lgs. 81/2008 e successive modificazioni, "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro";
- Legge 146/2006 e successive modificazioni "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001";
- Linee Guida ABI e successivi aggiornamenti, "Linee Guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche".

I PRINCIPI DEL DECRETO LEGISLATIVO N. 231/2001

Il 4 luglio 2001 sono entrate in vigore le disposizioni contenute nel Decreto Legislativo 8 giugno 2001, n. 231 ("*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*").

Il Decreto ha inteso adeguare la normativa nazionale in materia di responsabilità delle persone giuridiche ad alcune Convenzioni Internazionali a cui l'Italia aveva già da tempo aderito, quali la *Convenzione di Bruxelles del 26 luglio 1995* sulla tutela degli interessi finanziari delle Comunità Europee, la *Convenzione di Bruxelles del 26 maggio 1997* sulla lotta alla corruzione, nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri, e la *Convenzione OCSE del 17 dicembre 1997* sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Responsabilità amministrativa a carico delle Persone Giuridiche, Società e Associazioni

Il Decreto ha introdotto nell'ordinamento italiano un regime di **responsabilità amministrativa** (modellata sostanzialmente sullo schema della responsabilità penale) **a carico degli Enti** dotati di personalità giuridica e delle società e associazioni anche prive di personalità giuridica (di seguito gli "Enti"), per alcuni reati, analiticamente indicati dal Legislatore nel Decreto e sue successive integrazioni, qualora perpetrati nell'interesse o a vantaggio dell'Ente dai soggetti ad esso funzionalmente legati (soggetti in posizione apicale e soggetti sottoposti alla direzione e vigilanza di costoro) di cui all'art. 5 del Decreto, vale a dire:

- persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione e il controllo dell'Ente (cosiddetti "**soggetti apicali**");
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (cosiddetti "**soggetti sottoposti a direzione o vigilanza**").

In particolare, per soggetti apicali devono intendersi i componenti degli Organi Sociali ed il Direttore Generale.

Sono altresì da considerare apicali i soggetti cui è attribuita la responsabilità di un'Area della Banca.

Per l'individuazione dei soggetti sottoposti a direzione o vigilanza di uno dei soggetti apicali, di regola assumerà rilievo l'inquadramento in uno stabile rapporto di lavoro subordinato/parasubordinato, ma potranno rientrare nella previsione di legge anche situazioni particolari in cui un determinato incarico sia affidato a Soggetti Esterni legati alla **Banca** da specifico mandato (cfr. il successivo paragrafo "Destinatari").

La distinzione tra le due categorie di soggetti (apicali e sottoposti a direzione o vigilanza) rileva ai fini della responsabilità dell'Ente e dell'onere della prova; infatti, nel caso di reati commessi da soggetti apicali, sussiste in capo all'Ente una presunzione di responsabilità per la circostanza che

tali soggetti sono considerati espressione della politica aziendale e, quindi, rappresentanti della volontà dell'Ente.

Di contro, in caso di reato commesso dal soggetto sottoposto a direzione o vigilanza, ai sensi dell'art. 7 del **Decreto**, l'Ente è responsabile qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. In tal caso, la responsabilità dell'Ente è esclusa qualora, prima della commissione del reato, l'ente abbia adottato ed efficacemente attuato un **Modello** idoneo a prevenire reati della specie di quello compiuto.

Si sottolinea che il reato deve essere commesso dai soggetti *sub* a) o b) **nell'interesse o a vantaggio dell'Ente** stesso, conseguentemente resta esclusa la responsabilità dell'Ente qualora la persona fisica che commette il reato abbia agito nell'esclusivo interesse proprio o di soggetti terzi (art. 5, comma 2). I due requisiti dell'interesse e del vantaggio sono cumulabili, ma è sufficiente uno solo per delineare la responsabilità dell'Ente; il vantaggio, quale evento, fa riferimento alla concreta acquisizione di una utilità economica per l'Ente; l'interesse si configura qualora il soggetto abbia agito per una determinata finalità ed utilità, senza che sia necessario il suo effettivo conseguimento.

L'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli Enti che abbiano tratto vantaggio dalla commissione del reato o nell'interesse dei quali il reato sia stato commesso. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto, e sussiste anche quando l'autore del reato non è stato identificato o non è imputabile, ovvero quando il reato si estingue per causa diversa dall'amnistia.

Per tutti gli illeciti commessi sono infatti previste **sanzioni pecuniarie**; per i casi più gravi sono previste **misure interdittive**, quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione[(1)], l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi, oltre all'irrogazione di sanzioni amministrative/pecuniarie di varia entità.

Catalogo Illeciti amministrativi

I reati che fanno sorgere la responsabilità amministrativa dell'Ente sono espressamente indicati dal Legislatore e rientrano nelle seguenti **categorie**:

- Reati contro la Pubblica Amministrazione (art. 24 del **Decreto**);
- Delitti informatici e trattamento illecito dei dati (art. 24-*bis* del **Decreto**);
- Delitti di criminalità organizzata (art. 24-*ter* del **Decreto**);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione (art. 25 del **Decreto**);

---

(1) La **Pubblica Amministrazione** ricomprende le Autorità di Vigilanza, le Autorità Fiscali, nonché la Pubblica Amministrazione di Stati Esteri.

In tale ambito:

1. il **Pubblico Ufficiale** è la qualifica riconosciuta a tutti i soggetti, pubblici dipendenti o privati, che possono o debbono nell'ambito di una potestà regolata dal diritto pubblico formare e manifestare la volontà della Pubblica Amministrazione ovvero esercitare poteri autorizzativi o certificativi;
2. l'**Incaricato di Pubblico Servizio** è colui il quale, pur agendo nell'ambito di una attività disciplinata nelle forme della pubblica funzione, mancano dei poteri tipici di questa, purché non svolgano semplici mansioni d'ordine, né prestino opera meramente materiale;

- Falsità in monete, in carte di credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* del **Decreto**);
- Delitti contro l'industria e il commercio (art. 25-bis. 1 del **Decreto**);
- Reati societari (art. 25-*ter* del **Decreto**);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* del **Decreto**);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1 del **Decreto**);
- Delitti contro la personalità individuale (art. 25-*quinquies* del **Decreto**);
- Abusi di mercato (art. 25-*sexies* del **Decreto**);
- Omicidio colposo o lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies* del **Decreto**);
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché auto-riciclaggio (art. 25-*octies* del **Decreto**);
- Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies*.1 del **Decreto**);
- Delitti in materia di violazione del diritto d'autore (art. 25-*novies* del **Decreto**);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies* del **Decreto**);
- Reati ambientali (art. 25-*undecies* del **Decreto**);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25–*duodecies* del **Decreto**);
- Reati di razzismo e xenofobia (art. 25-*terdecies* del **Decreto**);
- Reato di frode in competizioni sportive e di esercizio abusivo di attività di gioco o di scommesse (art 25-*quaterdecies* del **Decreto**, rispettivamente art. 1 e art. 4 Legge 401/1989);
- Reati tributari (art 25-*quinquiesdecies* del **Decreto**) previsti da D.Lgs. 74/2000 ("Disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto");
- Reati di contrabbando (art. 25-*sexiesdecies* del **Decreto**);
- Delitti contro il patrimonio culturale (art. 25-*septiesdecies* del **Decreto**);
- Reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25- *octiesdecies*).

Per maggiori dettagli su tutti reati previsti dal Decreto si rinvia all'elenco analitico di cui all'**Allegato**.

L'elenco dei reati di cui all'**Allegato 1 – Catalogo degli illeciti amministrativi e dei reati presupposto della responsabilità degli Enti (decreto legislativo 8 giugno e 2001, n. 231)** ~~1~~ è suscettibile di modifiche ed integrazioni da parte del Legislatore. Da qui l'esigenza di una costante verifica sull'adeguatezza del **Modello** previsto dal **Decreto** e funzionale alla prevenzione dei reati (cfr. il successivo paragrafo "Regole di emanazione ed aggiornamento").

Il "Modello di Organizzazione, Gestione e Controllo" quale possibile esimente della responsabilità amministrativa

Soggetti "apicali"

L'art. 6 del **Decreto**, nell'introdurre il suddetto regime di responsabilità amministrativa per i reati commessi dai soggetti apicali, prevede una **forma** specifica **di esonero** da detta responsabilità qualora l'Ente dimostri che:

a. ha preventivamente adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b. il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo (cd. Organismo di Vigilanza);

c. le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli;

d. non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di cui alla precedente lett. b).

Per i reati commessi da soggetti apicali, quindi, non basta che l'Ente abbia adottato ed efficacemente attuato un **Modello di Organizzazione e di Gestione**. Occorre che l'Ente abbia anche affidato all'Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del **Modello**, e di curarne l'aggiornamento. È altresì necessario che l'Organismo di Vigilanza abbia svolto con cura i compiti di vigilanza e controllo e il reato sia stato commesso dai soggetti apicali eludendo fraudolentemente il **Modello** (art. 6, comma 1 del **Decreto**).

Sotto questo profilo, la funzione che l'Organismo di Vigilanza è chiamato ad adempiere è particolarmente delicata, in quanto lo stesso è chiamato a vigilare sull'effettiva operatività del **Modello**, a verificarne l'adeguatezza anche alla normativa vigente, a monitorare l'attività sociale ed a individuare eventuali nuove esigenze che richiedono un aggiornamento del **Modello** (si veda al riguardo il successivo paragrafo "ORGANISMO DI VIGILANZA").

Inoltre, sempre con riferimento all'esclusione della responsabilità dell'Ente nel caso in cui il reato sia stato commesso da un soggetto apicale, il **Decreto** prevede che – in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati - i modelli debbano rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati previsti dal **Decreto**;
- prevedere specifiche procedure dirette 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 reati;
- prevedere obblighi di informazione da parte dei soggetti coinvolti nei confronti dell'Organismo di Vigilanza;

- introdurre un sistema disciplinare interno, idoneo a sanzionare il mancato rispetto delle misure indicate nei modelli stessi.

Soggetti "sottoposti a direzione o vigilanza"

Diversamente, nel caso in cui il reato sia stato commesso dai soggetti sottoposti a direzione o vigilanza, l'art. 7 del **Decreto** prevede che l'Ente sia responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. Tali obblighi si presumono osservati qualora, prima della commissione del reato, l'Ente abbia "*adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi*".

Il **Decreto** stabilisce inoltre che l'efficace attuazione dei modelli richiede quantomeno: i) una verifica periodica e l'eventuale modifica dello stesso nell'ipotesi in cui vengano scoperte significative violazioni delle prescrizioni, ovvero qualora intervengano mutamenti nell'organizzazione o nell'attività dell'ente, nonché ii) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel **Modello**.

IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI BANCA PROFILO

Banca Profilo ha ritenuto opportuno adottare un **Modello di Organizzazione, Gestione e Controllo** ai sensi del **Decreto**, al fine di costruire un sistema strutturato e organico di presidi organizzativi, operativi e comportamentali nonché – più in generale - di attività di controllo, da svolgersi anche in via preventiva (controllo *ex ante),* volti a prevenire la commissione delle tipologie di illeciti contemplati dal **Decreto**.

Realizzazione del Modello

Per la costruzione del **Modello** la **Banca** ha analizzato tutte le fattispecie di reato richiamate dal Decreto al fine di identificare quelle rilevanti (di seguito "illeciti rilevanti") in relazione alla propria operatività, ovvero quelle che possono concretamente impegnare la responsabilità amministrativa della **Banca**.

La **Banca**, in relazione agli illeciti rilevanti, ha quindi: **i**) identificato i processi (e i soggetti coinvolti) nell'ambito dei quali può essere commessa ciascuna fattispecie di illecito rilevante, **ii**) mappato le misure ed i presidi adottati idonei a prevenire il rischio connesso al compimento di ciascun illecito.

Operativamente, con riferimento a ciascun **illecito rilevante** la **Banca**:

1. ha valutato il livello di rischio di compimento dell'illecito in considerazione della propria operatività, assegnando un livello di priorità (alto/basso);
2. ha identificato, per gli illeciti rilevanti a priorità alta, i processi (e i soggetti coinvolti) potenzialmente a "rischio reato", ossia i processi il cui svolgimento potrebbe costituire occasione di commissione dei reati di cui al Decreto, da sottoporre ad analisi e monitoraggio;
3. ha identificato e valutato l'idoneità dei presidi esistenti (descritti nelle disposizioni interne adottate dalla Banca) a prevenire il rischio di compimento dei reati;
4. qualora necessario, ha integrato i presidi esistenti con ulteriori presidi specifici ai fini del **Decreto**.

I risultati dell'analisi sono contenuti nella **Parte Speciale** del presente **Modello**.

Obiettivi perseguiti dalla Banca con l'adozione del Modello

Banca Profilo ritiene che l'adozione di un **Modello** possa concorrere efficacemente a sensibilizzare tutti coloro che operano in nome e per conto della **Banca** (cfr. paragrafo "Destinatari") affinché seguano comportamenti corretti e lineari nell'espletamento delle proprie attività.

In particolare, mediante la mappatura degli illeciti rilevanti, dei relativi processi "a rischio" e dei presidi posti in essere dalla **Banca**, il **Modello** si propone di:

- determinare, in tutti coloro che operano in nome e per conto della **Banca** nei processi "a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti, ma anche nei confronti della **Banca**;

- ribadire che tali forme di comportamento illecito sono condannate dalla Banca in quanto (anche nel caso in cui la **Banca** fosse apparentemente in condizione di trarne vantaggio) contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la **Banca** intende attenersi nell'espletamento della propria missione aziendale;
- consentire alla **Banca**, grazie a un'azione di monitoraggio sulle aree di attività "a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi;
- sensibilizzare e diffondere a tutti i livelli aziendali le regole comportamentali e le procedure istituite.

Destinatari

Sono destinatari del **Modello**:

- i soggetti in posizione apicale, ovvero componenti degli Organi Sociali, il Direttore Generale e i Responsabili di Area;
- i soggetti sottoposti a direzione o controllo, ovvero tutti coloro che intrattengano con la Banca un rapporto di lavoro subordinato (di seguito "Dipendenti") o parasubordinato (di seguito "Collaboratori") congiuntamente anche il "Personale";
- tutti coloro i quali, pur non essendo funzionalmente legati alla **Banca** da un rapporto di lavoro subordinato o parasubordinato, sono legati alla stessa da uno specifico mandato o da rapporti contrattuali (ad es. fornitura, ecc.), di seguito anche "Soggetti Esterni".

Si precisa che i contratti che regolano i rapporti con i Collaboratori e i Soggetti Esterni devono prevedere apposite clausole che indicano chiare responsabilità in merito al mancato rispetto del presente **Modello**.

L'insieme dei Destinatari, così come definito, è tenuto a rispettare tutte le disposizioni contenute nel **Modello** con la massima diligenza.

Diffusione del Modello e formazione dei Dipendenti e degli Organi Sociali

È obiettivo della **Banca** garantire, conformemente a quanto disposto dal **D.Lgs. 231/2001**, una corretta conoscenza e diffusione del contenuto del **Decreto** e del presente **Modello**, che ne costituisce l'attuazione, sia alle risorse già presenti nella Banca sia a quelle eventualmente da inserire.

Una copia del **Modello** è resa disponibile a tutti i **Dipendenti** della Banca tramite la pubblicazione del **Modello** stesso nella *Intranet* Aziendale.

In aggiunta a quanto sopra descritto, il **Modello** adottato e i relativi aggiornamenti:

- sono inviati dalla Funzione Organizzazione e Project Management a tutti i Dipendenti per *e-mail* con ricevuta di lettura; ciascun Dipendente deve attestare la ricezione del **Modello** secondo le modalità indicate dalla Funzione Organizzazione e Project Management stessa;

- sono consegnati a tutti i nuovi Dipendenti dalla Funzione Risorse Umane e Welfare Aziendale in sede di formalizzazione del rapporto contrattuale, che provvede alla raccolta della relativa attestazione di ricezione.

La diffusione del **Modello** e dei relativi aggiornamenti presso gli **Organi Sociali** è in capo alla Funzione Legale e Societario che inoltra via *e-mail* la documentazione e riceve tramite lo stesso canale da ciascun membro la relativa attestazione di ricezione.

Per quanto riguarda l'attività formativa, gestita dalla Funzione Risorse Umane e Welfare Aziendale in stretta cooperazione con l'OdV, ai Dipendenti e ai componenti degli Organi Sociali saranno fornite tutte le informazioni relative al **Modello** tramite un'apposita attività formativa periodica.

L'Organismo di Vigilanza cura, d'intesa con la Funzione Risorse Umane e Welfare Aziendale, che il programma di formazione sia adeguato ed efficacemente attuato. Le iniziative di formazione possono svolgersi anche a distanza o mediante l'utilizzo di sistemi informatici.

La partecipazione dei Dipendenti e dei componenti degli Organi Sociali alle attività formative è da ritenersi obbligatoria.

Diffusione del Modello ai Collaboratori e ai Soggetti Esterni

L'adozione ed il contenuto del presente **Modello** (nonché successivi aggiornamenti) sono altresì comunicati dalla Banca ai Collaboratori e ai Soggetti Esterni in modo che gli stessi possano provvedere a conformare il loro comportamento in base a quanto previsto dal **Modello** con riferimento alle attività in cui sono coinvolti e siano pertanto consapevoli delle conseguenze in caso di mancata osservanza dello stesso. A tal fine, la contrattualistica della **Banca** con i Collaboratori e i Soggetti Esterni prevede la consegna del **Modello** con relativa attestazione di ricezione.

Regole di emanazione ed aggiornamento

Il **Modello** viene adottato (e aggiornato) da parte della Banca con delibera del Consiglio di Amministrazione, sentito l'Organismo di Vigilanza. L'adozione del **Modello**, così come l'aggiornamento dello stesso devono essere comunicati alla Capogruppo Arepo BP, come richiesto dalla "Direttiva in materia di responsabilità amministrativa degli Enti" di Arepo BP S.p.A.

Il **Modello** deve essere aggiornato nel caso intervengano modifiche alla normativa di riferimento ovvero al sistema di procedure interne e di controlli adottato dalla **Banca**, nonché qualora si renda necessario integrare e/o modificare le regole e le norme comportamentali della **Banca**.
All'Organismo di Vigilanza spetta il compito di promuovere e coordinare il processo di aggiornamento e revisione del **Modello**, in stretta collaborazione con le altre Funzioni della **Banca** (es. Legale e Societario, Compliance e Antiriciclaggio, Organizzazione e Project Management, Internal Audit, Risorse Umane e Welfare Aziendale).

Whistleblowing

Ai sensi dell'art. 4 D.Lgs. 24/2023, gli enti soggetti alla normativa in materia di whistleblowing attivano "propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della

persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione".

La Banca ha dunque aggiornato – tramite una specifica procedura a cui si rimanda – il proprio sistema di segnalazione, attivando un canale interno atto a garantire la riservatezza delle segnalazioni di condotte illecite e delle violazioni del presente Modello, prevedendo altresì sanzioni disciplinari per le violazioni delle misure di tutela del segnalante e per le segnalazioni infondate effettuate con dolo o colpa grave.

I dipendenti sono informati dell'esistenza e delle modalità di uso di tali canali all'interno dei programmi di formazione nonché attraverso la consultazione del sito web della Banca all'indirizzo https://www.bancaprofilo.it/whistleblowing/.

Inoltre, al fine di rendere efficace la tutela del segnalante ed il funzionamento del meccanismo di segnalazione adottato a livello interno, la stessa norma sopra richiamata stabilisce che la gestione dei canali debba essere "affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato".

Nel caso di specie, come specificato al successivo paragrafo "Organismo di Vigilanza" del presente Modello, la gestione di tali canali è affidata all'Organismo di Vigilanza (Responsabile dei Sistemi Interni di Segnalazione o Responsabile Whistleblowing).

Quanto alle modalità di segnalazione, la normativa prevede che "le segnalazioni sono effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole".

