MODELLO ORGANIZZATIVO

AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica

SEZIONE SPECIALE

Versione 2.1

Aree e attività a rischio - Sistemi di presidio organizzativi e gestionali

SOMMARIO

Sommario

VERSIONI

VERSIONE	DESCRIZIONE	AUTORE/DATA	DELIBERAZIONE DEL CDA
1.0	Creazione documento	OdV 231	22 settembre 2010
2.0	Aggiornamento e revisione	OdV 231	3 giugno2021
2.1	Aggiornamento e revisione	OdV 231 (1/3/2022)	

PARTE I

PREMESSA

La parte speciale ha la finalità di definire le linee, le regole ed i principi di comportamento delle specifiche aree di rischio e delle attività sensibili della Banca.

Nel presente documento si riportano i protocolli riferiti ai reati presupposto, al fine di ottemperare a quanto previsto nel decreto 8 giugno 2001 numero 231 all'art 6 comma 2 lettera b che prescrive quanto segue: "*b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*"[1].

L'elaborazione del presente modello tiene conto della specificità aziendale, del settore in cui opera e la sua storia (anche giudiziaria).

L'esigenza di rinnovamento del modello, rispetto alla precedente versione, scaturisce anche dal tipo di approccio alla materia da parte delle nuove normative e che anche le recenti certificazioni adottate nel mondo delle imprese hanno deciso di utilizzare con frequenza ormai costante: il cosiddetto *risk-based approach*.

Sotto la pressione di queste nuove normative la gestione del rischio è diventato uno degli strumenti obbligatori per il *management*. Per fare alcuni esempi, risultano attualmente basate sul rischio:

- l'ISO 9001:2015 sui sistemi di gestione qualità;
- l'ISO 37001:2016 sui sistemi di prevenzione della corruzione;
- la recente normativa GDPR in materia di protezione dei dati personali.

Oggi più che mai la banca deve essere in grado di affrontare tutte le sfide di *compliance* (dalla sicurezza sul lavoro fino alla gestione della *cyber-sicurezza*) con una visione integrata e guidata dalla gestione dei rischi.

Per tale motivo gli *standard* internazionali considerano oggi il *risk management* come la base su cui costruire un Sistema di Controllo Interno in grado di funzionare davvero, come mezzo per integrare tra loro normative sempre più complesse e specialistiche.

Quindi ai fini della metodologia si vuole rappresentare in primo luogo un'opportunità di self-assessment sui processi di valutazione del rischio 231, attraverso un percorso a tre fasi:

[1] Con il termine protocollo e/o procedura si intende "*un insieme di principi, situazioni, meccanismi organizzativi e operativi di comportamento che é funzionale alla gestione del rischio-reato, nel senso che la sua corretta applicazione, anche in combinazione con altri protocolli e/o procedure, é tale da prevenire la commissione del reato da cui sorge la responsabilità ex d.lgs. 231/2001*".

- inventariazione degli ambiti aziendali di attività;
- analisi dei rischi potenziali;
- valutazione/costruzione/adeguamento del sistema di controlli preventivi

Va fatto altresì osservare che ogni reato viene scomposto nelle modalità attuative che sono in grado di azionarlo, tenendo conto che i rischi sono avvenimenti:

- specifici
- singoli
- possibili.

Pertanto, per ovviare alle difficoltà di ogni *risk identification*, le singole modalità attuative andranno a comporre la "*Mappa documentata delle potenziali modalità attuative degli illeciti nelle aree di rischio*" (Protocolli 231 descritti nel presente documento).

Dalla suindicata attività nelle aree di attività considerate a rischio reato o strumentali, vengono individuate e separate:

a) le aree/processi ritenute "*a rischio reato*" e le attività ''*sensibili*'' e quindi:
   - le funzioni e/o i servizi e/o gli uffici aziendali che operano nel suindicato ambito;
   - i reati astrattamente perpetrabili nella specifica area/processo;
   - laddove possibile in via esemplificativa, le modalità attraverso cui i reati in parola possono essere (astrattamente) commessi nonché i controlli preventivi;

b) le aree ritenute "*strumentali*" alle sopra indicate aree a rischio e quindi:
   - le funzioni e/o i servizi e/o gli uffici aziendali che operano nel predetto ambito;
   - i controlli preventivi per ridurre il rischio.

Si qualificano aree "*a rischio reato*", i settori e/o dei processi aziendali rispetto ai quali si ritiene sussistente il rischio di commissione di uno dei reati rilevanti ai sensi del D.lgs. 231/2001.

Sono aree "*strumentali*" quei processi aziendali la cui esecuzione non comporta un rischio diretto di reato, ma nel cui ambito è possibile individuare una funzione preparatoria o propedeutica al reato.

Altresì, ai fini dell'identificazione dei rischi 231, occorre tenere presente che:

- una stessa modalità attuativa (cioè uno stesso rischio) può azionare più di un reato;
- esiste un punto di equilibrio sulla quantità di rischi da identificare:
  - un numero troppo basso di rischi identificati condurrebbe ad un'elevata genericità, vanificando la corretta valutazione degli stessi;
  - un numero troppo elevato di rischi porterebbe a perdere di vista il reale obiettivo, cioè quello di evitare la commissione di reati.

Invece, con riferimento alla valutazione dei rischi, ciascuna modalità attuativa degli illeciti è stata valutata secondo due parametri:

- gravità;
- probabilità.

La gravità deriva direttamente dal reato-presupposto che un avvenimento (il rischio) potrebbe azionare. Il fattore di gravità lega quindi un rischio a ciò che esso è in grado di provocare, cioè ad un reato presupposto. Mentre la gravità di un rischio dipende dalle sanzioni ad esso legate, la sua probabilità risulta invece un fattore strettamente connesso all'attività aziendale. Esistono avvenimenti in grado di provocare taluni reati con una più alta probabilità di accadimento, mentre altri rischi, in grado anch'essi di causare gli stessi tipi di reati, avranno una probabilità minore.

Da ultimo si riporta che il collegamento degli specifici controlli interni e le singole minacce segnano il passaggio fondamentale per evitare duplicazione di costi e spreco di risorse aziendali.