In ossequio a tale disciplina, la Banca ha dunque attivato un canale di segnalazione tramite *tool* richiamabile all'indirizzo https://www.bancaprofilo.it/whistleblowing/, nonché previsto una modalità di invio delle segnalazioni tramite raccomandata. Tale *tool* e le segnalazioni cartacee sono gestite esclusivamente dal Responsabile Whistleblowing, nel rispetto della normativa relativa alla riservatezza.

Il D.Lgs. 24/2023 prevede altresì che la possibilità di effettuare **segnalazioni esterne** all'Autorità Nazionale Anticorruzione (ANAC), se ricorre, al momento della sua presentazione, una delle seguenti condizioni:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo non è attivo o, anche se attivato, non è conforme alla normativa esterna;
- è già stata effettuata una segnalazione interna e la stessa non ha avuto seguito, dove per "seguito" si intende l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;
- ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le informazioni relative ai canali di segnalazione interna ed esterna ed alle modalità di utilizzo sono disciplinate da apposita procedura detta "*Policy di Whistleblowing*", disponibile anche sul sito internet della Banca insieme alle istruzioni per la trasmissione di segnalazioni e all'informativa privacy.

Il Consiglio di Amministrazione della Banca ha altresì provveduto a nominare un Responsabile Sostituto dei Sistemi Interni di Segnalazione (*Responsabile Sostituto*), al quale andranno trasmesse le segnalazioni, all'indirizzo sostitutowhistleblowing@bancaprofilo.it, nel caso in cui il Responsabile Whistleblowing sia il presunto responsabile della violazione ovvero abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio, ovvero il Segnalatore coincida con il Responsabile Whistleblowing.

Ai sensi dell'art. 17 D.Lgs. 24/2023, i soggetti che adottano l'iniziativa della segnalazione non possono essere soggetti ad alcuna ritorsione.

L'art. 2, comma 1, lett. m), D.Lgs. 24/2023 definisce la ritorsione come "*qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto*".

In particolare, è previsto che "*nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati*" in quanto ritorsivi, "*si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere*".

Anche in tema di risarcimento del danno, la normativa prevede una presunzione a tutela delle persone protette in caso di segnalazione, stabilendo che "*in caso di domanda risarcitoria presentata all'autorità giudiziaria*" ed a condizione che le stesse dimostrino "*di aver effettuato, ai sensi del presente decreto, una segnalazione, una divulgazione pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno, si presume, salvo prova contraria, che il danno sia conseguenza di tale segnalazione, divulgazione pubblica o denuncia all'autorità giudiziaria o contabile*".

Per quanto riguarda il sistema disciplinare, in caso di violazione delle previsioni in materia di whistleblowing, si considera applicabile il sistema di sanzioni disciplinari di cui al paragrafo 5 della presente Parte Generale.

Ai sensi dell'art. 21 D.Lgs. 24/2023, "*fermi restando gli altri profili di responsabilità*", l'ANAC può applicare al responsabile le seguenti sanzioni amministrative pecuniarie:

- da 10.000 a 50.000 euro "quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza" dei soggetti tutelati;
- da 10.000 a 50.000 euro "quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme" alla normativa, "nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute".

ORGANISMO DI VIGILANZA

Nomina e composizione dell'Organismo di Vigilanza

L'Organismo di Vigilanza è un organo collegiale nominato da parte del Consiglio di Amministrazione della **Banca**, costituito da almeno 3 (tre) membri e la cui composizione deve essere comunicata alla Capogruppo, così come previsto dalla Direttiva.

La disciplina della nomina, della composizione, dei requisiti, della durata e del funzionamento dell'Organismo di Vigilanza è descritta nel dettaglio nel Regolamento interno dell'Organismo di Vigilanza, approvato dal Consiglio di Amministrazione della Banca.

Banca Profilo, nella seduta consiliare del 19 dicembre 2013, ha deciso di conformarsi al modello proposto dalla Banca d'Italia in materia prevedendo di investire il Collegio Sindacale dei compiti di OdV. Tale impostazione è stata successivamente attuata con delibera consiliare del 30 gennaio 2014.

Compiti e Poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza è **affidato** il compito di vigilare sul funzionamento e sull'osservanza del **Modello**. In particolare, il potere/dovere di vigilare che compete all'Organismo di Vigilanza riguarda:

- l'osservanza delle prescrizioni del **Modello** da parte dei destinatari, appositamente individuati nella **Parte Speciale** in relazione alle diverse tipologie di reati contemplate dal **Decreto**;
- la reale efficacia ed effettiva capacità del **Modello**, in relazione alla struttura aziendale, di prevenire la commissione dei reati di cui al **Decreto**;
- l'opportunità di aggiornamento del **Modello**, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali (cfr. il precedente paragrafo "Regole di emanazione ed aggiornamento").

In tale ambito, l'OdV può svolgere due tipi di verifiche nelle aree di attività "a rischio" identificate nel **Modello**:

- verifiche sugli atti: verifiche periodiche sugli atti prodotti dalla **Banca** o da essa comunque utilizzati/ricevuti (ad esempio: verifica dei principali atti societari in aree di attività a rischio);
- verifiche delle procedure: verifiche periodiche finalizzate ad analizzare l'effettivo funzionamento del presente **Modello**.

L'Organismo di Vigilanza svolge inoltre le funzioni di Responsabile dei Sistemi Interni di Segnalazione ai sensi della Policy di Whistleblowing (*Responsabile Whistleblowing)*.

Gli ulteriori poteri e le funzioni specifiche dell'Organismo di Vigilanza, così come le modalità di attuazione delle medesime, sono descritti in dettaglio nel Regolamento Interno dell'OdV.

FLUSSI INFORMATIVI DA E VERSO L'ORGANISMO DI VIGILANZA

L'art. 6, comma 2, lett. d) del **Decreto** individua specifici "obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli".

L'esistenza di sistematici flussi informativi rappresenta un fondamentale strumento per l'efficace svolgimento dei compiti dell'Organismo di Vigilanza.

Flussi informativi verso l'Organismo di Vigilanza e segnalazioni

Tutti i Destinatari dovranno portare a conoscenza dell'OdV, mediante invio allo stesso:

- ogni informazione, proveniente anche da terzi, attinente all'attuazione del **Modello**, sia di natura ufficiosa che relativa ad atti ufficiali;
- la documentazione prescritta nella **Parte Speciale** del **Modello** secondo le procedure ivi contemplate.

Flussi informativi verso l'Organismo di Vigilanza: obblighi di informativa relativi ad atti ufficiali

I Responsabili delle Funzioni della Banca devono trasmettere all'OdV, mediante invio all'indirizzo *e-mail* organismodivigilanza231@bancaprofilo.it, le informative concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per gli illeciti previsti dal **Decreto**;
- gli accessi o le richieste formulate delle Autorità di Vigilanza in sede di ispezione, aventi ad oggetto fattispecie che possano integrare la responsabilità della Banca ai sensi del **D.Lgs. 231/2001**;
- i rapporti preparati dai Responsabili stessi nell'ambito della loro attività di controllo (cd "di linea") dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del modello organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni erogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Flussi informativi verso l'Organismo di Vigilanza: flussi periodici e ad evento

Per quanto riguarda i flussi informativi periodici e ad evento indirizzati all'Organismo di Vigilanza da parte delle Funzioni della **Banca** si rimanda al Regolamento di Coordinamento e Collaborazione tra le Funzioni e gli Organi con Compiti di Controllo e alla documentazione allegata allo stesso.

Segnalazioni all'Organismo di Vigilanza anche nel ruolo di Responsabile Whistleblowing

In qualità di Responsabile Whistleblowing, l'Organismo di Vigilanza riceve le segnalazioni del Personale ai sensi della Policy di Whistleblowing.

Flussi informativi dall'Organismo di Vigilanza: flussi informativi nei confronti degli Organi Sociali

L'OdV riferisce in merito all'attuazione del **Modello** ed all'emersione di eventuali criticità. Sono assegnati all'OdV i seguenti flussi informativi verso gli organi sociali:

- su base continuativa, direttamente nei confronti dell'Amministratore Delegato e Direttore Generale;
- annualmente, nei confronti del Consiglio di Amministrazione.

In tale ambito, l'OdV predispone con cadenza annuale una relazione sull'attività svolta, avente per oggetto:

- l'attività svolta dall'OdV;
- le segnalazioni ricevute, anche ai sensi della Policy di Whistleblowing;
- gli eventi considerati rischiosi;
- le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni alla **Banca**, sia in termini di efficacia del **Modello**;
- annualmente, l'Organismo di Vigilanza invia al Consiglio di Amministrazione la programmazione delle attività per l'anno successivo.

Qualora l'OdV rilevi criticità riferibili all'Amministratore Delegato, al Presidente o ad uno o più membri del Consiglio d'Amministrazione, la corrispondente segnalazione verrà prontamente riferita a tutti i membri del Consiglio di Amministrazione che verranno prontamente convocati e riuniti con esclusione del soggetto interessato.

Gli incontri con gli Organi ai quali l'OdV riferisce devono essere verbalizzati e copie dei verbali devono essere custodite e archiviate dall'OdV stesso.

L'OdV potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione e dal Collegio Sindacale, qualora non coincida con l'Organismo di Vigilanza stesso, e potrà, a sua volta, presentare richiesta in tal senso, per riferire in merito al funzionamento del **Modello** o a situazioni specifiche.

Ove sia richiesta la presenza dell'OdV questa si ritiene sussistente anche ove non siano presenti tutti i suoi membri a condizione che:

- la convocazione sia stata inviata (o comunque sia nota) a tutti i membri;
- nessuno dei membri assenti si opponga con comunicazione scritta inviata in tempo utile agli altri membri.

L'OdV al fine di eseguire correttamente le proprie funzioni, ha la facoltà di coordinarsi con le Funzioni competenti presenti nella **Banca** per i diversi profili specifici.

Raccolta e conservazione delle informazioni

Ogni informazione, *report*, segnalazione sia cartacea sia su formato elettronico menzionata nel presente **Modello** o comunque inerente alle materie trattate nel medesimo, sarà opportunamente protocollata ed archiviata in formato cartaceo e/o per il tramite di apposita *directory* il cui accesso è riservato ai soli componenti dell´OdV.

Tutto il materiale di competenza e di interesse dell'OdV sarà archiviato nella *directory* per un periodo di tempo ordinariamente di 10 (dieci) anni, salvo che, per particolari necessità, l'OdV chieda un tempo di archiviazione maggiore. Il tempo di archiviazione della documentazione cartacea è al pari di quella informatica di 10 (dieci) anni, sempre fatto salvo che, per particolari necessità, l'OdV chieda un tempo maggiore.

I controlli dell'OdV

L'Organismo di Vigilanza della **Banca** effettua periodicamente dei controlli e delle ispezioni a campione sulle attività connesse ai processi sensibili individuati con particolare riferimento alle fattispecie di reato in esame nella **Parte Speciale**, allo scopo di verificare la conformità dei comportamenti posti in essere alle regole stabilite all'interno del **Modello**.

In particolare, in relazione alla prevenzione dei reati l'OdV deve:

- monitorare l'efficacia delle procedure interne;
- esaminare eventuali segnalazioni provenienti dagli organi di controllo, disponendo gli accertamenti ritenuti necessari;
- verificare periodicamente il rispetto delle altre procedure interne stabilite ai fini della prevenzione dai rischi-reato esaminati in tale **Parte Speciale**;
- compiere verifiche periodiche sulle comunicazioni alle Autorità pubbliche di vigilanza;
- verificare il sistema di deleghe e procure attualmente in vigore, individuando, ove necessario, le modifiche da apportare;
- indicare agli organi competenti le eventuali integrazioni ai sistemi di gestione finanziaria già adottati dalla **Banca**;
- decidere in merito all'opportunità di segnalare la necessità di adottare provvedimenti disciplinari.

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

L'OdV deve comunicare al Consiglio di Amministrazione i risultati della propria attività di vigilanza e controllo secondo le modalità e le tempistiche previste nella **Parte Generale** del presente **Modello di Organizzazione, Gestione e Controllo**.

SISTEMA DISCIPLINARE

In conformità alle disposizioni del **Decreto** (art. 6, comma 2, lett. e); art. 7, comma 4, lett. b)), la **Banca** prevede l'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel **Modello**.

Le misure disciplinari e le relative sanzioni, che compongono il sistema disciplinare, sono individuate dalla **Banca** in base ai principi di proporzionalità ed effettività (in base alla idoneità a svolgere una funzione deterrente e, successivamente, realmente sanzionatoria), e tenendo conto delle diverse qualifiche dei soggetti cui esse si applicano (dipendenti, amministratori, sindaci o collaboratori).

L'applicazione delle sanzioni disciplinari prescinde dall'esito di eventuali procedimenti penali e di procedimenti innanzi al Giudice del Lavoro, in quanto le regole di condotta imposte dal **Modello** sono assunte dalla **Banca** in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

Condotte sanzionabili

Costituiscono condotte sanzionabili ai sensi e per gli effetti del presente **Modello**:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, del **Modello** e dei principi e delle procedure dallo stesso previsti o stabiliti per la sua attuazione;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, anche mediante condotta omissiva, della redazione da parte di altri di documentazione non veritiera;
- l'omessa redazione della documentazione richiesta dal presente **Modello** o dalle procedure stabilite per la sua attuazione;
- la sottrazione, la distruzione o l'alterazione della documentazione concernente l'attuazione del **Modello**;
- l'ostacolo alla attività di vigilanza dell'Organismo di Vigilanza;
- l'impedimento dell'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti all'attuazione del **Modello**;
- la realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal **Modello**.

Costituiscono parimenti violazione del **Modello Organizzativo**:

- qualsiasi forma di ritorsione o di discriminazione, diretta o indiretta, nei confronti di chi ha fatto segnalazioni in buona fede di possibili violazioni del **Modello Organizzativo** o richieste di chiarimento sulle modalità applicative del **Modello** stesso[(2)];
- qualsiasi forma di violazione delle misure di tutela di coloro che effettuano le segnalazioni;

[(2)] l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo (art. 6, comma 2-*ter* del **D.Lgs. 231/2001**);

- il comportamento di chi dovesse accusare altri dipendenti di violazione dello stesso con la consapevolezza che tale violazione non sussiste.

In conformità con le disposizioni del Decreto è perseguibile, e pertanto sanzionabile, altresì il mero *tentativo* di attuazione delle condotte sopra descritte.

Inoltre, le sanzioni disciplinari sono comminate nei confronti dei membri del **Consiglio di Amministrazione** e dei **Responsabili** delle **Funzioni Banca** che, per negligenza o imperizia, non abbiano saputo individuare e conseguentemente eliminare, violazioni del **Modello** e, nei casi più gravi, la perpetrazione dei reati.

Sanzioni per i Dipendenti

I comportamenti sanzionabili ai sensi e per gli effetti del presente **Modello** tenuti dai lavoratori dipendenti costituiscono un inadempimento alle obbligazioni derivanti dal rapporto di lavoro, con ogni conseguenza contrattuale e di legge, anche con riferimento alla rilevanza delle stesse quale illecito disciplinare e/o alla conservazione del rapporto di lavoro. Con riferimento alle sanzioni erogabili nei riguardi di detti lavoratori dipendenti esse rientrano tra quelle previste dai Contratti Collettivi Nazionali di lavoro (Aree Professionali/Quadri Direttivi e Dirigenti), ai quali si rinvia per una completa trattazione del tema.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, in attuazione del principio di proporzionalità, saranno applicate in relazione:

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

Procedimento sanzionatorio a carico dei Dipendenti

Il procedimento sanzionatorio previsto dalla normativa interna della Banca è stato predisposto nel pieno rispetto delle procedure indicate dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e dal Contratto Collettivo Nazionale.

L'OdV, coerentemente con quanto previsto nel precedente paragrafo FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA del presente **Modello,** valuta direttamente tutte le segnalazioni ricevute e si confronta al riguardo con il Responsabile della Funzione Risorse Umane e Welfare Aziendale, salvo il caso in cui il soggetto coinvolto sia il medesimo Responsabile o un altro addetto operante in tale ufficio.

Nel corso di detta analisi, l'OdV collabora con il Responsabile della Funzione Risorse Umane e Welfare Aziendale comunicandogli tutte le informazioni di cui sia venuto in possesso in modo da attivare ed integrare efficacemente la procedura di indagine ed eventualmente il procedimento

disciplinare previsto dalla normativa interna della Banca (cfr. anche la procedura "Amministrazione del Personale" del Manuale delle Procedure Aziendali).

Concordemente l'OdV ed il Responsabile della Funzione Risorse Umane e Welfare Aziendale, determineranno altresì l'opportunità, ove possibile, di ascoltare direttamente l'autore della segnalazione e/o il responsabile della presunta violazione.

Il Responsabile della Funzione Risorse Umane e Welfare Aziendale o in sua vece l'OdV (nel caso in cui lo stesso Responsabile o un addetto dell'ufficio sia coinvolto nell'indagine), informerà l'Amministratore Delegato sugli sviluppi delle singole indagini attivate, interpellandolo per le decisioni risolutive da adottare.

In ogni caso nei confronti del Dipendente sospettato del compimento (o anche solo del tentato compimento) di condotte in violazione di quanto previsto dal presente **Modello** e più in generale della realizzazione di alcuno degli illeciti previsti nel **D.Lgs. 231/2001**, verrà applicato il procedimento disciplinare previsto dalla normativa interna della Banca (cfr. la procedura "Amministrazione del Personale" del Manuale delle Procedure Aziendali) e, qualora venga riconosciuto responsabile di tali condotte, verranno applicate le sanzioni previste dalla citata disciplina interna.

Misure nei confronti degli Amministratori

Nel caso in cui le condotte sanzionabili ai sensi e per gli effetti del presente **Modello** siano state poste in essere da parte di uno dei componenti del Consiglio di Amministrazione, l'OdV informerà il Consiglio di Amministrazione ed il Collegio Sindacale, anche ai fini della valutazione del corretto adempimento degli obblighi inerenti al mandato, i quali, con l'esclusione dell'Amministratore interessato, provvederanno ad assumere le iniziative ritenute opportune.

Nel caso in cui le condotte sanzionabili ai sensi e per gli effetti del presente **Modello** siano state poste in essere da parte della maggioranza dei componenti del Consiglio di Amministrazione, l'OdV informerà il Collegio Sindacale, ferma la competenza di cui all'art. 2406 c.c., provvederà a convocare l'Assemblea.

Misure nei confronti dei Collaboratori e Soggetti Esterni

Ogni comportamento posto in essere dai Collaboratori e dai Soggetti Esterni in contrasto con le linee di condotta indicate dal presente **Modello** e tale da comportare il rischio di commissione di illeciti potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o in altri accordi, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla **Banca**, come nel caso di applicazione da parte del Giudice competente delle misure previste dal **Decreto**.

Parte Speciale

La **Parte Speciale** del **Modello** definisce le regole operative, comportamentali e di controllo che devono guidare tutti i Destinatari del **Modello** nella gestione delle attività, al fine di prevenire la commissione dei reati previsti dal **Decreto**.

Tutti i Destinatari devono adottare comportamenti conformi a quanto prescritto nel Modello al fine di prevenire il verificarsi delle fattispecie di reato sotto descritte.