Per dare l'idea al lettore, si riportano di seguito alcune precisazioni metodologiche:

- un singolo controllo può diminuire diversi rischi, anche di differenti aree e connessi a differenti reati;
- un singolo controllo interno può essere più efficace nel rispondere ad un determinato rischio e meno efficace nel rispondere ad un altro;

Essenziale rimane il fatto che tutti i controlli sono parametrizzati sulla base del rischio e pensati con l'obiettivo di raggiungere il livello di accettabilità in ogni rischio residuo.

STRUTTURA DEL DOCUMENTO

La presente sezione viene suddivisa per categorie di reati presupposto, dove vengono:

- fornite le indicazioni per sintesi delle caratteristiche di ciascuna tipologia di reato;
- identificate le attività sensibili, ossia le attività della banca caratterizzate dal rischio insito di commissione dei reati presupposti;
- stabiliti e indicati gli standard di controllo, ossia la previsione per ciascuna delle suddette attività sensibili, principi, protocolli di prevenzione e relativi controlli, taluni anche trasversali, nel senso che sono applicabili a più attività sensibili, a loro volta associati agli strumenti normativi, alle procedure e istruzioni operative.

A fattor comune, per tutte le attività a rischio, valgono i seguenti presidi organizzativi e gestionali:

- ✓ Statuto aggiornato dall'Assemblea Straordinaria dei Soci.
- ✓ Codice Etico della Banca.
- ✓ Sistema di attribuzione dei poteri e delle deleghe da parte del CdA mediante conferimento ai livelli aziendali.
- ✓ Sistema sanzionatorio previsto nel Regolamento disciplinare e nel Codice aziendale di comportamento annesso al presente Modello.
- ✓ Istruzioni di vigilanza della Banca d'Italia e norme delle Autorità di Vigilanza.
- ✓ Procedure e strumenti normativi che regolamentano i vari processi aziendali.

LA METODOLOGIA SEGUITA PER L'INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI

Sulla base della matrice rischio-reato elaborata ai fini del presidio, la Banca provvede nel continuo – anche in ossequio a quanto previsto dall'art. 6, comma 2, lett. a) del D. Lgs. 231 - all'individuazione delle cosiddette "*aree sensibili*" o "*a rischio*", cioè all'identificazione dei processi e delle fasi di questi ultimi esposte al rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231.

La metodologia utilizzata è coerente con l'approccio utilizzato nel Progetto nazionale di Categoria e del GBCI sul "*Sistema dei Controlli Interni*" (valutazione dei rischi di processo) e viene personalizzata e resa coerente con le matrici utilizzate per le analisi dei rischi, al fine di utilizzare uno strumento facilmente gestibile, aggiornabile nel tempo e con una reportistica standard.

La metodologia prevede le seguenti fasi:

- l'analisi dei reati previsti dal Decreto e l'individuazione delle possibili modalità di realizzazione della condotta illecita all'interno dei processi di lavoro (anche attraverso l'esemplificazione di alcune fattispecie concrete);
- individuazione della probabilità di accadimento del reato in relazione alla specifica attività sensibile precedentemente individuata.

La descrizione delle attività sensibili è organizzata in un database di riferimento che costituisce il repository dei rischi 231 e che è di supporto nel monitoraggio periodico dei rischi e nel loro aggiornamento.

I risultati dell'analisi vengono riportati nel documento "*Report Ordinario sulla Responsabilità Amministrativa da reato*", soggetto a periodica valutazione da parte del C.d.A. e/o del Comitato Consultivo Controlli Interni della Banca ed a costante aggiornamento da parte dell'Organismo di Vigilanza.

LE ATTIVITÀ SENSIBILI (EX ART. 6 COMMA 2 LETTERA A)

Anche per l'individuazione delle attività sensibili ex D. Lgs. 231, come detto la Banca adotta perlopiù le metodologie elaborate nell'ambito dei Progetti di Categoria, al pari di tutte le attività a rischio presenti nei diversi ambiti operativi tipici dell'attività bancaria.

L'analisi viene effettuata con la collaborazione dei responsabili di processo, sia a presidio ex ante e sia ai fini del monitoraggio, sulla realtà operativa aziendale e viene, altresì, svolta con riferimento ai Soggetti apicali, particolarmente esposti ad alcune tipologie di reato per le specifiche responsabilità assegnate, attraverso un'attività di autovalutazione ai fini della stima delle probabilità di reato.

Vengono presi in considerazione i seguenti processi:

- Governo;
- Credito;
- Finanza;
- Risparmio;
- Incassi e Pagamenti;
- Estero;
- Contabilità, Bilancio e Segnalazioni di Vigilanza;
- Disposizioni Normative;
- Gestione Sistemi informativi;
- Contante e valori;
- Tesoreria Enti;
- Infrastrutture e Spese,
- Risorse Umane.

In particolare, per ogni attività a potenziale rischio di commissione reati vengono raccolti in uno specifico supporto, oggetto di costante aggiornamento, i seguenti elementi informativi:

- lo svolgimento, o meno, dell'attività sensibile presso la Banca, al fine di limitare l'analisi al perimetro di effettivo rischio aziendale;
- l'unità organizzativa responsabile dell'attività;
- la descrizione delle modalità di svolgimento del processo anche in termini di livello di definizione delle procedure rispetto all'obiettivo di prevenire la commissione del reato;
- le contromisure adottate e/o da adottare (normativa, poteri di firma e poteri autorizzativi, segregazione dell'attività, tracciabilità, altri presidi);
- l'indicazione delle criticità emerse e delle aree di miglioramento, sempre in ottica di prevenzione dei reati.

IL SISTEMA DEI CONTROLLI INTERNI

L'assetto organizzativo della Banca è un sistema strutturato ed organico di procedure, regole comportamentali, disposizioni e strutture organizzative che permea l'intera attività aziendale, attraverso la netta distinzione dei compiti operativi da quelli di controllo, evitando quindi le possibili situazioni di conflitto di interesse.

Il Sistema dei Controlli Interni, nel quale è assicurata la separazione delle funzioni di controllo da quelle produttive, è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il rispetto delle strategie e delle politiche aziendali nonché il conseguimento del corretto svolgimento dei procedimenti operativi, quindi assolutamente funzionale anche al presidio dei rischi reato.

Il Sistema di controllo contribuisce a rendere gli organi aziendali consapevoli del presidio dei rischi aziendali, orienta i mutamenti delle linee strategiche e delle politiche aziendali e consente di adattare in modo coerente il contesto organizzativo; presidia la funzionalità dei sistemi gestionali e il rispetto degli istituti di vigilanza prudenziale; favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori aziendali[2].

Il Sistema dei Controlli Interni è articolato su tre livelli di controllo (così come definiti dall'Organo di Vigilanza):

- controlli di linea (c.d. "controlli di I livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Tali controlli sono effettuati dalle stesse strutture operative, ovvero eseguiti nell'ambito del back office, tenendo presente che la Banca massimizza il ricorso a controlli di linea incorporati all'interno delle procedure informatiche.
- controlli sui rischi e sulla conformità (cd. "controlli di II livello"), assegnati a funzioni distinte da quelle produttive - contrattualmente esternalizzate al GBCI (Risk Management, Compliance e AML) - che hanno l'obiettivo di assicurare tra l'altro:
  i. la corretta attuazione del processo di gestione dei rischi;
  ii. il rispetto dei limiti operativi assegnati alle varie funzioni aziendali;
  iii. la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.
- revisione interna (cd. "controlli di III livello"), volta ad individuare la violazione delle procedure e della regolamentazione nonché a valutare la funzionalità e l'adeguatezza, in termini di efficienza e di efficacia, del Sistema dei Controlli Interni e del sistema informativo,

[2] Cfr. Circ. n.285/2013 Banca d'Italia

con cadenza determinata in relazione alla natura e all'intensità dei rischi.

Nell'ambito dell'architettura del Sistema dei Controlli Interni della Banca, si incardinano anche le attività di controllo rispetto ai rischi sottesi alla esternalizzazione di funzioni aziendali (outsourcing), in particolare quando trattasi di Funzioni Operative Importanti (FOI).

Tali attività di controllo riguardano i tre livelli di controllo sopra illustrati. Esse sono dirette a verificare:

- che l'Outsourcers mantenga le competenze e le capacità e le autorizzazioni richieste dalla legge per esercitare la prestazione in maniera professionale e affidabile;
- il rispetto delle clausole contrattuali con particolare riferimento ai livelli di servizio attesi;
- il corretto andamento delle "relazioni" con l'Outsourcers.

A tale riguardo, poiché le Disposizioni richiedono la predisposizione di adeguati presidi organizzativi volti a fronteggiare i rischi sottesi all'esternalizzazione delle FOI, la Banca ha individuato un Referente per le attività esternalizzate che ha come principale mandato il monitoraggio nel continuo delle attività esternalizzate.
Tali attività di controllo riguardano, altresì, le strutture operative della Banca impattate dalle esternalizzazioni, nonché la funzione di revisione interna che svolge i controlli di terzo livello sulle attività esternalizzate.

Il Modello di organizzazione e gestione ferma restando la sua finalità peculiare, come detto, viene integrato nel contesto del più ampio sistema di controlli interni in essere presso la Banca, così come tale sistema è in grado, con gli eventuali adattamenti che si rendessero necessari nel tempo, di essere utilizzato anche allo scopo di prevenire i reati contemplati dal D.Lgs. 231/01.

Funzionale allo scopo è l'istituzione dell'Ufficio Controlli Interni identificato dalla Banca, nell'ambito dell'Ufficio Organizzazione, come ruolo specifico per ottimizzare la gestione delle relazioni tra le funzioni di controllo esternalizzate e la struttura organizzativa interna.

Infatti, la U.O. incaricata - che agisce in coordinamento con il Consigliere Delegato al sistema dei controlli interni e partecipa alle riunioni del Comitato Consultivo dei Controlli per tutte le analisi e gli approfondimenti richiesti - svolge le seguenti attività in materia di controlli interni:

- è il ruolo aziendale incaricato di interfacciare le Funzioni Aziendali di Controllo esternalizzate:
- cura l'apertura degli audit e coordina la struttura interna nella produzione della documentazione richiesta;
- riceve ed accoglie gli auditor e li assiste durante l'esercizio dei controlli;
- su richiesta degli auditor coinvolge i responsabili di UO interessati dai controlli;

- partecipa agli exit meeting e funge da project office interno;
- ricevuto il report finale attribuisce a ciascun owner i task di remediation previste;
- svolge il follow-up dei remediation plan ed assicura le risposte nei tempi previsti.

A tal guisa è evidente che il sistema strutturato ed organico di procedure e le attività di controllo (preventive, ex-post, sia di routine che a sorpresa) disposte dalla Banca soddisfano l'obiettivo di una consapevole gestione del rischio di commissione dei reati ex Dlgs 231/01, anche mediante l'individuazione dei processi sensibili e la loro conseguente proceduralizzazione con implementazione di appositi protocolli di prevenzione.

Vengono, inoltre, prese in considerazione sistematiche procedure di ricerca e identificazione dei rischi per casi particolari, ad esempio in occasione della periodica rotazione del personale per ordinari avvicendamenti o per effettuare verifiche campionarie, oppure verifiche a sorpresa specialmente nell'ambito di attività più sensibili. Nondimeno assumono rilievo i controlli finalizzati alla prevenzione e al presidio dei rischi inerenti ai reati di natura colposa (sicurezza nei luoghi di lavoro). Per altro verso, ai fini del presidio del reato di riciclaggio l'OdV dispone, tra le altre, a titolo di esempio, verifiche sulla materialità dei questionari di adeguata verifica della clientela, al fine di evitare che gli operatori ai vari livelli possano agevolare condotte non consentite alla clientela: la questione assume rilievo perché se da un lato il sistema informativo non consente alcun tipo di operatività prima della compilazione del questionario, dall'altro solo la verifica della materialità del questionario, dove dovrà essere verificata quantomeno la presenza della firma del cliente, potrà consentire il corretto presidio. Parimenti, ai fini del medesimo rischio controlli campionari potranno consentire di accertare difformità nell'attribuzione di profili di rischio di riciclaggio a ciascun cliente nei casi di cointestazioni di rapporti.