I REATI CHE POSSONO INTERESSARE LA BANCA

Tra le categorie di reati attualmente contemplate dal **Decreto**, la **Banca** ha individuato quelle che concretamente possono impegnare la propria responsabilità:

- Reati contro la Pubblica Amministrazione (art. 24 e art. 25);
- Delitti informatici e trattamento illecito dei dati (art. 24-*bis*);
- Falsità in monete, in carte di credito, in valori di bollo o in strumenti o segni di riconoscimento (art. 25-*bis*);
- Reati societari (art. 25-*ter*);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater*);
- Intermediazione illecita e sfruttamento del lavoro (art. 25-*quinquies*);
- Abusi di mercato (art. 25-*sexies*);
- Omicidio colposo o lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*);
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché auto-riciclaggio (art. 25-*octies*). Con specifico riferimento al reato di auto-riciclaggio, la Banca ha ritenuto, anche sulla base dell'orientamento espresso da Confindustria nella Circolare n. 19867, di circoscrivere i reati fonte dell'auto-riciclaggio esclusivamente ai reati presupposto della responsabilità dell'ente ex D.Lgs. 231/2001 comportanti movimentazione di liquidità;
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*);
- Reati ambientali (art. 25-*undecies*). Le fattispecie di reati ambientali a basso rischio di commissione non sono riportate nella **Parte Speciale** del **Modello**;
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*);
- Reati tributari (art 25-*quinquiesdecies*);
- Delitti in materia di strumenti di pagamento diversi dai contanti (art.25-octies 1 c.p.);
- Reati contro il patrimonio culturale (art. 25-*septiesdecies*);

- Reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*octiesdecies*).

La scelta della **Banca** di limitare l'analisi a queste categorie di reati, e adottare per essi gli specifici presidi di cui al **Modello**, è stata effettuata sulla base di considerazioni che tengono conto:

1. dell'attività svolta;
2. del contesto socioeconomico in cui opera;
3. dei rapporti e delle relazioni giuridiche ed economiche che la Banca istaura con soggetti terzi.

Per ciascuna delle suddette categorie, la **Banca** ha identificato i reati rilevanti in relazione alla propria operatività e valutato il livello di rischio di compimento (alto/basso).

Si precisa che si è ritenuto ragionevole non prevedere all'interno del presente **Modello** procedure e presidi specifici idonei a prevenire i reati a basso rischio di compimento, ovvero quelli appartenenti alle seguenti categorie:

- Delitti di criminalità organizzata (art. 24-*ter*);
- Delitti contro l'industria e il commercio (art. 25-*bis* 1);
- Delitti contro la personalità individuale (art. 25-*quinquies* e art. 25-*quater* 1) ad eccezione del delitto di Intermediazione illecita e sfruttamento del lavoro;
- Delitti in materia di violazione del diritto d'autore (art. 25-*novies*);
- Reati transnazionali (art. 10 Legge n. 146 del 16 marzo 2006);
- Alcune fattispecie di reati ambientali (art. 25-*undecies*);
- Delitti di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies*);
- Delitto di contrabbando (art. 25-*sexiesdecies*);
- Tra i reati contro la Pubblica Amministrazione (artt. 24 e 25), il reato di Frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L. 898/1986), il reato di concussione.

Per i reati appartenenti alle suddette categorie, così come gli altri reati previsti dal Decreto – e non considerati dal presente **Modello** – la **Banca** ritiene che possa costituire efficace sistema di prevenzione l'insieme dei principi e delle regole di *corporate governance*, desumibili dallo Statuto della **Banca** e dalla Carta dei principi e codice di comportamento e dal complesso della normativa organizzativa interna, nonché le specifiche attività di monitoraggio e gli specifici controlli svolti nell'ambito dell'ordinaria attività della **Banca**.

Nel seguito della presente **Parte Speciale** sono riportati, suddivisi per categoria, gli illeciti penali e amministrativi "**rilevanti**" per la **Banca** ai sensi del **Decreto**, con indicazione dell'eventuale rischio connesso al verificarsi dei medesimi in ragione dell'operatività della **Banca**.

Per ciascun illecito rilevante, sono inoltre identificati:

- i processi di riferimento, ovvero i processi a rischio "reato". La possibilità di commissione dei reati è valutata con riferimento esclusivo alle caratteristiche intrinseche dell'attività,

indipendentemente da chi la svolga e senza tener conto dei sistemi di controllo già operativi;

- i principali soggetti coinvolti nei processi “a rischio”;
- i principi generali di controllo e comportamento;
- le procedure specifiche idonee a prevenire il compimento dell’illecito. I relativi presidi possono essere costituti da disposizioni interne della Banca (Statuto, Policy e Regolamenti, Procedure del Manuale delle Procedure Aziendale, Ordini di Servizio o qualsiasi alla disposizione interna di carattere normativo e/o precettivo) in quanto parti sostanziali del sistema dei controlli predisposto dalla **Banca**.

MAPPA DEI REATI RILEVANTI AI FINI DELLA RESPONSABILITA' PREVISTA DAL D.LGS. N.231

Reati contro la Pubblica Amministrazione

Le fattispecie di reato

La presente **Parte Speciale** si riferisce ai reati realizzabili nell'ambito dei rapporti che possono intercorrere tra la **Banca** e la Pubblica Amministrazione, previsti dagli artt. 24 e 25 del **Decreto**.

La conoscenza delle fattispecie di reato e delle modalità di configurazione degli stessi, alla cui commissione da parte dei "soggetti qualificati" è collegata la responsabilità a carico della **Banca**, ai sensi dell'art. 5 del **D.Lgs. 231/2001**, è funzionale alla prevenzione dei reati e, di conseguenza, all'intero sistema di controlli previsto dal **Decreto**.

Agli effetti della legge penale rientra nell'ambito della Pubblica Amministrazione qualsiasi soggetto che:

- svolga attività legislativa, giurisdizionale o amministrativa disciplinata da norme di diritto pubblico;
- persegua, realizzi o gestisca interessi pubblici.

A titolo meramente esemplificativo e avendo riguardo all'operatività della **Banca** si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione:

- lo Stato, le Regioni, le Province, i Comuni;
- i Ministeri, i Dipartimenti, le Commissioni;
- gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT);
- l'Autorità Giudiziaria.

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.[3]

In forza delle norme sopra menzionate, è possibile attribuire la qualifica di Pubblico Ufficiale a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. In genere, l'esercizio di una pubblica funzione amministrativa viene riconosciuto con riferimento ai soggetti che formano o concorrono a formare la volontà dell'Ente pubblico, che lo rappresentano di fronte ai terzi o che sono muniti di poteri certificativi.

---

[3] Ai sensi dell'art. 357 c.p.: *"[I]. Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa.*
[II]. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".
Invece, in base all'art. 358 c.p.: *"[I]. Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*
[II]. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

La qualifica di incaricato di Pubblico Servizio è ravvisabile per esclusione, spettando ai soggetti che svolgono attività di pubblico interesse, alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale e che non consistono in semplici mansioni d'ordine o opere meramente materiali.

In ogni caso, non è necessariamente richiesta la sussistenza di un rapporto di impiego con un Ente pubblico, ai fini del riconoscimento in capo ad un determinato soggetto della qualifica di Pubblico Ufficiale o Incaricato di Pubblico Servizio.

Per quanto riguarda infine le Funzioni e i soggetti coinvolti in processi attinenti ai rapporti tra la **Banca** e la Pubblica Amministrazione all'interno della **Banca**, si identificano:

- tutte le Funzioni incaricate della predisposizione e/o invio di documenti/comunicazioni per le Autorità di Vigilanza e/o altro Ente Pubblico, e in generale tutte le Funzioni che hanno rapporti con le Autorità di Vigilanza e/o altro Ente Pubblico;
- Funzione Risorse Umane e Welfare Aziendale;
- Funzione Legale e Societario;
- Area IT for Business e ogni altra Funzione che vi abbia accesso;
- Area Digital;
- Outsourcer Informatico;
- Amministratore Delegato;
- Direttore Generale;
- Vice Direttori Generali;
- Funzione Corporate Services;
- Funzione Contabilità Generale;
- Funzione Bilancio e Fiscale;
- qualsiasi altro soggetto incaricato della selezione di un Fornitore/Consulente;
- Area Finanza;
- Area Private Banking;
- Area Investment Banking e Strategic Equity;
- ogni altra Funzione interessata alla richiesta di finanziamenti pubblici o alla partecipazione a gare pubbliche;
- qualsiasi Funzione o soggetto coinvolto in un contenzioso.

Si riporta di seguito una sintetica descrizione dei reati richiamati agli artt. 24 e 25 del **D.Lgs. n. 231/01**, nonché una breve esposizione delle possibili modalità attuative dei reati in esame.

Indebita percezione di contributi, finanziamenti o altre erogazioni in danno dello Stato o di altro ente pubblico o delle Comunità Europee (art. 316-ter c.p.)

Tale ipotesi di reato si configura quando si ottengano, pur 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. In tale fattispecie non ha alcuna rilevanza l'uso che viene fatto delle erogazioni, poiché il reato si perfeziona con il solo ottenimento degli indebiti finanziamenti.

Tale ipotesi di reato è residuale rispetto alla più grave fattispecie di truffa in danno dello Stato, riportato di seguito.

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

Tale reato si configura nel caso in cui – al fine di conseguire indebitamente erogazioni dello Stato, di enti pubblici o dell'Unione Europea – la Banca ponga in essere artifici o raggiri che possono consistere nell'alterazione del contenuto della documentazione (falsificazione/omissione di dati/informazioni dovute) predisposta e trasmessa ai funzionari dell'ente pubblico promotore del bando di finanziamento fornendo, ad esempio:

- l'attestazione di requisiti e referenze non veritiere quali, a titolo meramente esemplificativo, informazioni contabili e di bilancio, referenze, caratteristiche tecniche di soluzioni e servizi, dati sul dimensionamento dell'organizzazione aziendale, etc.;
- dichiarazioni, prospetti, report, fatture, relazioni e altra documentazione giustificativa delle spese effettuate, falsi o contenenti informazioni non vere;
- l'attestazione di altre informazioni finanziarie non veritiere o non realistiche in merito all'utilizzo del finanziamento richiesto.

L'elemento qualificante è costituito dall'oggetto materiale della frode.

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

Il reato in oggetto si configura qualora, utilizzando raggiri o artifici e in tal modo inducendo in errore altri soggetti, si consegua un ingiusto profitto in danno dello Stato, di altro ente pubblico o dell'Unione Europea. A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si consegua l'aggiudicazione della gara pubblica fornendo informazioni non veritiere.

Il reato potrebbe configurarsi nel caso in cui si consegua l'aggiudicazione della gara pubblica fornendo informazioni non veritiere, ad esempio, in caso di:

- alterazione/contraffazione del contenuto della documentazione trasmessa ai Soggetti Pubblici competenti;
- omissione di dati/informazioni contenuti nella documentazione trasmessa ai Soggetti Pubblici competenti qualora sia ravvisabile un danno patrimoniale in capo al Soggetto Pubblico coinvolto.

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

Il reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto, in danno dello Stato o di altro ente pubblico.

In concreto, il reato in esame potrebbe configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto.

Tale reato potrebbe essere commesso in linea di principio attraverso l'intervento diretto sui registri informatici della P.A., ad esempio:

- far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.);
- modificare dati fiscali/previdenziali di interesse della Banca (es. mod. 770), già trasmessi alla P.A..

Turbata libertà degli incanti e turbata libertà del procedimento di scelta del contraente (artt. 353 e 353-bis c.p.)

- Tali ipotesi di reato puniscono coloro che, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impediscono o turbano la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche Amministrazioni, ovvero ne allontana gli offerenti (art. 353 c.p.) e coloro che, salvo il fatto non costituisca più grave reato, con le medesime modalità di cui all'articolo 353 c.p., turbano il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione.

Frode nelle pubbliche forniture (art. 356 c.p.)

Tali ipotesi di reato punisce colui il quale commetta atti fraudolenti nell'esecuzione di un contratto di fornitura o nell'adempimento degli obblighi contrattuali che gli derivano da un tale contratto concluso con lo Stato, con un altro ente pubblico o con imprese esercenti servizi pubblici o di pubblica necessità.

Corruzione per un atto d'Ufficio e per un atto contrario ai doveri d'Ufficio (artt. 318, 319/319-bis, 320)

Tali ipotesi di reato si configurano nel caso in cui il Pubblico Ufficiale o l'incaricato di pubblico servizio ricevano, per sé o per altri, denaro o altri vantaggi non dovuti per esercitare proprie funzioni o poteri, ovvero per omettere o ritardare, o aver omesso o ritardato, o per compiere o aver compiuto un atto contrario ai doveri d'ufficio (determinando un vantaggio in favore del corruttore). Si ricorda che il reato di corruzione è un reato a concorso necessario, in cui vengono puniti sia il corrotto che il corruttore (cfr. art. 321 c.p.).

Tali reati si differenziano dalla concussione e dalla induzione indebita a dare o promettere utilità in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione e nella induzione indebita il privato è mero soggetto passivo, che subisce la condotta del Pubblico Ufficiale o dell'incaricato del pubblico servizio.

Il reato potrebbe sussistere, ad esempio, sia nel caso in cui il pubblico ufficiale, dietro corrispettivo, compia un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di una gara).

Le principali modalità di realizzazione dei reati di corruzione, anche in concorso con altri soggetti aziendali, sono di seguito riportate a titolo esemplificativo e non esaustivo:

- dazione/promessa di denaro, anche in concorso con altri, a funzionari pubblici o a enti terzi che gestiscono i rapporti ed eseguono le verifiche per conto delle Amministrazioni Pubbliche.

La provvista di denaro potrebbe essere creata, ad esempio, attraverso:

- emissione di fatture relative a operazioni inesistenti o rimborsi spese fittizi o per un ammontare diverso da quello delle spese effettivamente sostenute;
- assegnazione dell'incarico di gestire il rapporto con i Funzionari Pubblici a consulenti (la «disponibilità economica» per la dazione illecita potrebbe scaturire da un compenso per il consulente superiore a quello corrispondente alla prestazione effettuata);
- gestione impropria di donazioni, sponsorizzazioni, omaggi, atti di liberalità;
- riconoscimento/promessa di altre utilità al funzionario/soggetto pubblico realizzabile, anche in concorso con altri, attraverso:
- assunzione di persona legata al funzionario/soggetto pubblico da vincoli di parentela, affinità, amicizia o comunque su segnalazione di quest'ultimo;
- gestione impropria di donazioni, sponsorizzazioni, omaggi, atti di liberalità;
- stipulazione di contratti/lettere di incarico e di collaborazione con funzionari pubblici o soggetti da questi segnalati, al di fuori delle normali procedure di acquisto di consulenze/servizi o a condizioni economiche ingiustificatamente vantaggiose;
- fornitura di prodotti a prezzi ingiustificatamente vantaggiosi;
- affidamento di lavori/attività manutentive/micro-fasi di attività produttive a persona legata al funzionario/soggetto pubblico da vincoli di parentela, affinità, amicizia o comunque su segnalazione di quest'ultimo, al di fuori delle normali procedure o a condizioni economiche ingiustificatamente vantaggiose;
- stipulazione di contratti/lettere di incarico di collaborazione con persone segnalate dal funzionario/soggetto pubblico a condizioni non congrue alla prestazione ricevuta;
- condizioni contrattuali favorevoli da cui derivi un beneficio in termini di "valutazione delle performance" a soggetto pubblico.

Peculato (art. 314 c.p.) **e peculato mediante profitto dell'errore altrui** (art. 316 c.p.)

Le ipotesi di reato indicate ricorrono nei casi in cui il pubblico ufficiale o l'incaricato di pubblico servizio:

- si appropria del denaro o della cosa mobile altrui di cui abbia il possesso o la disponibilità per ragione del suo ufficio o servizio (art. 314 c.p.);

- nell'esercizio delle funzioni o del servizio riceve o ritiene indebitamente – per sé o per un terzo – denaro o altra utilità giovandosi dell'errore altrui (art. 316 co. I c.p.), con un aggravio di pena nel caso in cui il fatto offenda gli interessi finanziari dell'Unione Europea e il danno o il profitto siano superiori ad euro 100.000 (art. 316 co. II c.p.);

salvo che il fatto non costituisca un più grave reato.

Tali reati comportano l'estensione della responsabilità penale all'ente nel cui interesse o vantaggio siano stati commessi soltanto qualora i rispettivi fatti-reato abbiano offeso gli interessi finanziari dell'Unione Europea.

Indebita destinazione di denaro o cose mobili (art. 314-*bis* c.p.)

Al di fuori dei casi previsti dall'articolo 314 richiamato sopra, la fattispecie di recente introduzione di cui all'art. 314-*bis* c.p. punisce il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di

altra cosa mobile altrui, li destina ad un uso diverso da quello previsto da specifiche disposizioni di legge o da atti aventi forza di legge dai quali non residuano margini di discrezionalità e intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale o ad altri un danno ingiusto.

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

Il reato in esame si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli.

Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-*bis* c.p.)

L'articolo in esame estende l'applicazione dei reati di peculato (art. 314 c.p.), peculato mediante profitto dell'errore altrui (art. 316 c.p.), concussione (art. 317 c.p.), corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319 ter c.p.), induzione indebita a dare o promettere utilità (art. 319-*quater* c.p.) e istigazione alla corruzione attiva (art. 322 co. 3 e 4 c.p.) ai casi in cui il soggetto attivo pubblico del reato appartenga ad enti, istituzioni o organi giurisdizionali dell'Unione Europea, della Corte Penale Internazionale o di organizzazioni internazionali, ovvero eserciti funzioni corrispondenti a quelle di pubblico ufficiale o incaricato di pubblico servizio nell'ambito dei predetti enti, istituzioni ed organi, oltre che nell'ambito di altri Stati membri dell'UE, oppure non membri dell'UE quando – in tal caso – il fatto offenda gli interessi finanziari dell'Unione.

La norma estende altresì l'applicazione dei reati di induzione indebita, corruzione e istigazione alla corruzione – di cui agli artt. 319 quater, 321 e 322 co. I e II c.p. – ai casi in cui il denaro sia dato, offerto o promesso ai predetti soggetti o alle persone che esercitano funzioni o attività

corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di altri Stati esteri o di organizzazioni pubbliche internazionali.

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

Il reato si configura nel caso in cui i fatti di corruzione di cui alle fattispecie precedenti siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Potrà dunque essere chiamata a rispondere del reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario) al fine di ottenerne la positiva definizione.

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

Il reato ricorre quando il Pubblico Ufficiale o l'Incaricato di un Pubblico Servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Mentre nella concussione (art. 317 c.p.) il privato è vittima di un abuso costrittivo sotto forma di una prospettazione di un male ingiusto, nell'induzione indebita il privato subisce un'attività di persuasione o pressione morale, a seguito della quale presta acquiescenza per la prospettiva di un indebito tornaconto personale. Per questo motivo, anche il privato che dà o promette di dare denaro o altra utilità è sottoposto a sanzione.

Costituisce, ad esempio, un'ipotesi di induzione indebita la proposta da parte di un ispettore del lavoro di omettere i controlli nei confronti di un'impresa in cambio di incarichi professionali al figlio, non essendovi in questo caso prospettazione di male ingiusto e agendo il privato in vista di un vantaggio indebito.

Traffico di influenze illecite (art. 346-*bis* c.p.)

Il reato in esame si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli dal soggetto privato, ovvero nel caso in cui quest'ultimo rifiuti di aderire alla richiesta o promessa di denaro o altre utilità proveniente dal funzionario pubblico.

Il reato in esame punisce la condotta di colui il quale, utilizzando intenzionalmente allo scopo relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di pubblico servizio, ovvero con taluno dei soggetti indicati all'art. 322-*bis* c.p., si faccia dare o promettere indebitamente, a sé o ad altri, denaro o altre utilità come prezzo della propria mediazione illecita con il funzionario pubblico ovvero per remunerarlo in relazione all'esercizio delle sue funzioni, prevedendo un innalzamento della sanzione nel caso in cui tali fatti siano commessi in relazione all'esercizio di attività giudiziarie.

I processi e le attività sensibili

L'art. 6, comma 2, lett. a) del **D.Lgs. n.231/2001** indica, come uno degli elementi essenziali dei Modelli di Organizzazione, Gestione e Controllo previsti dal **Decreto**, l'individuazione delle attività "sensibili" nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal **D.Lgs. n.231/2001**.