Tali attività consentono:

- al potenziale autore del reato di avere piena consapevolezza sia delle fattispecie a rischio di commissione di un illecito, sia della riprovazione della Banca nei confronti di tali condotte, ritenute contrarie agli interessi aziendali anche quando apparentemente la società potrebbe trarne un vantaggio;
- alla Banca di reagire tempestivamente per prevenire e/o impedire la commissione del reato stesso, grazie ad un monitoraggio costante delle attività.

IL SISTEMA DELLE SEGNALAZIONI

Come spiegato nella parte generale del presente documento, l'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231 prevede l'implementazione di adeguati canali informativi che consentano ai segnalanti di "*presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti*".

L'attivazione di tali procedure di segnalazione nel sistema organizzativo della Banca, con la logica intesa a incentivare le denunce ed a favorire il distacco individuale e la sana disobbedienza civile dei lavoratori contro prassi distorte imposte da colleghi e superiori, viene favorita per creare conflitti di interesse interni che portino i dirigenti, i quadri ed il personale tutto a denunciare forme di corruttela o di malaffare che eventualmente dovessero verificarsi nell'ambito aziendale.

Per quanto di interesse, di seguito si riporta lo schema riepilogativo dei processi esistenti in Banca nel cui ambito è prevista - per disposizione legislativa - l'applicazione della norma sul whistleblowing.

Materia/ambito di riferimento	Provvedimento	Ambito	Data di entrata in vigore
Linee Guida Anac	DETERMINAZIONE N. 6 DEL 28/04/2015	PUBBLICA AMMINISTRAZIONE	28/04/2015
Borsa italiana	ART. 7 - CODICE INTERNO DIAUTODISCIPLINA	SOCIETÀ QUOTATE	luglio 2015
Testo Unico Bancario	ART. 52-*BIS*	ATTIVITÀ BANCARIA	01/01/2016
Antiriciclaggio	ART. 48 - D.lgs. 25/05/2017, n. 90	ANTIRICICLAGGIO	04/07/2017
231/01	ART 2 - L. 30/11/2017, n. 179	REATI PRESUPPOSTO 231	29/12/2017
Testo Unico Finanza	ART. 4-UNDECIES	SERVIZI DI INVESTIMENTO IMPRESE ASSICURATIVE E MARKET ABUSE	03/01/2018

A fattor comune, si rappresenta peraltro che già nel D.Lgs. n. 81/2008 art. 20 è previsto che i lavoratori debbano "*segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi (...), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza*".

In Banca, in ottemperanza alla policy del GBCI, il destinatario delle segnalazioni per la ricezione, l'esame e la valutazione delle segnalazioni è il Comitato Sistemi Interni di Segnalazioni delle Violazioni, nominato dal Consiglio di Amministrazione della Banca ed è composto da:

- responsabile Internal Audit BCC, che è anche il responsabile del Comitato;
- Responsabile della Funzione Conformità della BCC;
- Responsabile Antiriciclaggio della BCC;
- Responsabile Risk Management della BCC.

Sono comunque previsti meccanismi di escalation nel caso di segnalazioni dei confronti dei membri del Comitato tramite la costituzione di apposite "funzioni di riserva" come disciplinato nella relativa Politica.

Qualora la segnalazione riguardi anche solo uno dei quattro membri del Comitato sia presunto responsabile o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità e l'indipendenza del giudizio la stessa dovrà essere indirizzata al Consigliere con delega al sistema dei controlli interni (o Comitato Rischi qualora istituito) della BCC.

Qualora, invece, la segnalazione riguardi il Direttore Generale o un membro degli Organi Aziendali della BCC, la stessa dovrà essere indirizzata al Comitato Sistemi Interni di Segnalazione delle Violazioni istituito presso la Capogruppo.

Tutti i membri del Comitato/ Consigliere con delega al sistema dei controlli interni (o Comitato Rischi qualora istituito) hanno l'obbligo di garantire la confidenzialità e riservatezza delle informazioni ricevute/ trattate in linea con quanto previsto dalla normativa vigente e nel rispetto della normativa in materia di trattamento dei dati personali.

Per quanto di specifico interesse, nella predetta policy viene precisato che qualora la segnalazione sia relativa a presunte violazioni riferibili ai reati di cui al D.Lgs. 231/01, la stessa viene indirizzata dal Comitato all'Organismo di Vigilanza 231/01 della banca, informandolo della fattispecie e degli esiti dell'attività istruttoria.

Sul punto, considerato che l'evento informativo previsto nella policy si attiverebbe solo nel caso di segnalazioni, ritenuto in fatto che il presente MOG si prefigge lo scopo di prevenire/presidiare eventi-reato e che tutte le segnalazioni hanno una sistematica e oggettiva attinenza a rischi di incorrere nella responsabilità penale del Decreto 231, si ritiene fondamentale che l'OdV venga sempre informato in merito a tutte le segnalazioni prodotte da cui eventualmente trarre opportune valutazioni al fine di proporre eventuali adeguamenti organizzativi per prevenire possibili ipotesi di reato. Per tali finalità, l'OdV si avvarrà dei flussi informativi acquisiti in seno ai CdA cui formalmente partecipa in quanto Collegio Sindacale.

Nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali, il Responsabile dei Sistemi Interni di Segnalazione delle violazioni della Banca redige una relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione delle violazioni, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute. Tale relazione comprende altresì le segnalazioni che hanno coinvolto il Direttore Generale e i membri degli Organi Aziendali.

Per le medesime finalità vengono previsti appositi contratti di prestazione di servizi volti a disciplinare i rapporti tra la holding e le controllate, che tengono conto delle attività che possono presentare rischi di commissione di reati rilevanti per la responsabilità amministrativa ex D.lgs. 231/2001. In coerenza con il contesto delineato, è quindi prassi che capogruppo prevede nei propri Modelli la possibilità di impartire criteri e direttive di carattere generale verso banca, nonché di verificare - normalmente tramite le funzioni di controllo e/o di governo accentrato - la rispondenza del Modello alle policy, regolamenti e procedure definite dalla stessa. D'altra parte, in termini di flussi informativi, frequentemente i Modelli 231 dei gruppi bancari prevedono la trasmissione alla capogruppo di report periodici, in relazione ad argomenti connessi al D.lgs. 231/2001.

Sono altrettanti utili e funzionali interventi di sensibilizzazione e formazione degli esponenti della capogruppo, al fine di stimolare una particolare attenzione ai processi nei quali sono chiamati a intervenire congiuntamente a esponenti della banca, rendendo consapevoli i primi della delicatezza di quanto è a loro richiesto quando si trovino ad agire in un ambito procedimentale condiviso. Centrale risulta in quest'ottica la previsione già consolidata dei flussi informativi infragruppo e delle attività di monitoring e warning, volte a coordinare le attività e la prevenzione dei rischi.

Ciò vale a maggior ragione con riferimento ai presidi già richiamati nella parte generale, quali fattori chiave del "rischio di risalita".

Inoltre, con riferimento al sistema di segnalazione, si evidenzia quanto di seguito specificato.

1) Su tale istituto giuridico Banca d'Italia ha attivato due canali telematici denominati "*Segnalazione Whistleblowing"* e "*Segnalazione Aziendale*", dedicati alla ricezione delle segnalazioni predisposte da differenti soggetti ed aventi per contenuto esclusivamente le possibili violazioni normative o le presunte irregolarità gestionali riscontrate presso gli intermediari vigilati[3].

[3] Cfr. Nota di Banca d'Italia del 2 maggio 2018

La piattaforma "*Segnalazione Whistleblowing"* può essere dai dipendenti o collaboratori di una banca o di un altro soggetto vigilato per segnalare le violazioni normative riguardanti le norme del titolo II e III del Testo Unico Bancario. In particolare, come indicazione, si può fare riferimento alla segnalazione di atti o fatti che costituiscono una violazione delle norme disciplinanti l'attività bancaria ai sensi dell'Articolo 10, commi 1, 2 e 3 del TUB[4]. Nell'ottica di quanto previsto dalle disposizioni legislative in materia (art. 52-ter del TUB, art. 4-duodecies del TUF e legge n. 179 del 2017), Banca d'Italia assicura la riservatezza dei dati personali del segnalante al fine di tutelare quest'ultimo da possibili ritorsioni.

Invece, la piattaforma "*Segnalazione Aziendale*" può essere utilizzata da coloro che non siano dipendenti o collaboratori di soggetti vigilati dalla Banca d'Italia per presentare una segnalazione su possibili violazioni della normativa o presunte anomalie gestionali riscontrate presso tali intermediari.

2) Rileva, altresì, il servizio tesoreria enti che la Banca svolge per conto di numerosi Comuni e il servizio di cassa per altrettanti istituti scolastici operanti nel territorio di competenza. Al riguardo si fa osservare che l'articolo 54-bis del decreto legislativo 30 marzo 2001, n. 165, come modificato dall'articolo 1 della legge 30 novembre 2017, n. 179 (Tutela del dipendente pubblico che segnala illeciti al responsabile della prevenzione della corruzione e della trasparenza o all'Autorità nazionale anticorruzione (ANAC), al comma 2 prevede che "*La disciplina di cui al presente articolo si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica*". Ne consegue che la Banca è esposta anche alle eventuali segnalazioni o comunicazioni inoltrate all'ANAC attinenti a questioni con la pubblica amministrazione.

Il successivo comma 4 precisa, inoltre, che la segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

L'ANAC, alla quale è affidato anche il potere sanzionatorio disciplinato con Delibera 30/10/2018 (GU 19/11/2018), ha disposto che le comunicazioni e le segnalazioni sono presentate, di norma, attraverso il modulo della piattaforma informatica disponibile sul sito istituzionale dell'Autorità, che utilizza strumenti di crittografia e garantisce la riservatezza dell'identità del segnalante e del contenuto della segnalazione nonché della relativa documentazione.

[4] Cfr Circolare 285 del 17 dicembre 2013, 11° aggiornamento. Titolo IV, Capitolo 3, Sezione VIII

Rinviando al documento di policy e al Regolamento interno ed al manuale utente rilasciato da BCC SI con riferimento all'applicativo informatico, si riportano di seguito alcune indicazioni che devono essere osservate e che sintetizzano i punti chiave della procedura:

a) OGGETTO DELLE SEGNALAZIONI

I dipendenti devono segnalare direttamente all'OdV, **a tutela dell'integrità della Banca**, solo illeciti rilevanti ai fini del D.Lgs. 231/2001 e quindi commessi nell'interesse o a vantaggio della banca medesima, ovvero violazioni del presente modello di organizzazione, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

La segnalazione potrà riguardare sia violazioni di legge, sia comportamenti contrari a regole interne, codice etico, regolamenti e, pertanto, dovranno essere comunicati fatti integranti reati, illeciti, comportamenti a danno della banca, abusi di potere

Tutte le rimanenti segnalazioni, funzionali ai processi diversi da quelli sopra descritti seguono le regole indicate nel regolamento generale sul whistleblowing e nelle eventuali specifiche disposizioni di servizio nel tempo diramate.

b) LA RICEZIONE DELLE SEGNALAZIONI

Le procedure interne disciplinano le modalità di gestione delle segnalazioni, identificando le funzioni aziendali competenti a procedere, con la dovuta autonomia e indipendenza, alle attività di analisi e di indagine.

c) FORMA E CONTENUTO

Le segnalazioni - specialmente quelle anonime ove consentite - devono essere circostanziate e fondate su fatti precisi e concordanti.

d) LE INVESTIGAZIONI

Le investigazioni possono essere svolte dall'OdV, da eventuale professionista esterno, da una funzione di controllo aziendale o ispettorato, al fine di verificarne la fondatezza e nel cui ambito possono essere avanzate richieste di chiarimenti al whistleblower.

e) LE TUTELE DEL SEGNALANTE

Ferma restando la protezione legale di cui il whistleblower gode, le procedure interne prevedono meccanismo di controllo preventivo sulle finalità e motivazioni delle iniziative aziendali nei suoi confronti. Sul punto si evidenzia che il profilo della riservatezza dell'identità del segnalante è diverso da quello dell'anonimato. Anche l'Autorità Nazionale Anticorruzione chiarisce che il primo presuppone la rivelazione della propria identità da parte del denunciante che, infatti, può godere

di una tutela adeguata soltanto se si rende riconoscibile (v. Determinazione ANAC n. 6 del 28 aprile 2015 – "Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti").