L'analisi dei processi posti in essere dalla **Banca** ha consentito l'individuazione delle attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato esaminate in questa sede.

Le attività ritenute sensibili in relazione ai reati verso la Pubblica Amministrazione all'interno di **Banca Profilo** S.p.A. sono le seguenti:

- gestione dei rapporti con le Autorità di Vigilanza e /o altro Ente Pubblico (in particolare, UIF, Guardia di Finanza, INPS, Ispettorato del Lavoro, Agenzia delle Entrate, ecc.);
- gestione del contenzioso (con i Dipendenti, tributario, ordinario o amministrativo);
- gestione sicurezza sistemi informativi;
- Outsourcer informativo;
- gestione del contenzioso (con i Dipendenti, tributario, ordinario o amministrativo);
- selezione/assunzione/gestione delle Risorse Umane;
- selezione dei Fornitori/Consulenti;
- prestazione servizi di investimento, attività bancaria o altri servizi alla Clientela.

Regole generali

Principi generali di controllo

I principi generali di controllo, alla base degli strumenti e delle metodologie utilizzate per il monitoraggio dei procedimenti sopra descritti, sono i seguenti:

- separazione delle attività, tra chi autorizza, chi esegue e chi controlla i processi sopra elencati;
- esistenza di procedure, norme e circolari formalizzate allo scopo di fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili, nonché di identificare le modalità di archiviazione della documentazione rilevante;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate, nonché chiaramente definiti e diffusi all'interno della Banca;
- tracciabilità di ogni operazione relativa a ciascuna attività sensibile individuata mediante la idonea registrazione di ogni fatto ad essa relativo. In tal modo è possibile verificare a posteriori il processo di decisione, autorizzazione e svolgimento delle attività sensibili in esame.

I principi generali di comportamento

La presente **Parte Speciale** prevede l'espresso divieto a carico del Consiglio di Amministrazione della **Banca** in via diretta, nonché dei suoi dirigenti, dipendenti, consulenti e partner, limitatamente agli obblighi previsti nelle specifiche procedure e nelle clausole inserite nei contratti, di:

- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire finanziamenti, contributi o erogazioni di varia natura;
- destinare le somme ricevute da detti organismi pubblici a scopi diversi da quelli per i quali sono stati concessi;
- presentare dichiarazioni non veritiere ad Organismi Pubblici nazionali o comunitari al fine di conseguire autorizzazioni, licenze e provvedimenti amministrativi di qualsivoglia natura;
- presentare alle Autorità Pubbliche documentazione falsa o attestante cose non vere ovvero omettere la comunicazione di fatti e informazioni rilevanti al fine di evitare ispezioni, sanzioni accertamenti;
- effettuare o promettere, a favore dei Clienti, condizioni che non trovano adeguata giustificazione in relazione del rapporto contrattuale con essi costituito;
- riconoscere, in favore dei fornitori e dei consulenti esterni, prestazioni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alla prassi vigente nel settore di attività interessato.

Alle eventuali ispezioni, perquisizione o comunque agli accessi condotti dalla Autorità pubbliche di Vigilanza presso la sede della Banca, devono intervenire i soggetti aziendali a ciò espressamente delegati. Ogni incontro deve essere debitamente documentato e deve avvenire alla presenza di almeno due rappresentanti della Banca, salvo casi di forza maggiore. In particolare, devono essere presenti almeno due persone, ovvero il Responsabile di Funzione accompagnato dalla Direzione e/o da uno dei più stretti Collaboratori.

In caso di visite ispettive, deve essere garantita la massima collaborazione di tutte le Funzioni interessate con l'individuazione di un referente, affinché sia garantita la più ampia e tempestiva collaborazione a dette Autorità, fornendo dati e documenti richiesti in modo tempestivo e completo; copia dei verbali redatti in sede di ispezione, perquisizione o accesso deve essere trasmessa all'Amministratore Delegato e Direttore Generale.

Nell'ambito della prestazione di servizi di investimento o bancari a Clientela legata alla Pubblica Amministrazione, è necessario godere di una specifica autorizzazione in tal senso da parte della Banca (consistente in un'apposita delega).

Gli amministratori ed i sindaci devono adempiere ai doveri loro imposti dalla legge e dallo statuto con la massima diligenza e, nel caso in cui vengano a conoscenza di fatti pregiudizievoli per la Banca, devono attivarsi, al fine di eliminarne o attenuarne le conseguenze dannose per la stessa, gli organi statutari e i rispettivi componenti nonché per i creditori, dandone segnalazione all'Organismo di Vigilanza.

Procedure specifiche

La **Banca** ha altresì implementato procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Regolamento della Funzione Internal Audit
- Regolamento della Funzione Compliance
- Regolamento Antiriciclaggio
- Regolamento ICAAP
- Rischio informatico e Continuità operativa
- Policy di Sicurezza Informatica
- Policy di Sicurezza Informatica per i servizi di pagamento via internet
- Documento di Indirizzo Strategico in materia di Sistemi Informativi
- Norme contrattuali con Outsourcer informatico
- Strategia di classificazione della Clientela
- Capitolo S.02.01 - Gestione comunicazioni periodiche
- Capitolo S.02.02 - Gestione di comunicazioni e di richieste di dati e di informazioni
- Capitolo S.02.03 - Segnalazioni di vigilanza
- Capitolo S.03.01 - Monitoraggio dei rischi
- Capitolo S.04.01 - Antiriciclaggio e antiterrorismo
- Capitolo S.06.01 – Gestione delle attività societarie
- Capitolo S.06.02 - Gestione dell'attività legale e del contenzioso
- Capitolo S.08.07 - Fornitori e fatturazione
- Capitolo S.08.10 - Fatturazione e altre attività contabili relative all'Area Investment Banking e Strategic Equity e all'Area Finanza
- Capitolo S.09.01 - Selezione, assunzione, trasferimento e cessazione del Personale
- Capitolo S.09.02 - Valutazione, sviluppo, formazione e revisione salariale
- Capitolo S.09.03 - Amministrazione del Personale
- Capitolo S.11.01 - Gestione delle Tecnologie e Sistemi, Applicazioni e attività connesse (con Appendici sulla Sicurezza Informativa)
- Capitolo S.13.01 - Gestione acquisti e servizi logistici/ausiliari
- Capitolo B.01.01 - Apertura rapporti della Clientela Private Banking (gestione deroghe)
- Capitolo B.01.03 - Gestione rapporti della Clientela Finanza
- Capitolo B.09.01 - Investment Banking e Strategic Equity - Gestione delle attività di Business dell'Area

- Capitolo B.10.06 - Prevenzione e gestione delle frodi

Reati informatici

Le fattispecie di reato

L'art. 24-*bis* del **D.Lgs. n.231/2001** individua le fattispecie di reati informatici e trattamento illecito di dati la cui commissione espone la **Banca** a responsabilità amministrativa.

L'ambito applicativo della norma è stato ulteriormente esteso dall'art. 1, comma 11 *bis* D.L. 21 settembre 2019, n. 105 (convertito con modificazioni dalla L. 18 novembre 2019, n. 133), che ha introdotto tra i reati presupposto le fattispecie criminose previste dalla medesima fonte a tutela del c.d. Perimetro di Sicurezza Nazionale Cibernetica.

Tali fattispecie, tuttavia, sono soggette ad un'applicazione settoriale, in quanto poste a tutela della "*sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale*", così come individuati dal D.P.C.M. 131/2020.

Deve inoltre considerarsi che tra i reati a carattere informatico rilevanti ai fini del Decreto rientra altresì la fattispecie di frode informatica *ex* art. 640-*ter* c.p., previsto come reato presupposto dall'art. 24 del Decreto "*se commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea*".

Da ultimo, va segnalato il recente intervento della Legge 28 giugno 2024, n. 90, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", che ha:

- apportato modifiche alle fattispecie già esistenti con inasprimenti delle pene;
- abrogato l'art. 615 *quinquies* c.p.;
- introdotto nuove fattispecie ("*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" (art. 635 *quater* 1 c.p., in sostituzione dell'art. 615 quinquies c.p. abrogato) ed una particolare ipotesi di estorsione (art. 629, comma 3, c.p.)) e nuove attenuanti e aggravanti;
- nonché introdotto **modifiche all'art. 24 *bis* del Decreto**.

Tali modifiche hanno comportato un inasprimento delle sanzioni pecuniarie previste e l'inclusione delle fattispecie di nuova introduzione (artt. 629, comma 3, e 635 *quater* 1 c.p.) nel novero dei reati presupposto.

La diffusione capillare di strumenti informatici, come *personal computer* fissi e portatili, cellulari altamente sofisticati, e dispositivi in grado di effettuare connessioni veloci a sistemi complessi che regolano le operazioni di centinaia di persone presenti all'interno di strutture organizzative è essenziale quanto foriera di rischi per qualsiasi impresa.

La digitalizzazione e crescente adozione di *devices* tecnologici ha dunque imposto una specifica necessità di impostazione degli standard di sicurezza nel rispetto dei quali tutti i soggetti aziendali possano operare in via informatica o telematica nel rispetto delle limitazioni imposte dalla

normativa a tutela della *privacy*, senza esporre la **Banca** a conseguenze ai sensi del **D.Lgs. n.231/2001**.

Le attività nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizzi le tecnologie dell'informazione. La presente **Parte Speciale** si applica, quindi, a tutte le funzioni coinvolte nella gestione e nell'utilizzo dei sistemi informatici e del patrimonio informativo e si riferisce ai comportamenti posti in essere da amministratori, sindaci, dirigenti, dipendenti, collaboratori, clienti, fornitori e, più in generale, ogni altro soggetto che, direttamente e/o indirettamente, instaura a qualsiasi titolo rapporti e relazioni di collaborazione con la **Banca** o opera per perseguirne gli obiettivi, con particolare riferimento alle seguenti Aree e Funzioni:

- Area IT for Business e tutte le Aree/le Funzioni della Banca che vi hanno accesso;
- Area Digital;
- tutte le Aree/le Funzioni incaricate della produzione di documenti informativi con idoneità probatoria;
- Outsourcer Informatico;
- Area Private Banking;
- Area Amministrazione e Controllo.

Le fattispecie di reato previste sono le seguenti:

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

Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico.

In particolare, per sistema informatico, ai fini della configurabilità del delitto di cui all'art. 615-*ter* c.p., deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche. Il sistema è dunque tale esclusivamente se gestisce ed elabora dati, mentre tutto ciò che non è in grado di gestire o elaborare dati per lo svolgimento di una funzione non è sistema informatico.

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

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

Detenzione, diffusione abusiva di apparecchiature, codici e altri mezzi atti all'accesso ai sistemi informatici o telematici (art. 615-*quater* c.p.)

L'art. 615-*quater* punisce la condotta di detenzione e di diffusione abusiva di codici di accesso che può portare alla commissione di altri reati informatici quali, ad esempio, l'accesso abusivo o la diffusione di tali codici a soggetti terzi, nonché, in seguito alla recente riforma in materia, l'installazione abusiva di apparecchiature o altri mezzi volti ad accedere abusivamente a sistemi informatici. L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo: può infatti trattarsi di una password, di un codice d'accesso o semplicemente di informazioni che consentano di eludere le misure di protezione. La disposizione in esame incrimina due tipi di condotte volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui oppure a procurare ad altri tali mezzi o comunque le informazioni sul modo di eludere le barriere di protezione; non è invece punita la semplice detenzione di codici di accesso o di strumenti similari da parte di chi non sia autorizzato a farne uso.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-*quarter*.1 c.p.)

La norma, di recente introduzione, punisce colui il quale, allo scopo di:

- danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti; o
- favorirne l'interruzione totale o parziale o totale o l'alterazione;
- abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o comunque, mette in altro modo a disposizione di altri o comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

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

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

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

La comunicazione è invece impedita quando se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati; una comunicazione può invece essere

interrotta sia agendo sul sistema che invia e che deve ricevere la comunicazione sia, ad esempio, deviando il flusso dei dati in corso di trasmissione da un elaboratore ad un altro.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche *(art. 617-quinquies c.p.)*

La norma punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

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

Oggetto del danneggiamento può essere innanzitutto un sistema informatico di qualsiasi tipo e dimensione eventualmente collegato a distanza con altri elaboratori come nel caso dei sistemi telematici.

L'aggressione può rivolgersi tanto al sistema nel suo complesso quanto a una o più delle sue componenti materiali, quali a titolo esemplificativo, le periferiche.

Non possono invece essere considerati componenti di un sistema informatico, ma anche di interrompere o alterare il funzionamento di quest'ultimo i supporti magnetici o ottici sui quali non siano memorizzati dati o programmi, in quanto il loro danneggiamento non arreca nessun pregiudizio alla funzionalità del sistema informatico nel quale dovrebbero essere utilizzati.

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

Suscettibili di danneggiamento possono essere anche dati o programmi immagazzinati nella memoria interna dell'elaboratore oppure su un supporto esterno.

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

Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e la inservibilità totale o parziale. L'ipotesi di distruzione di dati e programmi più frequente e significativa è rappresentata dalla loro cancellazione: sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con nuovi dati diversi, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa.

Poiché la distruzione deve essere totale, non ricorre questa ipotesi quando i dati o i programmi cancellati siano ancora recuperabili in una zona remota dell'elaboratore, utilizzando un determinato tipo di programma oppure ne sia stata solo impedita la visualizzazione sullo schermo del computer.

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

La norma punisce, con clausola di riserva, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

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

La norma punisce chiunque, mediante le condotte di cui all'articolo 635-*bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

La norma prevede un aumento di pena nel caso in cui il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

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

La condotta incriminata dall'art. 635-*quinquies* c.p. consiste nel danneggiamento diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

La norma prevede un aumento di pena se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, nonché nel caso in cui il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

Documenti informatici (art. 491-*bis* c.p.)

La norma sanziona con le disposizioni del Capo III del Titolo VII del Libro II del codice penale le falsità previste da quel Capo che riguardano un documento informatico pubblico avente efficacia probatoria.

Estorsione informatica (art. 629, terzo comma c.p.)

La norma punisce colui il quale, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies* ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Violazione delle norme in materia di Perimetro di sicurezza nazionale *cibernetica* (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

La norma punisce colui che, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle

attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

I processi e le attività sensibili

I delitti oggetto della presente **Parte Speciale** trovano come presupposto l'utilizzo della rete informatica intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e precisamente:

- tutte le attività aziendali svolte dal personale tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e accesso a *Internet*;
- gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa di *Information Technology* nonché la sicurezza informatica.

L'analisi dei processi posti in essere dalla Banca ha consentito pertanto l'individuazione delle seguenti attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato esaminate in questa sede:

- gestione delle attività di accesso ai sistemi informatici/telematici e applicazioni (autenticazione, account e profili);
- attività di manutenzione dei sistemi informatici/telematici e di accesso alle applicazioni;
- gestione della sicurezza della rete;
- gestione degli applicativi software, della rete *internet*, della casella *e-mail* e dei sistemi informativi;
- gestione dei sistemi *hardware* e degli accessi fisici ove risiedono le infrastrutture di *Information Technology*;
- gestione dei database e trattamento dei dati;
- gestione degli incidenti e dei problemi di sicurezza informatica;
- gestione e protezione della postazione di lavoro;
- gestione delle Risorse umane e sicurezza fisica;
- gestione dei *backup*;
- gestione dei rapporti con *outsourcer* e *provider* esterni;
- *scanning* dei documenti degli interlocutori contrattuali ed istituzionali, dei *partners* e dei terzi e gestione della documentazione in formato digitale;
- gestione dei rapporti con il Garante della Privacy;
- gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio;
- esecuzione contrattuale;
- gestione delle chiavi elettroniche;

- accessi alle infrastrutture di *Information Technology* degli interlocutori contrattuali ed istituzionali, dei *partners* e dei terzi.

Regole generali

Principi generali di controllo

I principi generali di controllo relativi alla sicurezza informatica sono i seguenti:

- costante attività di monitoraggio tramite l'utilizzo di adeguate misure per la protezione delle informazioni di tipo tecnologico, organizzativo e infrastrutturale;
- continuità operativa, anche a fronte di situazioni di emergenza;
- 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;
- definizione di livelli autorizzativi nell'ambito delle fasi operative caratteristiche dei processi a protezione della gestione e dell'utilizzo dei sistemi informatici;
- segregazione dei compiti nelle attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del *software*;
- riservatezza, garanzia che un dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati (le informazioni riservate devono essere protette sia nella fase di elaborazione che in quella di conservazione);
- integrità, garanzia che un dato sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato in modo legittimo, lo scopo è quello di evitare intromissioni non legittime;
- disponibilità, garanzia di reperibilità dei dati informatici relativi alle attività della Banca in funzione delle esigenze conoscitive;
- controllo e monitoraggio, per quanto nella sfera di controllo della Banca, della legittimità dell'operato di eventuali fornitori in materia informatica

Principi generali di comportamento

La **Banca**, e in particolare tutte le relative strutture interne a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e dei dati ivi contenuti, sono tenute ad osservare le modalità esposte nei protocolli applicabili, e in ogni caso a rispettare i seguenti principi:

- predisporre e mantenere, tramite apposito incarico, 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;
- ogni dipendente/amministratore del sistema è tenuto alla pronta segnalazione alle competenti Funzioni aziendali di eventuali incidenti di sicurezza, mettendo a disposizione e archiviando tutta la eventuale documentazione relativa all'incidente;
- ogni dipendente è responsabile del corretto utilizzo e della conservazione delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere

utilizzate esclusivamente per l'espletamento della propria attività. La Banca dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;

- qualora sia previsto il coinvolgimento di soggetti terzi o dell'Outsourcer nella gestione dei sistemi informatici e dei dati, nonché dell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, nonché nella fornitura di servizi connessi a banche dati o sistemi informatici pubblici o di terzi, 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.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Rischio informatico e Continuità operativa
- Policy di Sicurezza Informatica, in particolare con riferimento ai servizi di pagamento via internet
- Documento di Indirizzo Strategico in materia di Sistemi Informativi
- Business Continuity Management - Gestione della Continuità Operativa
- Norme contrattuali con Outsourcer informatico
- Capitolo S.11.01 - Gestione delle Tecnologie e Sistemi, Applicazioni e attività connesse (con Appendici sulla Sicurezza Informativa)
- Capitolo S.11.03 - Posta Elettronica Certificata e Certificati di Firma Elettronica
- Capitolo B.10.06 - Prevenzione e gestione delle frodi

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Le fattispecie di reato

L'art. 25-*bis* del **Decreto** elenca una serie di reati previsti dal codice penale a tutela della fede pubblica. Le condotte contemplate dal suddetto articolo hanno ad oggetto monete – 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.

Le Aree e le Funzioni principalmente coinvolte da attività a rischio di commissione dei reati contemplati dalla presente **Parte Speciale** sono pertanto l'Area Private Banking, l'Area Business Operations e l'Area Amministrazione e Controllo.

Di seguito si illustrano le fattispecie rilevanti ai fini della presente **Parte Speciale**:

Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.) **e spendita di monete falsificate ricevute in buona fede** (art. 457 c.p.)

La fattispecie prevista dall'art. 455 c.p. presuppone la consapevolezza o il sospetto *ab origine*, nel soggetto che pone in essere la condotta di spendita o introduzione, della non autenticità delle monete, ancorché in assenza di accordi 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 spende o introduce moneta falsa. La buona fede viene tuttavia meno soltanto al momento della spendita o, più in generale, della messa in circolazione della moneta contraffatta o alterata. Potrebbe dunque rispondere del reato in oggetto l'operatore bancario che utilizzi per operazioni di sportello banconote contraffatte, anche se ricevute in buona fede, al fine di evitare di causare pregiudizio alla banca o di dover procedere denuncia della falsità.

I processi e le attività sensibili

La principale attività sensibile svolta dalla **Banca** è la gestione dell'operatività di cassa e dei valori in generale e tutti i relativi processi.

Regole generali

Principi generali di controllo

Il sistema di controllo a presidio dell'area di attività sensibile descritta deve basarsi sui seguenti principi:

- segregazione dei compiti tra i differenti soggetti coinvolti nel processo;
- definizione dei livelli autorizzativi, in particolare in relazione all'individuazione e all'autorizzazione dei soggetti che intervengono nel processo di movimentazione di valori, anche mediante assegnazione individuale di dispositivi atti alla movimentazione e/o alla

custodia dei valori stessi, con evidenza di tali assegnazioni nelle specifiche procedure gestionali;

- definizione delle attività di controllo interno a cura di ciascuna struttura coinvolta nello svolgimento delle attività di gestione dei valori, in particolare dal punto di vista contabile e di giacenza reale dei valori in cassa, raccolta dei valori tramite intermediari, gestione delle apparecchiature ATM/Mercato Telematico Azionario.

Principi generali di comportamento

Le aree e le strutture della **Banca** coinvolte nella gestione dei valori sono tenute ad osservare le modalità esposte negli appositi protocolli e procedure, nonché le disposizioni di legge esistenti in materia. 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 nelle specifiche procedure gestionali;
- sono tenuti ad operare con onestà, integrità, correttezza e buona fede;
- sono tenuti ad operare con prudenza in caso di rapporti 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, anche attraverso l'utilizzo di apparecchiature di selezione e accettazione delle banconote atte a verificarne sia l'autenticità sia l'idoneità alla circolazione;
- sono tenuti, in presenza di banconote sospette di falsità, a predisporre tempestivamente un verbale di ritiro delle banconote sospette di falsità e a farne segnalazione alle competenti Autorità (CNA/Centro Nazionale di Analisi di 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 mezzi forti nel periodo intercorrente tra la data di accertamento/ritiro del valore a quella di inoltro alla Banca d'Italia;
- segnalare immediatamente 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, con le modalità ed entro i termini prescritti dalla normativa interna.

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.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano configurare le fattispecie di reato considerate nella presente **Parte Speciale**, e in particolare, a titolo meramente esemplificativo, di:

- mettere in circolazione, in concorso o meno con terzi, valori falsi, ancorché ricevuti in buona fede. In caso di dubbi sulla legittimità, il soggetto che riceva moneta sospetta di falsità non deve tentare a sua volta di metterla nuovamente in circolazione, né restituirla all'esibitore, né 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.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Capitolo B.02.01 - Operatività di cassa (in contanti o con assegni)
- Capitolo S.04.01 – Antiriciclaggio e antiterrorismo
- Capitolo S.08.09 - Altre attività contabili e amministrative (gestione piccola cassa)

Reati societari

Le fattispecie di reato

L'art. 25-*ter* del **D.Lgs. n.231/2001** individua specifiche ipotesi di reato in materia societaria, la cui commissione è suscettibile di arrecare un beneficio alla **Banca** ed espone quest'ultima a responsabilità amministrativa.

Il suddetto articolo compendia quasi tutti i reati societari previsti dal Titolo XI del codice civile, applicabili in quanto reati generali, non specificamente riferibili all'esercizio dell'attività bancaria. I reati societari oggetto della presente **Parte Speciale** hanno ad oggetto differenti ambiti e sono accomunati dalla finalità di tutelare la trasparenza dei documenti contabili.

La presente **Parte Speciale** si applica, quindi, a tutti i soggetti e a tutte le Funzioni coinvolte in tali ambiti, quali:

- Soci;
- Amministratori;
- Amministratore Delegato;
- Membri del Collegio Sindacale;
- Direttore Generale;
- Dirigente Preposto;
- Vice Direttori Generali;
- Liquidatori;
- Funzione Contabilità Generale;
- Funzione Bilancio e Fiscale;
- Funzione Crediti;
- Funzione Segnalazioni di Vigilanza;
- Funzione Pianificazione e Controllo;
- Funzione Risk Management;
- Funzione Comunicazione;
- Funzione Sviluppo Prodotti e Iniziative Commerciali;
- Funzione Legale e Societario;
- Comitato Crediti;
- Area Finanza;
- Area Private Banking;
- Area Private Offering & Alternative Investments;
- Area Investment Banking e Strategic Equity;

- Ogni altra Funzione coinvolta nella predisposizione, elaborazione dei documenti contabili;
- Qualsiasi soggetto riconducibile alla Banca, sottoposto alla direzione e vigilanza dei soggetti sopra elencati, in particolar modo appartenente alle Funzioni di business;
- Coloro che svolgono attività lavorativa nella Banca con l'esercizio di funzioni direttive;
- Ogni Funzione coinvolta di volta in volta nella trasmissione di comunicazioni e informazioni alle Autorità.

Si riporta di seguito una breve descrizione dei reati in esame.

False comunicazioni sociali delle società quotate (art. 2622 c.c.)

La consumazione di questo reato avviene qualora gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato, al fine di conseguire per sé o per altri un ingiusto profitto, espongano consapevolmente nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali rilevanti non rispondenti al vero ovvero omettano fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Banca o del gruppo al quale essa appartiene, in modo concretamente idoneo ad indurre altri in errore.

La responsabilità è ravvisabile altresì nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla Banca per conto di terzi.

Per società quotate si intendono quelle società che emettano finanziari in un mercato regolamentato italiano o di altro Paese dell'Unione Europea, dalle loro società controllanti, da quelle richiedenti l'ammissione alla negoziazione in tali mercati ovvero da società che facciano appello al pubblico risparmio o comunque lo gestiscano.

Impedito controllo (art. 2625 c.c.)

Il reato si configura quando si ostacoli o si impedisca lo svolgimento delle attività di controllo, legalmente attribuite ai soci o ad altri organi sociali. Tale condotta può essere integrata dall'occultamento di documenti o l'utilizzo di altri artifici. Soggetti attivi del reato sono gli amministratori.

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

Il reato si configura qualora si proceda, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione anche simulata, dei conferimenti ai soci, o alla liberazione degli stessi dall'obbligo di eseguirli. Soggetti attivi del reato sono gli amministratori, anche se i soci beneficiari della restituzione possono concorrere al reato.

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

La condotta in esame si realizza qualora si ripartiscano utili o acconti sugli utili non effettivamente conseguito o destinati per legge a riserva, ovvero si ripartiscano riserve, anche non costituite con

utili, che non possono essere distribuite per legge. Soggetti attivi del reato sono gli amministratori. I soci beneficiari possono concorrere al reato.

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

Il reato si configura qualora si proceda all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società o della controllante, in modo da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Soggetti attivi del reato sono gli amministratori.

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

Il reato si configura quando siano realizzate riduzioni di capitale sociale, fusioni con altre società o scissioni, in violazione delle disposizioni di legge o che cagionino un danno ai creditori. Soggetti attivi sono gli amministratori.

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

L'amministratore o il componente del Consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58 e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209 o del decreto legislativo 21 aprile 1993, n. 124 che viola gli obblighi previsti dall'articolo 2391, primo comma, (obblighi di comunicare agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; se si tratta di 'Amministratore Delegato, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale, se si tratta di amministratore unico, deve darne notizia anche alla prima 'Assemblea utile) "*è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi*".

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

Tale ipotesi di reato si realizza quando viene formato o aumentato in modo fittizio il capitale della società mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti di beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione. Soggetti attivi sono gli amministratori e i soci conferenti.

Corruzione tra privati (art. 2635 c.c.)

Tale ipotesi di reato è realizzabile da parte di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori, che, anche per interposta persona, o da soggetti sottoposti alla loro direzione e vigilanza, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà (corruzione passiva).

È altresì realizzabile in forma attiva, ossia qualora sia connesso alla dazione o alla promessa di denaro o di altra utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o soggetti sottoposti alla loro direzione e vigilanza qualora sia idonea a determinare il soggetto attivo a porre in essere la condotta di corruzione passiva (corruzione attiva).

Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.)

Tale reato è configurabile nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti, i sindaci e i liquidatori, nonché coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

Illecita influenza sull'Assemblea (art. 2636 c.c.)

Il reato si configura qualora, con atti simulati o frode, si determina la maggioranza in Assemblea, allo scopo di conseguire per sé o per altri un ingiusto profitto. Il reato in esame può essere commesso da chiunque, anche da soggetti esterni alla società.

Aggiotaggio (art. 2637 c.c.)

Il reato si configura qualora si proceda alla diffusione di notizie false ovvero alla realizzazione di operazioni simulate o ad altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo degli strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ovvero a incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Il reato si configura mediante la realizzazione di due tipologie di condotta finalizzate a ostacolare l'attività di vigilanza delle autorità pubbliche preposte nei confronti delle società che alle stesse sono sottoposte: attraverso la comunicazione alle autorità pubbliche di vigilanza di fatti non veritieri relativi alla situazione economica, finanziaria e patrimoniale della società, ovvero con l'occultamento di fatti che avrebbero dovuto essere comunicati; attraverso l'ostacolo all'esercizio delle funzioni di vigilanza svolte da pubbliche autorità, attuato consapevolmente e in qualsiasi modo, anche omettendo le comunicazioni dovute alle autorità medesime. Soggetti attivi sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

False o omesse dichiarazioni per il rilascio del certificato preliminare per le trasformazioni, le fusioni e le scissioni transfrontaliere (art. 54 D.Lgs. 19/2023)

Il reato si configura nell'ipotesi in cui al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare da parte del notaio, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti.

I processi e le attività sensibili

L'analisi dei processi posti in essere dalla Banca ha permesso l'individuazione delle seguenti attività nel cui ambito potrebbero realizzarsi le fattispecie di reato esaminate in questa sede:

- tenuta della contabilità;
- predisposizione della situazione contabile annuale e infra-annuale;
- tutti processi inerenti all'individuazione e la gestione dei conflitti di interesse degli Amministratori;
- selezione dei Fornitori/dei Consulenti;
- prestazione servizi di investimento, attività bancaria o altri servizi alla Clientela;
- tutti i processi che possono riguardare un atto o un'attività mirati ad influenzare artificiosamente le decisioni assembleari;
- tutti i processi relativi alla gestione delle informazioni "*price sensitive*" relative a strumenti finanziari non quotati e finalizzati ad evitarne la diffusione e/o l'utilizzo per operazioni di investimento e disinvestimento;
- gestione dei rapporti con le Autorità di Vigilanza.

Regole generali

Principi generali di controllo

I principi generali di controllo, alla base degli strumenti e delle metodologie utilizzate per definire le procedure specifiche di controllo, sono i seguenti:

- separazione delle attività, tra chi autorizza, chi esegue e chi controlla;
- esistenza di procedure, norme e circolari formalizzate allo scopo di fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili, nonché di identificare le modalità di archiviazione della documentazione rilevante;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate, nonché chiaramente definiti e diffusi all'interno della **Banca**;
- tracciabilità di ogni operazione relativa a ciascuna attività sensibile individuata, mediante idonea registrazione di ogni fatto aziendale compiuto. In tal modo è possibile verificare a posteriori il processo di decisione, autorizzazione e svolgimento delle attività sensibili in esame.

Principi generali di comportamento

I principi generali identificati sono i seguenti:

- nei bilanci e nelle altre comunicazioni sociali dirette ai soci o al pubblico, è vietato:
  - esporre fatti materiali non rispondenti al vero;

- porre in essere attività e/o operazioni volte a creare disponibilità extra-contabili (ad esempio, ricorrendo a fatture per operazioni inesistenti o alla sovra-fatturazione), ovvero volte a creare "fondi neri" o "contabilità parallele";
- omettere informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della **Banca**.

- nei rapporti con i Soci, la società di revisione e gli altri Organi Sociali è fatto divieto:
  - occultare documenti;
  - rifiutare di fornire informazioni o documentazione richieste;
  - produrre documentazione falsa o attestante cose non vere;
  - omettere la comunicazione di fatti e informazioni rilevanti;
  - ostacolare l'accesso ad archivi/database (sia cartacei che informatici) e alle informazioni ivi contenute;
  - impedire o comunque ostacolare lo svolgimento delle attività di controllo o di revisione;
- in merito alle operazioni relative al capitale, è vietato:
  - restituire, anche simulatamente, i conferimenti ai soci o liberarli dall'obbligo di eseguirli, fatte salve ovviamente le ipotesi di legittima riduzione del capitale sociale;
  - ripartire utili o acconti su 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;
  - acquistare o sottoscrivere azioni sociali o della società controllante al di fuori dei casi consentiti dalla legge, con ciò cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;
  - effettuare riduzioni del capitale sociale o fusioni con altre società o scissioni in violazione delle norme di legge, con ciò cagionando un danno ai creditori;
  - formare o aumentare fittiziamente il capitale sociale mediante attribuzioni di azioni per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio sociale in caso di trasformazione;
- nell'ambito delle attività di acquisto di beni o di servizi, è fatto divieto agli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, e ai soggetti sottoposti alla loro direzione e vigilanza, di compiere od omettere atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società a seguito della dazione o promessa di denaro o altra utilità per sé o per altri;
- nell'ambito di attività di fornitura di servizi ad imprese, è vietata la dazione o la promessa di denaro o altra utilità agli esponenti delle stesse al fine di determinare questi soggetti a porre in essere od omettere atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà;

- è vietato determinare o influenzare illecitamente l'assunzione delle delibere Assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà Assembleare;
- nei rapporti con la Pubblica Vigilanza è fatto divieto di:
  - esporre fatti materiali non rispondenti al vero ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza;
  - occultare, con altri mezzi fraudolenti, in tutto o in parte, fatti che avrebbero dovuto comunicare concernenti la situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza;
  - occultare documenti;
  - porre in essere comportamenti ostruzionistici o di mancata collaborazione;
  - rifiutare di fornire informazioni o documentazione richieste;
  - produrre documentazione falsa o attestante cose non vere;
  - omettere la comunicazione di fatti e informazioni rilevanti;
  - impedire o comunque ostacolare lo svolgimento delle attività di controllo, anche in sede di ispezione;
- alle eventuali ispezioni, perquisizione o comunque agli accessi condotti dalla Autorità pubbliche di Vigilanza presso la sede della banca, devono intervenire i soggetti aziendali a ciò espressamente delegati; ogni incontro deve essere debitamente documentato e deve avvenire alla presenza di almeno due rappresentanti della **Banca**, salvo casi di forza maggiore. In particolare, devono essere presenti almeno due persone, ovvero il Responsabile di Funzione accompagnato dalla Direzione e/o da uno dei più stretti Collaboratori;
- in caso di visite ispettive, deve essere garantita la massima collaborazione di tutte le Funzioni interessate con l'individuazione di un referente, affinché sia garantita la più ampia e tempestiva collaborazione a dette Autorità, fornendo dati e documenti richiesti in modo tempestivo e completo; copia dei verbali redatti in sede di ispezione, perquisizione o accesso devono essere trasmessi all'Amministratore Delegato e Direttore Generale.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Statuto
- Regolamento del Consiglio di Amministrazione e dei Comitati
- Regolamento della Funzione Internal Audit

- Regolamento della Funzione Compliance
- Regolamento Antiriciclaggio
- Regolamento ICAAP
- Strategia di classificazione della Clientela
- Politica di Remunerazione e Incentivazione del Personale
- Capitolo S.02.01 - Gestione comunicazioni periodiche
- Capitolo S.02.02 - Gestione di comunicazioni e di richieste di dati e di informazioni
- Capitolo S.02.03 - Segnalazioni di vigilanza
- Capitolo S.03.01 - Monitoraggio dei rischi
- Capitolo S.04.01 - Antiriciclaggio e antiterrorismo
- Capitolo S.04.03 - Gestione operazioni con Parti Correlate o con potenziale interesse degli Amministratori
- Capitolo S.04.08 - Market Abuse
- Capitolo S.06.01 - Gestione delle attività societarie
- Capitolo S.07.02 - Gestione attività di comunicazione ed eventi
- Capitolo S.08.02 - Attività contabili mensili
- Capitolo S.08.03 - Bilancio d'esercizio e situazioni finanziarie periodiche
- Capitolo S.08.04 - Bilancio Consolidato e situazioni finanziarie periodiche
- Capitolo S.08.05 - Dirigente preposto alla Redazione dei documenti contabili societari
- Capitolo S.08.06 - Redazione delle situazioni finanziarie annuali e infra-annuali
- Capitolo S.08.07 - Fornitori e fatturazione
- Capitolo S.09.01 - Selezione, assunzione, trasferimento e cessazione del Personale
- Capitolo S.13.01 - Gestione acquisti e servizi logistici/ausiliari
- Capitolo B.01.01 - Apertura rapporti della Clientela Private Banking (gestione deroghe)
- Capitolo B.01.03 - Gestione rapporti della Clientela Finanza
- Capitolo B.03.01 - Esecuzione, Ricezione e trasmissione, Negoziazione in conto proprio (Intermediazione mobiliare) – Gestione ordini
- Capitolo B.03.02 - Collocamento – Offerta di OICR
- Capitolo B.03.03 - Collocamento – Offerte Pubbliche (OPV, OPS, OPA)
- Capitolo B.03.04 - Gestione individuale di portafogli
- Capitolo B. 03.05 - Consulenza in materia di investimenti
- Capitolo B.03.08 - Intermediazione assicurativa
- Capitolo B.04.02 - Acquisto e vendita delle azioni di Banca Profilo

- Capitolo B.09.01- Investment Banking e Strategic Equity - Gestione delle attività di Business dell'Area
- Capitolo B.10.01 - Gestione delle attività di onboarding
- Capitolo B.10.02 - Movimentazione e gestione account
- Capitolo B.10.03 - Carte Prepagate
- Capitolo B.10.05 - Clientela Corporate

I delitti contro la persona

Le fattispecie di reato

L'art. 25-*quinquies* del **D.Lgs. n.231/2001** individua specifiche ipotesi di reato in materia di reati contro la personalità individuale, la cui commissione espone la Banca a responsabilità amministrativa.

A livello interno, la presente **Parte Speciale** si applica, quindi, alle strutture principalmente coinvolte nei processi di selezione del personale, quali la Funzione Risorse Umane e Welfare Aziendale.

Si riporta di seguito una breve descrizione del reato rilevante in esame.

Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.)

Si tratta di un reato connesso:

- al reclutamento di manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
- all'utilizzo, l'assunzione o l'impiego di manodopera, anche mediante l'attività di intermediazione di cui al punto precedente, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

I processi e le attività sensibili

In particolare, per la **Banca** l'attenzione è stata rivolta soprattutto ai processi di selezione, assunzione e gestione delle risorse umane, nonché del personale utilizzato dai fornitori.

Regole generali

Principi generali di controllo e comportamento

Tutte le attività sensibili devono essere svolte conformemente alle disposizioni normative e regolamentari, ai principi generali di comportamento enucleati nella **Parte Generale** del presente **Modello**, alle norme del Carta dei principi e codice di comportamento, nonché alle procedure a presidio dei rischi reato individuati.

I Destinatari della presente **Parte Speciale** devono:

- accertarsi che i fornitori utilizzino manodopera in conformità con la normativa vigente in materia previdenziale anche attraverso la verifica del DURC e delle certificazioni di cui sono in possesso;
- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dalle autorità di pubblica sicurezza;

- in generale, mantenere nei confronti delle autorità di pubblica sicurezza un comportamento corretto, cordiale e disponibile in qualsiasi situazione.

È fatto inoltre divieto, a titolo esemplificativo, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare, individualmente o collettivamente, direttamente o indirettamente, le fattispecie di reato previste dall'articolo 25-*quinquies* del **Decreto**;
- sottoporre i lavoratori a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
- violare la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria e alle ferie;
- corrispondere retribuzioni in difformità dai contratti collettivi nazionali o territoriali;
- violare i principi enunciati nella Carta dei principi e codice di comportamento e nelle procedure operative richiamate dalla presente **Parte Speciale**;
- utilizzare anche occasionalmente la **Banca** o gli spazi fisici della stessa allo scopo di consentire o agevolare la commissione dei reati di cui all'art. 25-*quinquies* del **Decreto**.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Capitolo S.09.01 - Selezione, assunzione, trasferimento e cessazione del Personale
- Capitolo S.13.01 - Gestione acquisti e servizi logistici/ausiliari

I reati e gli illeciti amministrativi riconducibili ad abusi di mercato

Le fattispecie di reato

L'art. 25-*sexies* del **Decreto** individua specifiche ipotesi di reato in materia di abusi di mercato, la cui commissione è suscettibile di arrecare un beneficio alla **Banca** ed implicarne perciò la responsabilità.