Invece, nel caso di segnalazione anonima, considerato che tale ipotesi rende più complessa la verifica della fondatezza della denuncia, per contenere il rischio di alimentare denunce infondate e mere doglianze che hanno poco a che fare con la tutela dell'integrità dell'ente, è necessario rafforzare il fondamento della denuncia. Pertanto, è previsto che la denuncia anonima deve essere documentata adeguatamente ovvero che sia resa con dovizia di particolari e in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

f) IL CODICE DISCIPLINARE

Il codice disciplinare aziendale prevede sanzioni sia per chi viola le tutele del segnalante e sia per colui che presenti una segnalazione infondata per dolo o colpa grave. A tal fine, l'Organismo di Vigilanza effettua controlli sia sul rispetto del divieto di atti ritorsivi o discriminatori, sia sulle eventuali violazioni sopra indicate e, nel caso in cui dovesse verificare l'eventuale violazione di tali precetti provvederà a segnalarle al Consiglio di Amministrazione così che possano essere disposte le sanzioni proporzionate alla violazione. Per il dettaglio si rinvia al Codice aziendale di comportamento.

g) LE DISPOSIZIONI IN MATERIA LAVORISTICA

Ferme restando le disposizioni previste dall'articolo 54-bis del Decreto Legislativo 30 marzo 2001 n. 165, ai sensi dell'articolo 6 comma 2-ter del D.Lgs. 231/2001, il segnalante e l'organizzazione sindacale di riferimento possono denunciare all'Ispettorato Nazionale del Lavoro le misure discriminatorie eventualmente adottate dall'ente.

Ai sensi dell'articolo 6 comma 2-quater, sono ritenute nulle le misure ritorsive o discriminatorie, compresi il licenziamento e il mutamento di mansioni, assunte nei confronti del soggetto segnalante in una fase successiva alla denuncia.

Sul punto si evidenzia che, nel caso di controversie legate all'irrogazione di sanzioni disciplinari o all'adozione di misure organizzative, con effetti negativi sulle condizioni di lavoro del segnalante (demansionamenti; licenziamenti; trasferimenti), il datore di lavoro ha l'onere di dimostrare che esse sono fondate su ragioni estranee alla segnalazione stessa.

LA SEGRETERIA TECNICA

Al fine di garantire l'efficacia del Modello, è istituita una Segreteria Tecnica, di tipo interfunzionale che non svolge attività collegiale, dove i componenti garantiscono – sulla base delle rispettive competenze e responsabilità - continuità di azione, nonché l'attivazione e la verifica del rispetto dei protocolli e dei presidi riportati nel presente modello, ancorché fornire supporto all'OdV, poiché rappresentano il fulcro organizzativo delle attività svolte nell'ambito dei processi sensibili.

La Segreteria[5] è composta dai responsabili pro tempore delle funzioni aziendali che il C.d.A. della Banca ha formalmente designato nell'incarico di:

1) Direttore Generale, in quanto capo del personale ed esclusivamente per gli aspetti inerenti a tale funzione[6];
2) Vicedirettore Generale, anche in quanto responsabile/coordinatore di specifiche aree;
3) Responsabile della Funzione Organizzazione
4) Incaricato all'Ufficio Controlli Interni
5) Responsabile dell'Ufficio Legale e Contenzioso;
6) Responsabile del Servizio Finanza;
7) Responsabile dell'Area Crediti;
8) Responsabile della Segreteria Generale;
9) Responsabile dell'Ufficio tesoreria enti;
10) Responsabile della Direzione Marketing;
11) Responsabile del servizio monitoraggio crediti e gestione NPLs
12) Responsabile del Settore Infrastrutture e Spese, Economato e servizi ausiliari,
13) Responsabile di area territoriale, limitatamente all'area di competenza,

poiché risultano essere quelle funzioni aziendali che:

- hanno elevata conoscenza dei processi e possono assicurare e garantire un processo di formazione e attuazione delle decisioni chiaro, trasparente e competente;
- possono facilmente monitorare la funzionalità del Modello, nonché consentire/proporre gli eventuali adeguamenti necessari.

In base alle indicazioni ed alle risultanze delle analisi dei rischi – anche da parte dell'OdV - ciascuna delle suindicate funzioni aziendali elabora ed implementa, per la parte di competenza, le

[5] I componenti della segreteria Tecnica in gran parte sono anche componenti del Comitato di direzione/rischi.

[6] Per le rimanenti attività il Direttore Generale svolge ruolo proattivo ai fini della puntuale e corretta attuazione dei protocolli e dei presidi, essendo beneficiario di tutti i flussi informativi in quanto a capo dell'intera struttura ed in quanto partecipante al Consiglio di Amministrazione.

procedure aziendali relative alle aree di attività a rischio, anche ad integrazione di procedure già esistenti.

Più in particolare, la Segreteria Tecnica, attraverso i suoi componenti, inoltre:

1) redige ed invia flussi informativi all'Organismo di Vigilanza, per le diverse aree di attività a rischio, tenendo anche conto di quanto previsto nel Regolamento dei flussi informativi in vigore.
2) assicura il rispetto delle procedure, garantendo anche il sistema di tracciabilità dell'intero processo, secondo cui ogni operazione deve essere munita di adeguato supporto documentale;
3) redige e aggiorna le procedure ed altre tipologie documentali correlate alle attività a rischio, prevedendo un adeguato sistema di controllo;
4) con riferimento al rischio reato, propone all'OdV, eventuali aggiornamenti dei processi sensibili e miglioramenti al sistema di controllo interno;
5) promuove la diffusione e la conoscenza del Modello e del Codice Etico anche mediante l'identificazione dei fabbisogni formativi e informativi.

Nel caso in cui l'estensione del processo presidiato e la complessità delle operazioni lo richiedano, i singoli componenti della Segreteria Tecnica potranno attribuire, in coerenza con i processi e le responsabilità organizzative aziendali, parte delle proprie competenze a una o più Sub-Funzione, che saranno corresponsabili delle operazioni svolte relativamente alla parte di processo assegnata.

Tale attribuzione sarà coordinata preventivamente anche con l'OdV.

Qualora la gestione del processo, ferma restando la sua unitarietà, in considerazione di particolari esigenze aziendali, preveda la delega di specifiche attività e l'attribuzione delle conseguenti responsabilità a Funzioni aziendali diverse da quella di riferimento, il Direttore Generale, previo coordinamento con l'OdV, potrà proporre al CdA la nomina di distinti Sub Responsabili Delegati a cui affidare con responsabilità autonoma, in tutto o in parte, le competenze della Funzione primaria relativamente alla gestione delle attività oggetto di delega.

PARTE II

L'ANALISI DEI RISCHI E I PRESIDI ORGANIZZATIVI E GESTIONALI

Appare fondamentale rappresentare in premessa alcune peculiarità che risultano essere prodromiche alla valutazione dei rischi ed ai conseguenti presidi organizzativi e gestionali.

L'attività bancaria secondo l'ordinamento italiano è l'esercizio congiunto dell'attività di raccolta di risparmio tra il pubblico e l'attività di concessione del credito.

L'art. 1, c. 2, del Decreto stabilisce che le disposizioni del corpus normativo "*si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica*". Nessun dubbio, quindi, che le disposizioni di cui al d.lgs. n. 231/2001 si applichino alla BCC di Buccino e dei Comuni Cilentani, anche in quanto intermediario finanziario ed assicurativo.

La peculiarità della banca, infatti, è costituita dal fitto e specifico apparato normativo riferibile a ciascuna delle categorie citate, le quali, operando in ambiti di interesse collettivo pregnante, sono soggette di per sé ad una rete di controlli interni ed esterni: ci si riferisce, segnatamente, alle previsioni del Testo unico delle leggi in materia bancaria e creditizia (d.lgs. 1.9.1993, n. 385); del Testo unico delle disposizioni in materia di intermediazione finanziaria (d.lgs. 24.2.1998, n. 58),; del Codice delle assicurazioni private (d.lgs. 7.9.2005, n. 20.).

Per chiarire il concetto, ad esempio, l'Autorità di vigilanza ha creato un sistema integrato di controlli che permea l'intera attività aziendale e coinvolge soggetti diversi, a significare che nel caso di specie trattasi evidentemente di persona giuridica tra le più normate e controllate.

In tale prospettiva, gli artt. 97-bis TUB, 60-bis TUF e 266 cod. ass., prevedono rispettivamente una disciplina speciale e derogatoria rispetto alle norme generali in materia di responsabilità amministrativa delle persone giuridiche, volta - da un lato - a conferire un ruolo particolare alle rispettive Autorità di Vigilanza sia nella fase delle indagini, che in quella dibattimentale, che in quella esecutiva; - dall'altro - a delimitare l'incidenza delle sanzioni e misure interdittive nei settori specifici che ci occupano.

Preme sin da ora evidenziare che tali Autorità non sono parte del procedimento penale-amministrativo, bensì svolgono un ruolo di informativa.

Tali "modelli atipici" derivano dalla esigenza di coordinare il d.lgs. n. 231/2001 con la disciplina dettata nella sede propria, come espressamente previsto dal d.lgs. n. 197/2004 attuativo della Direttiva n.2001/24/CE il cui capo II è per l'appunto rubricato "*Coordinamento del testo unico bancario e del testo unico della finanza con il decreto legislativo 8 giugno 2001, n. 231*".

La ratio sottostante va rinvenuta nel dichiarato fine di "*assicurare le preminenti finalità di salvaguardia della stabilità del sistema bancario e finanziario e di tutela dei diritti dei depositanti e degli investitori*" (così, l'art. 29, lett. e), l. 3.2.2003 n. 14 recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2002").

Le norme citate prevedono una sorta di "partecipazione necessaria" delle Autorità di Vigilanza al procedimento, che si esplica - per quanto attiene la fase delle indagini preliminari:

(i) nell'obbligo gravante sul Pubblico Ministero di comunicare all'Autorità di Vigilanza l'avvenuta iscrizione nel registro delle notizie di reato di un illecito amministrativo a carico di una banca (art. 97-bis TUB),

(ii) la possibilità per il titolare delle indagini di sentire le Autorità di Vigilanza,

(iii) la facoltà in capo alle medesime di presentare relazioni scritte.

La ratio di tale previsione è consentire all'Autorità di Vigilanza di esercitare i propri poteri di vigilanza ispettiva, informativa e regolamentare sin dall'avvio del procedimento a carico delle persone giuridiche. Il PM è, infatti, tenuto a dare comunicazione alle Autorità di Vigilanza in merito all'iscrizione di qualsivoglia illecito amministrativo, ivi comprese, quindi, ipotesi estranee alla specifica area di competenza delle medesime (si pensi, ad esempio all'illecito di cui all'art. 25-septies, d.lgs. n. 231/2001 in combinato con l'art. 589 o 590 c.p.).

Ad ulteriore sostegno della rilevanza dell'apporto conoscitivo delle Autorità di Vigilanza è prevista l'acquisizione "*in ogni grado del processo di merito, prima della sentenza" di una sorta di parere tecnico rilasciato dalle authorities, il cui contenuto è identificato dalla normativa in "aggiornate informazioni sulla situazione della banca con particolare riguardo alla struttura organizzativa e di controllo*".

Quanto alla natura di tali atti, così come per le relazioni scritte, la giurisprudenza va inquadrata nella categoria della prova documentale e non può, tuttavia, ignorarsi che il contenuto di tali documenti che le aggiornate informazioni sulla struttura organizzativa e di controllo non possono che tradursi in un parere sull'idoneità del modello organizzativo adottato.