Tali fattispecie sono previste in particolare dal T.U.F., che prevede due fattispecie di reato (artt. 184 e 185) ed illeciti amministrativi (artt. 187-*bis* e 187-*ter*). Mentre la responsabilità dell'ente per la commissione dei reati è sancita dall'art. 25-*sexies* del **Decreto**, è la disciplina del T.U.F. a prevedere direttamente una responsabilità amministrativa in capo all'ente per le fattispecie di illeciti ammnistrativi, secondo i medesimi principi, condizioni ed esenzioni del Decreto, salvo stabilire che per tali illeciti amministrativi la responsabilità dell'Ente sussiste in ogni caso in cui lo stesso non riesca a fornire la prova che l'autore dell'illecito ha agito esclusivamente nell'interesse proprio o di un terzo.

Le regole per l'attuazione dei principi stabiliti dal T.U.F. e per la repressione delle sue violazioni sono stabilite dalla legislazione dell'Unione europea, in particolare dalla Direttiva 2014/57/UE (c.d. MAD II) e dal Regolamento (UE) n. 596/2014 (c.d. MAR), e dall'ordinamento italiano con il D. Lgs. n. 107/2018, che ha riformulato anche le disposizioni sanzionatorie del T.U.F. di cui sopra.

I soggetti e le aree maggiormente coinvolti nei processi di cui alla presente **Parte Speciale** sono i seguenti:

- chiunque sia in possesso di informazioni privilegiate in ragione (**i**) della sua qualità di Amministratore Delegato, membro del Consiglio di Amministrazione, o del Collegio Sindacale, (**ii**) della partecipazione al capitale dell'emittente, ovvero (**iii**) dell'esercizio dell'attività lavorativa presso l'emittente;
- Funzione Compliance e Antiriciclaggio;
- Area IT for Business;
- Area Finanza;
- Area Investment Banking e Strategic Equity;
- Area Private Banking;
- Funzione Investment Advisory;
- Amministratore Delegato e membri del Consiglio di Amministrazione;
- Investor Relator.
- .

Si riporta di seguito una breve descrizione delle fattispecie sopra menzionate.

Abuso di informazioni privilegiate (art. 184 T.U.F.)

Tale reato punisce chi abusa direttamente o indirettamente di informazioni privilegiate di cui sia venuto in possesso (**i**) per la sua qualità di membro degli organi di amministrazione, direzione o

controllo dell'emittente; (**ii**) perché partecipa al capitale dell'emittente; (**iii**) in ragione dell'esercizio di un'attività lavorativa, professionale o di una funzione o di un ufficio; (**iv**) in conseguenza della preparazione o commissione di un reato (come ad esempio l'intrusione in un sistema informatico ed estrazione di informazioni privilegiate).

Per informazione privilegiata si intende un'informazione avente un "*carattere preciso, che non è stata resa pubblica*[4]*, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati*"[5].

Manipolazione di mercato (art. 185 T.U.F.)

Il reato di manipolazione di mercato viene integrato qualora un soggetto diffonda notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari. Non è punibile la condotta costituita da ordini di compravendita o da altre operazioni che, pur potendo dare al mercato segnali fuorvianti o fissare artificialmente il prezzo, sia giustificata da motivi legittimi e sia stata tenuta in conformità a una prassi di mercato ammessa dall'Autorità competente del mercato di riferimento, ai sensi dell'art. 13 del MAR.

Sanzioni amministrative: abuso e comunicazione illecita di informazioni privilegiate e manipolazione del mercato (art. 187-*bis* e art. 187-*ter* T.U.F.)

Come illustrato sopra, sono previste specifiche sanzioni amministrative mirate a condotte nella sostanza corrispondenti a quelle che formano oggetto delle fattispecie penali (artt. 184 e 185 T.U.F.). Gli illeciti amministrativi di cui all'art. 187-*bis* e all'art. 187-*ter* del T.U.F., infatti, anziché descrivere la condotta vietata, rinviano semplicemente ai divieti di abuso e comunicazione illecita di informazioni privilegiate e di manipolazione del mercato, come definiti dagli articoli 14 e 15 del MAR. Il richiamo alle definizioni delle fattispecie contenute nella normativa europea comporta un generale rinvio anche alle altre disposizioni del MAR che definiscono le nozioni di abuso, di comunicazione illecita e di manipolazione e che costituiscono la fonte di riferimento anche per le sopra illustrate fattispecie penali, benché le medesime non ne facciano espresso integrale richiamo.

Le fattispecie di illecito amministrativo, la cui applicazione è di competenza della Consob, potrebbero pertanto colpire una più ampia gamma di condotte, nella misura in cui siano ritenuti rilevanti elementi e modalità ripresi tramite il riferimento diretto agli artt. 14 e 15 del MAR che non lo siano invece per le condotte penali, che sono state descritte senza fare rinvio espresso al MAR se non per aspetti circoscritti.

[4] l'art. 17 del MAR prevede i casi, i tempi e le modalità dell'obbligo di comunicazione al pubblico delle informazioni privilegiate da parte degli emittenti strumenti finanziari o dei partecipanti al mercato delle quote di emissioni di gas a effetto serra;

[5] la definizione di informazione privilegiata è stabilita dall'art. 180, comma 1, lettera b-*ter*, del T.U.F., mediante rinvio all'art. 7, paragrafi da 1 a 4 del MAR.

I processi e le attività sensibili

L'analisi dei processi posti in essere dalla **Banca** ha condotto all'individuazione delle seguenti attività nel cui ambito potrebbero realizzarsi le fattispecie di reato esaminate in questa sede:

- i processi relativi alla gestione delle informazioni privilegiate "*price sensitive*" al fine di evitarne la diffusione e/o l'utilizzo per operazioni di investimento e disinvestimento in strumenti finanziari quotati o quotandi;
- i processi che riguardano la prevenzione degli abusi di mercato nonché la comunicazione al pubblico delle informazioni privilegiate.

Regole generali

Principi generali di controllo

I principi su cui deve essere improntato il controllo delle aree sensibili sopra identificate sono i seguenti:

- segregazione dei compiti;
- attività di controllo da parte di ciascuna area competente, in particolare controlli di completezza, correttezza ed accuratezza delle informazioni riportate sui documenti di specifica competenza, e controlli di carattere giuridico sulla conformità alla normativa di riferimento;
- tracciabilità del processo, sia a livello di sistema informativo, sia in termini documentali.

Principi generali di comportamento

I principi di comportamento identificati sono espressi in termini di divieto di:

- alterare con il proprio comportamento la corretta formazione dei prezzi degli strumenti finanziari, in particolare di porre in essere operazioni simulate ovvero altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o non quotati;
- diffondere come certe notizie false o ritenute non affidabili, incomplete o erronee;
- qualificare come "notizie" le voci, i c.d. "*rumor*", le semplici previsioni o altre informazioni che non siano notizie;
- percepire dagli emittenti terzi, direttamente o indirettamente, somme di denaro, benefici, compensi o favori di varia natura, in particolare qualora i medesimi siano finalizzati ad ottenere vantaggi impropri o ad indurre i destinatari del presente **Modello** a tenere comportamenti comunque in contrasto con gli interessi degli investitori o dei soggetti per i quali operano.

Gli addetti delle Funzioni interessate devono astenersi da:

- utilizzare (i.e. ordini effettuati non ancora eseguiti), comunicare o diffondere (anche mediante attività di "consulenza", ad es. raccomandando determinate operazioni) informazioni privilegiate sia all'interno della struttura della **Banca**, che all'esterno;

- utilizzare, negli eventuali propri colloqui con i Clienti, termini o espressioni consapevolmente iperboliche, suggestive o denigratorie allo scopo di trarre in inganno il Cliente;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa e dalle procedure aziendali) e se tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;
- vendere la totalità o la quasi totalità degli strumenti finanziari presenti nel portafoglio per investire la liquidità ricavata su uno specifico strumento finanziario, a meno che tale operazione non risulti specificamente approvata dai competenti Organi aziendali e sulla base delle deleghe interne conferite;
- richiedere l'immediata esecuzione di un ordine senza indicazioni di prezzo;
- utilizzare acriticamente gli input informativi ricevuti dalle società emittenti, bensì effettuare tutte le verifiche necessarie o opportune che siano consentite in base ai ruoli ricoperti nell'ambito dell'operazione.

In relazione alle operazioni di collocamento, gli addetti delle strutture interessate:

- garantiscono, nel corso delle operazioni di collocamento, la assoluta riservatezza sulle operazioni oggetto di mandato, in particolar modo nei confronti degli addetti alla negoziazione;
- con riferimento alle operazioni alle quali la **Banca** partecipi con ruoli di Responsabile del collocamento o partecipi a consorzi di collocamento, predispongono e comunicano con la massima cautela alle funzioni competenti tutte le informazioni eventualmente necessarie ai fini di pervenire alla definizione dell'intervallo di prezzo, nonché di preparare eventuali analisi a supporto delle operazioni oggetto del mandato;
- non si limitano ad utilizzare acriticamente gli input informativi ricevuti dalle società emittenti, bensì effettuare tutte le verifiche necessarie o opportune che siano consentite in base ai ruoli ricoperti nell'ambito dell'operazione.

Presso l'Area Finanza è mantenuta una costante e necessaria presenza fisica dei Responsabili delle Funzioni Intermediazione e Mercati Azionari (con particolare riferimento al Desk Equity) durante tutto il periodo di apertura dei mercati, al fine di permettere che gli stessi possano monitorare l'operatività degli addetti.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Regolamento Aziendale
- Regolamento Area Finanza
- Regolamento per l'assunzione dei rischi di credito

- Capitolo S.03.01 – Monitoraggio dei rischi
- Capitolo S.04.03 - Gestione operazioni con Parti Correlate o con potenziale interesse degli Amministratori
- Capitolo S.04.08 – Market Abuse
- Capitolo S.08.03 - Bilancio d'esercizio e situazioni finanziarie periodiche
- Capitolo S.08.04 - Bilancio Consolidato e situazioni finanziarie periodiche
- Capitolo S.08.06 – Redazione delle situazioni finanziarie annuali e infra-annuali
- Capitolo B.03.01 – Esecuzione, Ricezione e trasmissione, Negoziazione in conto proprio (Intermediazione mobiliare) – Gestione ordini
- Capitolo B.03.02 – Collocamento – Offerta di OICR
- Capitolo B.03.03 – Collocamento – Offerte Pubbliche (OPV, OPS, OPA)
- Capitolo B.04.01 – Operatività della Proprietà
- Capitolo B.05.03 - Operatività di mercato aperto
- Capitolo B.06.02 - Operations Post trade

I reati di omicidio colposo o lesioni gravi/gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Le fattispecie di reato

La Legge 3 agosto 2007 n. 123, all'art. 9, ha introdotto nel **D.Lgs. n.231/2001** l'articolo 25-*septies* in forza del quale l'ente è responsabile per le ipotesi di omicidio colposo (art. 589 c.p.) e di lesioni colpose gravi o gravissime (art. 590 c.p.), laddove i suddetti reati siano commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro la cui disciplina è contenuta nel relativo Testo Unico, D.Lgs. n. 81/2008.

Ai sensi del predetto art. 25-*septies* del Decreto, le condotte di seguito descritte devono dunque 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 di cui al Testo Unico.

A completamento del corpo normativo così delineato, 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.

I soggetti e le aree maggiormente coinvolti nei processi di cui alla presente **Parte Speciale** sono i seguenti:

- Datore di Lavoro;
- Dirigente delegato alla sicurezza;
- Outsourcer per la sicurezza.

In generale, tuttavia, tutte le Funzioni possono essere coinvolte.

Si riporta di seguito una breve descrizione dei due reati richiamati:

Omicidio colposo (art. 589 c.p.)

Il reato in oggetto si configura nel caso in cui si cagioni, per colpa, la morte di una persona. Ai fini della commissione del reato in esame non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, imprudenza o imperizia del soggetto agente, ovvero l'inosservanza, da parte di quest'ultimo, di leggi, regolamenti, ordini o discipline.

Lesioni personali colpose (art. 590 c.p.)

Il reato si configura nel caso in cui si cagionino a una persona lesioni gravi o gravissime. Le lesioni si considerano gravi nel caso in cui:

a. dal fatto deriva una malattia che mette in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo

superiore ai quaranta giorni;

b. il fatto produce l'indebolimento permanente di un senso o di un organo.

Le lesioni personali si considerano gravissime se dal fatto deriva:

a. una malattia certamente o probabilmente insanabile;

b. la perdita di un senso;

c. la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

d. la deformazione, ovvero lo sfregio permanente del viso. Anche ai fini della configurabilità del reato in esame, non è necessario che il soggetto agente abbia agito con coscienza e volontà di cagionare l'evento lesivo, essendo sufficiente la mera negligenza, imprudenza o imperizia dello stesso, ovvero l'inosservanza di leggi, regolamenti, ordini o discipline.

I processi e le attività sensibili

In relazione all'attività specifica della **Banca**, e al fine di prevenire i reati di cui alla presente **Parte Speciale**, sono state identificate le seguenti aree sensibili:

- utilizzo e manutenzione di attrezzature e *devices* informatici in uso alla Banca (*computer*, stampanti, ecc.);
- utilizzo, manutenzione e gestione dei locali presenti presso le sedi ove si svolgono le attività;
- sorveglianza sanitaria (gestione delle attività dirette a garantire l'effettuazione della sorveglianza sanitaria previste per ogni categoria lavorativa);
- formazione del personale generale e specifica;
- affidamento di lavori a Soggetti Esterni e svolgimento delle relative attività;
- gestione delle emergenze;
- espletamento delle attività lavorative anche amministrative;
- misure di protezione collettiva e/o individuale atte a contenere o eliminare i rischi;
- coinvolgimento del personale e mantenimento delle misure di protezione implementate e nelle segnalazioni di eventuali anomalie.

Regole generali

Principi generali di controllo

In materia di salute e sicurezza sul lavoro, la **Banca** si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente, nell'ottica di eliminare, ridurre e gestire i rischi per i dipendenti aziendali.

Nell'ambito di tale struttura organizzativa operano i soggetti di seguito indicati.

- **Datore di lavoro** (DdL)

  Conformemente a quanto stabilito nell'art. 2 del D.Lgs. 81/2008, il DdL rappresenta il soggetto all'apice della struttura organizzativa aziendale, responsabile dell'organizzazione nel cui ambito i lavoratori prestano la propria attività, poiché esercita i poteri decisionali e di spesa. All'interno della Banca, il ruolo di DdL è stato affidato all'Amministratore Delegato.

- **Responsabile dei servizi di prevenzione e protezione** (RSPP)

  Figura nominata dal Datore di lavoro ed in possesso dei requisiti previsti dalla normativa vigente. Collabora con il datore di lavoro e con gli addetti interni al Servizio di Prevenzione e Protezione nell'individuazione e nella valutazione dei rischi per la sicurezza, e nell'individuazione delle misure preventive di sicurezza e per la salubrità degli ambienti di lavoro; elabora le procedure di sicurezza per le attività aziendali in collaborazione con il Referente per il sistema integrato qualità, ambiente e sicurezza. L'RSPP concorre a proporre programmi di formazione e informazione per i lavoratori e partecipa ad eventuali consultazioni in materia di tutela della salute e sicurezza, provvedendo inoltre a fornire ai lavoratori le informazioni previste per legge.

- **Rappresentante dei Lavoratori per la Sicurezza** (RLS)

  Eletto dai lavoratori della Divisione nell'ambito delle RSU, riceve una formazione adeguata allo svolgimento delle proprie funzioni ed un aggiornamento periodico secondo quanto definito dalla legislazione vigente. Il nominativo del RLS viene comunicato dall'azienda all'INAIL.

  Il rappresentante dei lavoratori per la sicurezza promuove l'identificazione e l'attuazione delle misure di prevenzione e protezione, partecipa alla riunione annuale per la sicurezza, è consultato in merito alla scelta dei DPI, in merito ai criteri adottati per la valutazione dei rischi ed ai risultati da questa scaturiti, fa proposte circa l'attività di prevenzione e può fare ricorso alle autorità competenti qualora lo ritenga necessario.

- **Medico competente**

  Nominato dal datore di lavoro ed in possesso dei requisiti definiti dalla legislazione vigente, ha la responsabilità di collaborare con il datore di lavoro alla predisposizione dell'attuazione delle misure per la tutela della salute e dell'integrità psico-fisica dei lavoratori. Pertanto, effettua la sorveglianza sanitaria definita, il sopralluogo periodico negli ambienti di lavoro almeno una volta all'anno, esprime i giudizi di idoneità alla mansione, partecipa alla riunione annuale per la sicurezza, aggiorna le cartelle sanitarie di rischio e si rende disponibile a fornire informazioni ai lavoratori in merito alle visite mediche effettuate. È compito del medico competente collaborare nel processo di informazione ai lavoratori e nelle fasi di scelta del personale addetto alle emergenze.

- **Addetti primo soccorso e antincendio**

  Designati dal Datore di Lavoro, si attivano in casi di emergenza di tipo ambientale o di sicurezza, mettendo in atto le procedure di emergenza predisposte. Vengono formati come previsto dalla normativa vigente sulla base del livello di rischio presente in azienda (formazione antincendio e formazione primo soccorso). Le esercitazioni pianificate con una

determinata periodicità costituiscono una formazione periodica per il personale preposto alle emergenze.

- **Lavoratori**

  Tutti i soggetti che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa all'interno della struttura organizzativa della Banca.

Principi generali di comportamento

La **Banca** si impegna, come previsto dalla normativa vigente, a garantire il rispetto della normativa in tema di tutela della salute e sicurezza sul lavoro, nonché ad assicurare un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività lavorativa, attraverso:

- la continua valutazione dei rischi per la sicurezza e la salute, con conseguente adozione e il continuo aggiornamento del Documento di Valutazione dei Rischi (DVR);
- l'eliminazione, oppure laddove non sia possibile, la riduzione dei rischi individuati;
- la definizione di adeguate misure di prevenzione e protezione collettiva e individuale;
- la comunicazione e il coinvolgimento di tutti i lavoratori, nonché dei Soggetti Esterni alla compagine aziendale;
- una adeguata formazione e addestramento di tutti i dipendenti aziendali in funzione dei ruoli, dei compiti e delle responsabilità assegnate;
- la definizione e la più ampia diffusione di idonee misure di gestione delle emergenze;
- la regolare manutenzione di attrezzature e macchinari di qualsiasi tipo utilizzati dai lavoratori nonché dei dispositivi di sicurezza.

L'art. 30 del Testo Unico in materia di sicurezza individua, inoltre, le caratteristiche che deve possedere il **Modello** al fine di avere efficacia esimente con riferimento ai rischi reato esaminati all'interno di questa **Parte Speciale**. In particolare, il **Modello** adottato deve assicurare l'adempimento dei seguenti obblighi giuridici relativi a:

- rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza; attività di sorveglianza sanitaria;
- attività di informazione e formazione dei lavoratori;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documentazioni e certificazioni obbligatorie di legge;
- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Capitolo S.12.01 – Gestione della sicurezza ambientale e fisica
- DPS (documento programmatico per la sicurezza)
- DVR (documento per la valutazione dei rischi)
- DUVRI (documento unico per la valutazione dei rischi da interferenze)
- Procura del Delegato
- Norme contrattuali con Outsourcer

Il riciclaggio e i delitti con finalità di terrorismo

Le fattispecie di reato

Il D.Lgs. 21 novembre 2007, n. 231 (il "**Decreto Antiriciclaggio**") e il D.Lgs. 22.6.2007 n. 109, in attuazione di disposizioni comunitarie, hanno rafforzato la normativa nazionale 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.231/01**, introdotto dal **Decreto Antiriciclaggio**, ha di conseguenza esteso la responsabilità dell'ente ai reati di ricettazione, riciclaggio e impiego illecito anche per le ipotesi in cui non siano commessi con finalità di terrorismo o di eversione dell'ordine democratico – non presentino le caratteristiche di transnazionalità.

Sempre in attuazione di disposizioni internazionali di contrasto a crimini a carattere transnazionale, 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 dalla Convenzione internazionale per la repressione del finanziamento del terrorismo, firmata a New York il 9 dicembre 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.

I soggetti individuati all'interno della compagine aziendale come maggiormente coinvolti in aree potenzialmente a rischio sono:

- Amministratore Delegato
- Direttore Generale
- Vice Direttori Generali
- Area Finanza
- Area Private Banking
- Area Investment Banking e Strategic Equity
- Area Digital
- Area Amministrazione e Controllo
- Funzione Internal Audit
- Funzione Compliance e Antiriciclaggio

Qui di seguito si descrivono i reati rilevanti ai fini della presente **Parte Speciale** di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, cui si riferisce l'art. 25-*octies* del **D.Lgs. n.231/2001**, nonché i reati di associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico, di finanziamento di condotte con finalità di terrorismo, e di sottrazione di beni sequestrati previsti dall'art. 25-*quater* del Decreto.

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 "acquisto" deve intendersi l'effetto di un'attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.

Il termine "ricevere" indica, invece, ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.

Per "occultamento", infine, deve intendersi l'attività posta in essere al fine di celare l'esistenza del bene ricevuto, in quanto proveniente dal delitto.

La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento del bene: la condotta che viene in rilievo va intesa come ogni attività di mediazione tra l'autore del reato principale e il terzo acquirente.

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. È 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 è 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.

Quindi il riciclaggio (*money laundering*) consiste nel rimettere in circolazione nella, per così dire, economia legale, denaro derivante da attività illecite, al fine di dissimularne o occultarne l'origine: la mera ricezione od occultamento potrebbero integrare solamente il reato di ricettazione.

Non è necessario che il soggetto riciclatore conosca quale sia il delitto presupposto, ma è sufficiente che sappia (consapevolezza) che si tratta di proventi illeciti. 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.

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).

Così come per il reato di ricettazione, il reato di riciclaggio non si applica a chi ha commesso il reato presupposto: quindi ad esempio, non è punibile per riciclaggio un soggetto che con denaro frutto di evasione fiscale nella propria società, attiva un conto corrente bancario e poi effettua un'operazione commerciale o finanziaria.

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 illecito, 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 possono dar luogo a proventi oggetto di riciclaggio.

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 c.p. (ricettazione) e 648-*bis* c.p. (riciclaggio).

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.

Il legislatore ha inteso punire anche quelle "attività mediate" che non sostituiscono immediatamente i beni provenienti da alcuni gravi delitti, ma che contribuiscono in ogni caso alla "ripulitura" dei capitali acquisti illecitamente, colpendo in tal modo una serie di attività di investimento apparentemente legali, ma che, in realtà, costituiscono un bacino in cui far confluire il denaro proveniente da attività criminose.

Peraltro, in considerazione dell'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..

Le principali modalità di realizzazione dei reati di ricettazione, riciclaggio o impiego di denaro, beni o utilità di provenienza illecita, anche in concorso con altri soggetti aziendali, sono di seguito riportate a titolo esemplificativo e non esaustivo:

- esecuzione di pagamenti verso fornitori e partner commerciali/finanziari non effettivamente coinvolti nelle transazioni di acquisto e/o vendita;
- stipula di contratti con fornitori e partner commerciali/finanziari senza una accurata verifica dell'attendibilità commerciale e professionale;
- stipula di contratti senza una preventiva definizione da parte di un soggetto responsabile, di clausole *standard*.

Autoriciclaggio (art. 648-*ter*.1 c.p.)

Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che abbia anche 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. Tale ipotesi può configurarsi come reato commesso dall'autore del reato principale che poi, da solo, usa i proventi per investirli o immetterli in attività economiche o finanziarie.

Le astratte modalità di commissione del delitto di autoriciclaggio coincidono con quelle sopra delineate relative alla condotta di riciclaggio, fatta eccezione per la possibilità, in questa fattispecie, che chi se ne rende responsabile ha anche realizzato o concorso a realizzare il reato presupposto.

Pertanto, in caso di reati tributari eventualmente consumati dalla società, o dall'ente in genere, è molto probabile incorrere anche nel nuovo delitto di autoriciclaggio qualora, ad esempio, i proventi derivanti dall'evasione fiscale (o il risparmio di imposta generato da dichiarazioni infedeli) siano impiegati in attività economiche, finanziarie, imprenditoriali o speculative.

Inoltre, l'autore di autoriciclaggio è punibile anche se egli non è imputabile o non è punibile per il reato presupposto o questo non è procedibile per difetto di una condizione di procedibilità.

E da sottolineare come il fatto non è punibile se il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale del reo. Quest'ultima clausola di non punibilità risulta di difficile applicabilità, in quanto, se si ritiene tale utilizzo o godimento riferibile all'ente stesso, la clausola viene a confligge con il requisito fondamentale per l'operatività della responsabilità *ex* **D.Lgs. n.231/2001**, secondo cui l'ente risponde solo se il reato (l'autoriciclaggio) è commesso nel suo "*interesse o vantaggio*" (art. 5, **D.Lgs. n.231/2001**).

Considerato che il reato di autoriciclaggio ha quale momento costitutivo quello della sostituzione, trasferimento in attività economiche, finanziarie, imprenditoriali o speculative, di denaro, beni o le altre utilità, provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa, appare evidente la necessità di attivare un sistema di controllo, per così dire, a monte e a valle. In altre parole, si tratta:

- a monte, di individuare, al momento della provenienza del denaro, beni o altre utilità, se detta provenienza sia legittima o frutto di un reato;
- a valle, di individuare, al momento della sostituzione, trasferimento in attività economiche, finanziarie, imprenditoriali o speculative di denaro o utilità se si sta utilizzando denaro/utilità di provenienza illecita.

Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis* c.p.)

Tale reato è ipotizzabile in caso di finanziamento di associazioni con finalità di terrorismo o eversione dell'ordine democratico.

Finanziamento di condotte con finalità di terrorismo (270-*quinquies*.1 comma 1 e 2 c.p.)

Il reato in analisi è configurabile in caso di raccolta, erogazione, messa a disposizione di denaro o di beni destinati ad essere in tutto o in parte utilizzati per sostenere il compimento di condotte con

finalità terroristiche e ipotizzabile in caso di deposito o custodia di beni o somme di denaro destinati ad essere in tutto o in parte utilizzati per sostenere il compimento di condotte con finalità terroristiche.

Sottrazione di beni sequestrati (270-*quinquies*.2 c.p.)

Tale reato è ipotizzabile in caso di sottrazione, distruzione, dispersione, soppressione o deterioramento di beni o denaro, sottoposti a sequestro per prevenire il finanziamento delle condotte con finalità di terrorismo.

I processi e le attività sensibili

Tra le attività sensibili per la **Banca**, l'attenzione è stata rivolta soprattutto ai processi relativi all'apertura dei rapporti e alla movimentazione della liquidità.

Nello specifico, devono essere oggetto di particolare attenzione le aree c.d. strumentali, quali:

- gestione degli acquisti di beni e servizi (selezione, valutazione e gestione dei rapporti con i fornitori ai fini della stipula di contratti di acquisto di beni o servizi);
- gestione delle consulenze (es. in ambito *Information Technology*, legali, finanziarie, sicurezza, risorse umane, ecc.);
- gestione delle trasferte (autorizzazione, giustificativi, rimborsi spese, ecc.);
- gestione dei regali, degli omaggi e delle spese di rappresentanza;
- gestione della contabilità ordinaria (registrazione fatture passive, storno fatture, emissione note di credito, ecc.);
- gestione fatturazione attiva;
- gestione esecuzione contrattuale;
- gestione redazione del bilancio preventivo e del bilancio d'esercizio;
- gestione finanziaria (es. incasso e pagamenti tramite denaro contante, assegni, bonifici bancari);
- gestione delle attività di *marketing* (iniziative promozionale, sponsorizzazioni, ecc.).

Regole generali

Principi generali di controllo

Al fine di prevenire la commissione dei reati descritti nella presente **Parte Speciale** in relazione alle attività sensibili precedentemente indicate, la **Banca** ha identificato i seguenti principi di controllo:

- la verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari, sulla base di alcuni indici rilevanti (protesti; procedure concorsuali; acquisizioni d'informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate);

- la verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- il controllo formale e sostanziale dei flussi finanziari aziendali. Tali controlli devono tener conto della sede legale della società controparte, degli eventuali altri istituti di credito utilizzati e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o per azioni straordinarie;
- l'adozione di adeguati programmi di formazione per personale ritenuto esposto a rischio di riciclaggio e autoriciclaggio.

In tal senso, sono da attenzionare le operazioni sensibili considerate come "sospette", quali, ad esempio:

- il coinvolgimento di soggetti costituiti, operanti o insediati in Paesi caratterizzati da regimi privilegiati sotto il profilo fiscale o del segreto bancario ovvero in Paesi indicati dal GAFI come non cooperativi;
- le operazioni prospettate o effettuate a condizioni o valori palesemente diversi da quelli di mercato;
- le operazioni che appaiono incongrue rispetto alle finalità dichiarate;
- l'esistenza di ingiustificate incongruenze rispetto alle caratteristiche soggettive del cliente e alla sua normale operatività, sia sotto il profilo quantitativo, sia sotto quello degli atti giuridici utilizzati;
- il ricorso ingiustificato a tecniche di frazionamento delle operazioni;
- l'ingiustificata interposizione di soggetti terzi;
- l'ingiustificato impiego di denaro contante o di mezzi di pagamento non appropriati rispetto alla prassi comune e in considerazione della natura dell'operazione;
- il comportamento tenuto dai vertici aziendali, avuto riguardo, tra l'altro, alla reticenza nel fornire informazioni;
- l'effettuazione di pagamenti da parte di soggetti, persone fisiche o società non coincidenti con il debitore effettivo;
- l'intestazione di documenti contabili o di pagamento a società non coincidente con l'effettivo debitore;
- la sede *off-shore* di talune società;
- la genericità dell'oggetto della fattura ricevuta da parte di un fornitore.

Principi generali di comportamento

Tutti i Destinatari del **Modello**, nella misura in cui i medesimi possano essere coinvolti nello svolgimento di attività riconducibili alle attività sensibili ed in considerazione dei diversi obblighi e posizioni che ciascuno assume nei confronti della Banca, si attengono al rispetto di regole generali di condotta finalizzate a prevenire ed impedire il verificarsi degli illeciti in materia di riciclaggio e i delitti con finalità di terrorismo.

Al fine di prevenire la commissione dei reati sopracitati, è a carico dei Destinatari del **Modello** l'espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- porre comportamenti non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure della **Banca** o, comunque, non in linea con i principi espressi nel **Modello** e nel Codice di comportamento;
- acquisire a titolo oneroso o gratuito o dall'entrare in qualsiasi altro modo in possesso di danaro o cose provenienti da un qualsiasi delitto, anche se temporaneamente o per mera compiacenza;
- occultare danaro o cose provenienti da un qualsiasi delitto, anche se temporaneamente o per mera compiacenza;
- partecipare in alcun modo all'acquisto, alla ricezione o all'occultamento di denaro o cose provenienti da un qualsiasi delitto, anche se temporaneamente o per mera compiacenza;
- compiere operazioni (trasferimento, sostituzione o altre attività) atte ad ostacolare l'identificazione della effettiva provenienza di denaro, beni o altre utilità;
- impiegare in attività economiche e finanziarie, denaro, beni o altre utilità provenienti da delitto.

La presente **Parte Speciale** prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- attenersi ai provvedimenti riguardanti le limitazioni dell'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio ovvero di riciclaggio;
- consentire l'identificazione dei ruoli e delle responsabilità di autorizzazione, esecuzione e controllo del pagamento, con espressa indicazione dei soggetti chiamati ad eseguire le riconciliazioni bancarie;
- valutare periodicamente se, in ragione dell'area geografica in cui la Banca di volta in volta opera o di altre circostanze da cui emerga un maggiore rischio di infiltrazione criminale, sia necessario porre in essere un maggiore monitoraggio circa la selezione dei fornitori o circa la corretta e lecita esecuzione dei lavori affidati;
- evitare ogni tipo di intesa illecita con fornitori, potenziali fornitori, concorrenti, anche qualora questi dovessero promettere forniture a condizioni economiche particolarmente vantaggiose;
- 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);
- garantire il rispetto delle leggi e delle regolamentazioni vigenti in ogni contesto geografico ed ambito operativo, in particolare per quanto attiene ai provvedimenti per limitare l'uso

del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio ovvero di autoriciclaggio;

- seguire scrupolosamente tutte le regole aziendali previste in materia di gestione dei flussi finanziari in entrata e in uscita;
- consentire l'identificazione dei ruoli e delle responsabilità di autorizzazione, esecuzione e controllo del pagamento, con espressa indicazione dei soggetti chiamati ad eseguire le riconciliazioni bancarie;
- essere particolarmente scrupolosi nella verifica delle offerte anormalmente basse, poiché potrebbero celare tentativi di riciclaggio o, per l'acquisto di beni, potrebbero avere ad oggetto beni di provenienza illecita;
- richiedere tutte le informazioni necessarie a verificare l'attendibilità commerciale/professionale dei consulenti, fornitori e, in genere, delle controparti contrattuali;
- garantire il rispetto dei principi di correttezza, trasparenza e buona fede nell'ambito dei rapporti con i consulenti, i fornitori e, in genere, con le controparti contrattuali;
- monitorare nel tempo il permanere in capo ai consulenti, fornitori e, in genere, alle controparti contrattuali i requisiti di affidabilità, correttezza, professionalità e onorabilità;
- adottare adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio;
- gestire gli adempimenti fiscali nel pieno rispetto della normativa di riferimento sia per quanto concerne i calcoli di imposte e tasse, sia per quanto concerne i termini di pagamento;
- informare prontamente l'OdV, qualora sorga il ragionevole dubbio di trovarsi di fronte ad un'evenienza che possa ricondurre a situazioni connesse ai reati di cui sopra;
- assicurare la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure operative della Banca, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività sensibili nelle aree a rischio reato.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Regolamento Aziendale
- Regolamento Antiriciclaggio
- Strategia di classificazione della Clientela
- Regolamento per l'assunzione dei rischi di credito
- Capitolo S.04.01 - Antiriciclaggio e antiterrorismo

- Capitolo B.01.01 - Apertura rapporti della Clientela Private Banking
- Capitolo B.01.03 - Gestione rapporti della Clientela Finanza
- Capitolo B.02.01 - Operatività di cassa (in contanti o con assegni)
- Capitolo B.02.02 - Operatività con bonifico
- Capitolo B.07.01 - Richieste di credito della Clientela
- Capitolo B.07.04 - Gestione Linee di Credito Operativo Clientela Finanza
- Capitolo B.09.01 - Investment Banking e Strategic Equity - Gestione delle attività di Business dell'Area
- Capitolo B.01.06 - Rapporti dormienti e intestati al Fondo Unico di Giustizia
- Capitolo B.10.01 - Gestione delle attività di onboarding
- Capitolo B.10.02 - Movimentazione e gestione account
- Capitolo B.10.03 - Carte Prepagate
- Capitolo B.10.05 - Clientela Corporate

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Le fattispecie di reato

La Legge 3 agosto 2009, n. 116 di ratifica della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dall'Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4 e firmata dallo Stato italiano il 9 dicembre 2003 ha introdotto l'art. 25-*decies* del **D.Lgs. n.231/2001**, che individua specifiche ipotesi di reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, la cui commissione è suscettibile di implicare la responsabilità amministrativa della Banca.

A livello interno, i soggetti coinvolti nelle attività sensibili sono principalmente l'Amministratore Delegato, il Direttore Generale, i Vice Direttori Generali, oltre a tutte le Funzioni potenzialmente coinvolte in qualsiasi tipo di procedimento.

Si riporta di seguito una breve descrizione del reato rilevante in esame:

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

Il reato si configura qualora un soggetto, con violenza o minaccia, o con offerta o promessa di denaro o altra utilità, induca a non rendere dichiarazioni o a rendere dichiarazioni mendaci, la persona chiamata a rendere davanti all'Autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, qualora questa ha la facoltà di rispondere. Tali condotte delittuose possono verificarsi unicamente nel contesto di indagini e procedimenti giudiziari abbia effetti sostanziali in un altro Stato.

Il reato *de quo* è sussidiario in quanto trova applicazione solo quando la condotta criminosa posta in essere non sia riconducibile ad un'altra figura delittuosa. Tale ipotesi di reato si configura come reato comune in quanto può essere compiuto da chiunque ponga in essere i comportamenti incriminati.

I processi e le attività sensibili

Nell'identificazione delle aree sensibili, l'attenzione è stata rivolta in primo luogo a Rapporti con l'Autorità Giudiziaria in occasione di indagini e procedimenti giudiziari.

Regole generali

Principi generali di controllo e comportamento

Al fine di prevenire la commissione del reato sopracitato, è a carico dei Destinatari del **Modello** l'obbligo di:

- garantire piena libertà di espressione ai soggetti chiamati a rendere dichiarazioni davanti all'autorità giudiziaria;
- mantenere la riservatezza su eventuali dichiarazioni rilasciate all'autorità giudiziaria;
- promuovere il valore della leale collaborazione con l'autorità giudiziaria.

Al contempo, è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato previste dall'articolo 25-decies del Decreto;
- esercitare pressioni nei confronti di coloro che sono chiamati a rendere dichiarazioni davanti all'Autorità giudiziaria;
- realizzare comportamenti ritorsivi nei confronti di coloro che abbiano già rilasciato dichiarazioni all'Autorità giudiziaria;
- convocare i soggetti chiamati a rendere dichiarazioni davanti all'Autorità giudiziaria al fine di suggerirne i contenuti.

Con riguardo alle condotte relative al delitto di favoreggiamento:

- fornire informazioni o indicazioni non veritiere alla polizia giudiziaria o all'Autorità giudiziaria;
- aiutare o favorire l'occultamento o la fuga di persone ricercate dall'Autorità giudiziaria o sulle quali penda un procedimento penale.

Procedure specifiche

La Banca ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati

I reati ambientali

Le fattispecie di reato

In data 1° agosto 2011 è stato pubblicato sulla Gazzetta Ufficiale (Serie generale, n. 177) il D.Lgs. 7 luglio 2011, n. 121, che introduce i reati ambientali all'interno del **D.Lgs. n.231/2001** (art. 25-*undecies*).

La responsabilità amministrativa degli enti ai sensi del **Decreto** è stata quindi estesa anche ad alcuni illeciti commessi in violazione delle norme a protezione dell'ambiente.

I reati presupposto introdotti dall'articolo 25-*undecies* del **D.Lgs. 231/2001** rilevanti ai fini della presente **Parte Speciale** riguardano principalmente il non rispetto della normativa in materia di tracciamento e smaltimento dei rifiuti e di scarichi di acque reflue, e sono di seguito elencati:

- Scarichi di acque reflue (art. 137 del D.Lgs. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/2006);
- Divieto di abbandono (art. 192 D.Lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 D.Lgs. 152/2006);
- Traffico illecito di rifiuti (art. 259 D.Lgs. 152/2006);
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 6 c. 2 D. L. 138/2011).

I soggetti maggiormente coinvolti sono pertanto:

- Legale Rappresentante;
- Contractor e/o Outsourcer;
- Dipendenti;
- Fornitori/Enti esterni.

I processi e le attività sensibili

Tra le attività sensibili per la **Banca**, l'attenzione è stata rivolta soprattutto ai seguenti processi:

- censimento degli scarichi;
- gestione della richiesta e del rinnovo delle autorizzazioni o l'esecuzione di adempimenti verso la PA;
- individuazione della tipologia dei rifiuti prodotti e da smaltire;
- modalità di raccolta/deposito dei rifiuti;
- selezione fornitori di servizi di smaltimento dei rifiuti;
- affidamento dei rifiuti allo smaltitore;
- valutazione del merito creditizio da parte della Banca a favore di imprese o di soggetti che professionalmente svolgono attività che possono presentare un rischio ambientale.

Regole generali

Principi di controllo

Al fine di prevenire la commissione dei reati descritti nella presente **Parte Speciale** in relazione alle attività sensibili precedentemente indicate, la **Banca** ha identificato i seguenti principi di controllo:

- massimo rispetto delle leggi e normativa vigenti, dei principi di correttezza e trasparenza, nonché delle procedure e dei protocolli aziendali in materia di gestione ed impiego delle risorse e dei beni aziendali;
- chiarezza, trasparenza, diligenza e spirito di collaborazione con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti ed Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste.

Principi generali di comportamento

Nell'espletamento della propria attività, i soggetti coinvolti sono tenuti ad osservare i principi di comportamento di seguito indicati:

- rispettare le procedure specifiche, con specifico riguardo alla parte in cui prevede che le attività aziendali vengano svolte nel rispetto della salubrità ambientale;
- identificare gli aspetti ambientali connessi a tutte le proprie attività e ai luoghi di lavoro;
- considerare ed ottemperare a tutte le prescrizioni legali ed alle altre prescrizioni applicabili alla materia ambientale;
- gestire e smaltire correttamente i rifiuti prodotti;
- supervisionare e predisporre ogni azione necessaria affinché la caratterizzazione dei rifiuti e la definizione delle specifiche modalità di smaltimento avvenga secondo i principi di accuratezza e nel rispetto delle prescrizioni autorizzative e normative.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento;
- Poteri Delegati;
- Strategia di classificazione della Clientela;
- Capitolo - S.13.01 Gestione acquisti e servizi logistici/ausiliari;
- nel caso in cui vi siano cantieri e/o lavori in corso: norme contrattuali con Contractor e/o Outsourcer;
- nel caso in cui la **Banca** si avvalga di fornitori per la gestione e lo smaltimento di rifiuti particolarmente inquinanti: norme contrattuali.

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Le fattispecie di reato

L'art. 25-*duodecies* del **D.Lgs. n.231/2001** individua specifiche ipotesi di reato in materia di immigrazione, la cui commissione è suscettibile di implicare la responsabilità della **Banca** ai sensi del **Decreto**.

In particolare, si riporta di seguito una breve descrizione della fattispecie di reato individuato come rilevante per la **Banca**:

Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 2 del D.Lgs. 286/1998 - Testo Unico sull'immigrazione)

Tale reato si configura nel procedimento relativo all'assunzione di lavoratori subordinati stranieri, a tempo determinato e/o indeterminato, sprovvisti del permesso di soggiorno.

I processi e le attività sensibili

I processi sensibili relativi all'attività svolta dalla **Banca** sono quelli di selezione, assunzione e gestione delle Risorse Umane.

Regole generali

Principi generali di controllo e comportamento

Tutte le attività sensibili devono essere svolte conformemente alle disposizioni normative e regolamentari vigenti, alle norme della Carta dei principi e codice di comportamento, ai principi generali di comportamento enucleati nella **Parte Generale** del presente **Modello**, nonché ai protocolli (e alle ulteriori procedure organizzative esistenti) a presidio dei rischi reato individuati.

La Banca si impegna in particolare a:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla selezione/gestione/amministrazione del personale;
- tenere un comportamento collaborativo anche con le agenzie di somministrazione di cui dovesse avvalersi, sì da facilitare lo scambio continuo di informazioni;
- richiedere e acquisire, in fase di assunzione, copia del permesso di soggiorno del lavoratore, qualora richiesto dalla legge;
- monitorare lo *status* degli eventuali lavoratori in prossimità della scadenza del permesso di soggiorno in vista di eventuali rinnovi contrattuali che non potranno prescindere da provvedimenti di rinnovo del permesso di soggiorno.

Al contempo, è fatto divieto di:

- violare i principi, i protocolli e le procedure di assunzione esistenti;
- assumere lavoratori stranieri privi di permesso di soggiorno o con permesso di soggiorno irregolare;
- stipulare contratti a tempo determinato con durata successiva alla scadenza del permesso di soggiorno;
- comunicare dati o informazioni non corrispondenti al vero;
- fornire collaborazione o supporto, anche indiretto, a condotte non oneste o potenzialmente illecite da parte degli esercenti e in particolare fornire collaborazione nei casi in cui vi è ragionevole dubbio che essi possano mettere in atto condotte che configurino reati di cui alla presente **Parte Speciale**;
- utilizzare le lettere d'invito al solo fine di introdurre nel paese lavoratori irregolari.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Capitolo S.09.01 – Selezione, assunzione, trasferimento e cessazione del Personale

I Reati tributari

Le fattispecie di reato

L'introduzione dei delitti tributari nel catalogo dei reati-presupposto della responsabilità amministrativa degli enti *ex* D.Lgs. n. 231/01 costituisce il recepimento da parte del legislatore delle indicazioni europee contenute nella Direttiva 1371/2017 UE in materia di tutela degli interessi finanziari dell'Unione Europea. Tale normativa impone infatti agli Stati membri di adottare misure, anche nei confronti degli enti, volte a reprimere le frodi fiscali.

Con l'art. 25-*quinquiesdecies* del **D.Lgs. 231/2001**, il legislatore ha dunque introdotto nuove fattispecie di reati presupposto principalmente riconducibili alle fattispecie di cui al D.Lgs. 10 marzo 2000, n. 74, che detta la nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto.

Secondo la disciplina dettata dall'art. 25-*quinquiesdecies,* la sanzione pecuniaria da irrogare all'ente che abbia conseguito un profitto di rilevante entità in virtù della commissione di un reato presupposto ivi previsto, è inoltre aumentata di un terzo.

I soggetti e le strutture individuati all'interno della compagine aziendale come maggiormente coinvolti in aree potenzialmente a rischio sono:

- Dirigente Preposto;
- Funzione Contabilità Generale;
- Funzione Bilancio e Fiscale;
- Funzione Corporate Services;
- Fornitori/consulenti esterni;
- Ogni altra Funzione coinvolta nella predisposizione ed elaborazione dei documenti contabili societari.

Di seguito si procede con una breve descrizione dei reati rilevanti ai fini della presente **Parte Speciale**:

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 co. 1, D.Lgs. 74/2000)

È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 comma 2-bis, D.Lgs. 74/2000)

Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 74/2000)

Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

a. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a € 30.000,00;
b. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a € 1.500.000,00, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a euro € 30.000,00.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Emissione di fatture o di altri documenti per operazioni inesistenti (art. 8 comma 1, D.Lgs. 74/2000)

È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.
Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a € 100.000,00, si applica la reclusione da un anno e sei mesi a sei anni.

Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 74/2000)

Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Sottrazione fraudolenta al pagamento delle imposte (art. 11, D.Lgs. 74/2000)

È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o

compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Reati tributari commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'IVA per un importo complessivo non inferiore a 10 milioni di euro, ed in particolare: Dichiarazione infedele (art. 4, D.Lgs. 74/2000)

Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

a. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
b. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

Fuori dei casi di cui al paragrafo precedente, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste *sub* lett. a) e b).

Omessa dichiarazione (art. 5, D.Lgs. 74/2000)

È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore a euro cinquantamila.

Non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Indebita compensazione (art. 10-*quater*, D.Lgs. 74/2000)

È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.

È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

I processi e le attività sensibili

L'analisi dei processi posti in essere dalla Banca ha consentito l'individuazione delle attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato esaminate in questa sede.

A tal fine è necessario evidenziare che i rischi di commissione dei delitti sopra indicati possono annidarsi anche nei rapporti commerciali con soggetti terzi, siano essi privati o pubblici (contratti di acquisto e/o vendita) e nella gestione dei flussi finanziari.

Sono pertanto fortemente raccomandate misure preventive, mutuate dai principi fondamentali della normativa antiriciclaggio.

Tra le attività sensibili per la **Banca**, l'attenzione è stata rivolta soprattutto ai processi che riguardano in particolare:

- le dichiarazioni fiscali;
- la tenuta della contabilità;
- la predisposizione della situazione contabile annuale e infra-annuale e altri documenti rappresentanti la situazione economica, finanziaria e patrimoniale della **Banca**.

Regole generali

Principi di controllo

Tutti i Destinatari del **Modello**, nella misura in cui i medesimi possano essere coinvolti nello svolgimento di attività riconducibili alle attività sensibili ed in considerazione dei diversi obblighi e posizioni che ciascuno assume nei confronti della **Banca**, si attengono al rispetto di regole generali di condotta finalizzate a prevenire ed impedire il verificarsi degli illeciti in materia di illeciti in materia di reati tributari.

In base all'analisi volta all'individuazione dei processi decisionali, organizzativi e operativi potenzialmente esposti al rischio di commissione dei reati tributari in commento, la **Banca** ha individuato i seguenti principi di controllo:

- controlli di correttezza ed accuratezza in fase di determinazione delle imposte dirette e indirette;

- adeguato monitoraggio dell'evoluzione del quadro normativo di riferimento;
- adeguata gestione degli aspetti contrattuali con l'eventuale fornitore dei servizi in ambito fiscale;
- controlli di correttezza ed accuratezza dei dati da inserire nei modelli di versamento/dichiarativi;
- controlli di accuratezza e completezza della documentazione a supporto dei versamenti in materia fiscale;
- individuazione formale delle figure aziendali incaricate di effettuare la predisposizione dei modelli di versamento/dichiarativi;
- formale approvazione, da parte di adeguati livelli organizzativi, della documentazione relativa ai modelli di versamento/dichiarazioni al fine di effettuare l'invio telematico degli stessi;
- controlli, svolti dalla Funzione coinvolta, atti a verificare l'accuratezza e la correttezza dei modelli di versamento / dichiarativi predisposti dallo l'eventuale fornitore dei servizi in ambito fiscale, nel rispetto dei contratti in essere;
- definire con chiarezza ruoli e compiti delle Funzioni organizzative responsabili della gestione delle varie fasi del processo sensibile;
- garantire la tracciabilità del processo decisionale, mediante la predisposizione e l'archiviazione della relativa documentazione di supporto.

Principi di comportamento

Tutti i Destinatari del **Modello**, nella misura in cui i medesimi possano essere coinvolti nello svolgimento di attività riconducibili alle attività sensibili ed in considerazione dei diversi obblighi e posizioni che ciascuno assume nei confronti della **Banca**, si attengono al rispetto di regole generali di condotta finalizzate a prevenire ed impedire il verificarsi degli illeciti in materia di reati tributari.

Al fine di prevenire la commissione dei reati sopracitati, è a carico dei Destinatari del **Modello** l'espresso divieto di:

- presentare dichiarazioni fiscali falsate con elementi passivi fittizi, avvalendosi di fatture o di altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria;
- simulare operazioni o falsare documenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria;
- rilasciare fatture e altri documenti per operazioni inesistenti con lo scopo di consentire a terzi di evadere le imposte sui redditi o l'Iva, ovvero occultare o distruggere documentazione contabile tale da non permette la ricostruzione dei redditi o del volume di affari;
- alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria;

- indicare in una delle dichiarazioni annuali relative alle imposte sui redditi o sul valore aggiunto, elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti;
- non presentare, essendovi obbligato, una delle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto;
- utilizzare impropriamente in compensazione (ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241) crediti non spettanti.

È inoltre obbligatoria:

- la tracciabilità dell'operazione tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del processo da parte della funzione coinvolta;
- l'utilizzo del sistema informatico dedicato per la registrazione delle fatture attive e passive, nonché di ogni altro accadimento economico;
- la verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni commerciali;
- la contabilizzazione da parte dell'ufficio responsabile delle sole fatture attive/passive che hanno ricevuto il benestare alla registrazione e al loro pagamento/incasso solo dopo aver ricevuto il benestare del responsabile di funzione;
- la rilevazione di tutti i fatti amministrativi aziendali che hanno riflesso economico e patrimoniale;
- il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette;
- la diffusione delle principali novità normative in materia fiscale al personale coinvolto nella gestione della fiscalità;
- la verifica con un consulente terzo di qualsivoglia implicazione fiscale derivante dall'esecuzione di un'operazione avente carattere ordinario o straordinario.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Sezione S.8 – Gestione contabile del Manuale delle Procedure Aziendali:
- Capitolo S.08.01 - Gestione del Piano dei Conti di Contabilità Generale
- Capitolo S.08.02 – Attività contabili mensili
- Capitolo S.08.03 – Bilancio Individuale e situazioni finanziarie periodiche
- Capitolo S.08.04 - Bilancio Consolidato e situazioni finanziarie periodiche
- Capitolo S.08.05 - Dirigente preposto alla redazione dei documenti contabili societari

- Capitolo S.08.06 – Redazione situazioni finanziarie annuali e infra-annuali
- Capitolo S.08.07 – Fornitori e fatturazione
- Capitolo S.08.08 - Gestione degli adempimenti Fiscali e formalità annesse
- Capitolo S.08.09 – Altre attività contabili e amministrative
- Capitolo S.08.10 – Fatturazione e altre attività contabili relative all'Area Investment Banking e Strategic Equity e all'Area Finanza
- Capitolo S.08.11 – Conferimento dell'incarico di revisione legale dei conti
- Capitolo S.13.01 - Gestione acquisti e servizi logistici/ausiliari
- Capitolo S.04.03 - Gestione operazioni con Parti Correlate o con potenziale interesse degli Amministratori
- Capitolo S.06.01 - Gestione delle attività societarie

Delitti in materia di strumenti di pagamento diversi dai contanti

Le fattispecie di reato

L'art. 25-*octies.*1 del Decreto elenca una serie di reati previsti dal codice penale e riguardanti gli strumenti di pagamento diversi dal contante.

I soggetti e le strutture individuati all'interno della compagine aziendale come maggiormente coinvolti in aree potenzialmente a rischio sono:

- Dirigente Preposto;
- Area Private Banking;
- Area Operations;
- Area Digital;
- Outsourcer Informatico.

Di seguito si illustrano la fattispecie rilevanti ai fini della presente **Parte Speciale**:

Indebito utilizzo e falsificazione di carte di credito o di carte di pagamento (art. 493-*ter* c.p.)

Tale reato è ipotizzabile qualora un soggetto utilizzi indebitamente, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo o comunque ogni altro strumento di pagamento diverso dai contanti che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, oppure qualora un soggetto falsifichi o alteri carte di credito o di pagamento o qualsiasi altro documento analogo o comunque ogni altro strumento di pagamento diverso dai contanti che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero si possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché' ordini di pagamento prodotti con essi.

Detenzione e diffusione di apparecchiature, dispositivi, programmi informatico diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* c.p.)

Il reato è configurabile il soggetto produca, importi, esporti, venda, trasporti, distribuisca, metta a disposizione o in qualsiasi modo procuri a sé o ad altri apparecchiature, dispositivi o programmi informatici progettati principalmente per le finalità elencate per la fattispecie di reato di cui sopra, o adattati a tale scopo.

Frode informatica nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro (art. 640-*ter* c.p. come integrato dal D.Lgs. 184/2021)

Il reato si configura qualora si alteri il sistema informatico per procurare un profitto a sé stessi o un danno a un terzo e tale azione implichi un trasferimento di denaro, di valore monetario, di valuta virtuale.

Trasferimento fraudolento di valori (art. 512-*bis* c.p.)

La norma punisce, con clausola di riserva:

- chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-*ter*;
- chiunque, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

Si tratta dunque di un reato a forma libera, che può essere commesso da chiunque, e che si concretizza nella dolosa determinazione di una situazione di apparenza giuridica e formale della titolarità o della disponibilità di un bene, difforme dalla realtà, al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniale o di contrabbando.

L'espressione "*attribuzione fittizia della titolarità o della disponibilità di denaro, beni o altre utilità*" ha, quindi, una valenza ampia che si riferisce non soltanto alle forme negoziali tradizionalmente intese, ma a qualsiasi tipologia di atto idonea a creare un apparente rapporto di signoria tra un determinato soggetto e il bene, rispetto al quale permane intatto il potere di colui che effettua l'attribuzione.

Dal punto di vista soggettivo, il reato è punito a titolo di dolo specifico che consiste nel fine di eludere le disposizioni di legge in materia di misure di prevenzione e può essere configurato non solo quando sia già in atto la procedura di prevenzione, ma anche prima che la detta procedura sia intrapresa, quando l'interessato possa fondatamente presumerne l'inizio.

Ai fini della configurabilità del delitto di trasferimento fraudolento di valori, non occorre la preventiva emanazione delle misure di prevenzione, né la pendenza del relativo procedimento, bastando soltanto che l'autore ne possa temere l'instaurazione.

I processi e le attività sensibili

Tra le attività sensibili per la **Banca**, l'attenzione è stata rivolta soprattutto ai processi che riguardano in particolare:

- la movimentazione della Liquidità e Strumenti di Pagamento;
- la gestione dei sistemi informativi.

Regole generali

Principi generali di controllo

Il sistema di controllo a presidio dell'area di attività sensibile descritta deve basarsi sui seguenti principi:

- definizione dei livelli autorizzativi, in particolare in relazione all'individuazione e all'autorizzazione dei soggetti che hanno accesso a dispositivi atti alla movimentazione

della liquidità e degli strumenti di pagamento, con evidenza di tali assegnazioni nelle specifiche procedure gestionali;

- segregazione dei compiti tra i differenti soggetti coinvolti nel processo, in particolare nella gestione dei sistemi informativi;
- definizione delle attività di controllo interno nello svolgimento delle attività di gestione dei dispositivi atti alla movimentazione della liquidità e agli strumenti di gestione dei relativi sistemi informativi, anche con riferimento alle apparecchiature ATM/MTA.

Principi generali di comportamento

Le Aree e le strutture della **Banca** coinvolte nei processi sensibili sono tenute ad osservare le modalità esposte negli appositi protocolli e procedure, nonché le disposizioni di legge esistenti in materia, e:

- devono essere appositamente incaricati nelle specifiche procedure gestionali;
- hanno l'obbligo di astenersi dal compiere attività/operazioni volte a utilizzare indebitamente o ad alterare/falsificare strumenti di pagamento, quali carte di credito o ogni altro strumento di pagamento diverso dai contanti che abilitino al prelievo di denaro e all'acquisto di beni e servizi;
- hanno l'obbligo di astenersi dal produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per alterare/falsificare strumenti di pagamento;
- hanno l'obbligo di astenersi dal compiere attività/operazioni che possano compromettere il sistema informatico in uso dando luogo a trasferimenti di denaro, di valore monetario o valuta in maniera indebita.

Procedure specifiche

La **Banca** ha implementato le seguenti procedure specifiche a presidio dell'area di rischio, compendiate nei seguenti documenti, cui si fa rinvio:

- Carta dei principi e codice di comportamento
- Poteri Delegati
- Regolamento Aziendale
- Rischio informatico e Continuità operativa
- Policy di Sicurezza Informatica
- Policy di Sicurezza Informatica per i servizi di pagamento via internet
- Documento di Indirizzo Strategico in materia di Sistemi Informativi
- Capitolo B.02.03 - Distribuzione delle Carte di Credito
- Capitolo B.10.06 - Prevenzione e gestione delle frodi

- Capitolo S.11.01 - Gestione delle Tecnologie, Sistemi e Applicazioni (con Appendici sulla Sicurezza Informativa)