Le norme di settore sopra citate ritagliano un ulteriore importante ruolo all'Autorità di Vigilanza, prevedendo che la sentenza irrevocabile che irroga nei confronti delle banche è trasmessa a Banca d'Italia che può "proporre o adottare" le misure previste dal TUB per la disciplina delle crisi o quelle di risanamento, che deve anche salvaguardare la stabilità e la tutela dei diritti" di depositanti, clienti, investitori. Quindi, Banca d'Italia – nel caso di specie - dispone dei poteri di

sospendere gli organi gestori degli enti e nominare uno o più commissari operanti sotto il suo diretto controllo.

In linea generale possiamo, dunque, affermare che la regolamentazione interna viene periodicamente aggiornata in ragione di nuove norme e/o di nuovi presidi che vengono di volta in volta individuati ed attuati alla luce della nuova normativa che interviene.

Avuto riguardo a quanto sopra esposto, vengono riportati di seguito i risultati dell'analisi dei rischi suddivisi per ciascuna tipologia di reato, con l'evidenza dei principali e specifici presidi organizzativi e gestionali.

Per il dettaglio, sia ai fini dell'analisi che dei presidi, si fa rinvio anche a specifici protocolli riportati nel seguito del presente documento, modificabili e manutenuti da eventuale incaricato nominativamente individuato.

A fattor comune, a presidio dei rischi nell'ambito delle FOI, delle attività esternalizzate e di taluni presidi specialistici, connesse ad aree sensibili a rischio reato, la responsabilità viene ricondotta nelle seguenti U.O., parte delle quali anche componenti della Segreteria Tecnica più avanti descritta:

- Responsabile della Direzione Marketing quale referente della Sicurezza sui luoghi di lavoro (D.Lgs. *81/08)*;
- Responsabile della Segreteria Fidi quale Referente locale Anagrafe (RL);
- Responsabile del Monitoraggio Crediti Npls, quale Referente unico Project DAC 6 (sullo scambio automatico obbligatorio di informazioni relative a meccanismi transfrontalieri che presentano determinati rischi di elusione o evasione);
- Responsabile XXXXXXX quale:
  - *Referente della Funzione Reclami e Conciliatore Bancario e Finanziario e*
  - *Referente SIAR (Segnalazioni Infrazioni Anti Riciclaggio)*
- Responsabile dell'Ufficio Organizzazione, quale:
  - *Referente per le Funzioni Operative Importanti (FOI) esternalizzate con la Capogruppo ICCREA;*
  - *Referente Privacy e Protezione Dati (RPD);*
  - *Rappresentante BCC per la partecipazione al Comitato Utenti istituito dalla BCC Sistemi Informatici;*
  - *Referente Oro, ovvero per la dichiarazione di operazioni in oro per le quali vige l'obbligo di dare comunicazione alla UIF (Unità di Informazione Finanziaria per l'Italia);*
  - *Referente e Responsabile del Piano di Continuità Operativa.*
  - *Sovraintendente all'ufficio Controlli interni.*

- Responsabile del Settore Bancassurrance, quale:
  - *Referente del contratto di esternalizzazione (RAE) con la Capogruppo, nell'ambito del conferimento della delega a Iccrea Banca per assolvere all'obbligo di segnalazione di cui al Regolamento (UE) 2015/2365 (c.d. SFTR);*
  - *Responsabile Attività della Distribuzione Assicurativa (RADA).*
- Responsabile dell'Ufficio Contabilità generale e segnalazioni, quale:
  - *Funzione Segnalazione di Vigilanza;*
  - *Referente Unico Consulente Fiscale;*
  - *Referente Assistenza fiscale e Adempimenti Fiscali.*
- Vicedirettore Generale, formalmente designato nel ruolo di:
  - *Local Data Manager (LDM) per una corretta gestione del patrimonio informativo e per garantire il costante miglioramento della qualità dei dati e l'integrità delle informazioni prodotte;*
  - *Tutor Aziendale della formazione del personale dipendente;*
- Responsabile dell'Ufficio pianificazione e controllo di gestione, quale:
  - *Referente Gestione delle Verifiche Tributarie, del Pre-Contenzioso, del Contenzioso Tributario e delle Istanze di Interpello.*
  - *Referente Operativo Locale (ROL) del Single Customer View (SCV), ovvero "Singola Visione del Cliente";*
  - *Referente (DCNF) per la Dichiarazione Consolidata non Finanziaria.*
- Responsabile dell'Area Operativa, quale:
  - *Referente per le Attività Esternalizzate (RAE) con la Capogruppo ICCREA, ovvero per i servizi:*
    - *gestione delle verifiche tributarie, del precontenzioso, del contenzioso tributario e delle istanze di interpello;*
    - *verifiche di Compliance e Consulenza su nuovi prodotti/servizi;*
    - *Consulenza, Assistenza e Adempimenti fiscali.*
  - *Referente Sostituto Locale (sostituto del ROL) del Single Customer View (SCV), ovvero "Singola Visione del Cliente";*
- Incaricato periferico di Iccrea Banca S.p.A., quale Referente DPO (Data Protection Officer)
- Addetto al Servizio Finanza, quale Referente Unico per la salvaguardia degli strumenti finanziari e delle disponibilità liquide dei clienti;
- Responsabile dell'Ufficio Incassi e Pagamenti, quale:

- *Referente "PSD2 – Obblighi di segnalazione per i dati sulle frodi" e*
- *Responsabile della gestione della Cassa Centralizzata per i valori in bianco*

- Responsabile dell'Ufficio Tecnologie e sistemi informatici e Security Manager, quale incaricato della funzione di Incident Manager (gestione degli incidenti e di framework di continuità operativa);
- I responsabili e gli addetti alle segnalazioni rispettivamente dell'Unità Legale e dell'Unità Contabilità e Segnalazioni di Bilancio, quali referenti per l'applicazione della Politica di Gruppo "LOSS DATA COLLECTION"

SPECIFICI PROTOCOLLI PER I REATI PRESUPPOSTO

I Protocolli definiscono i presidi e le regole di comportamento cui sono assoggettati coloro i quali operano nelle aree aziendali "mappate" come "sensibili".

Si ricorda con il termine protocollo e/o procedura si intende "*un insieme di principi, situazioni, meccanismi organizzativi e operativi di comportamento che é funzionale alla gestione del rischio-reato, nel senso che la sua corretta applicazione, anche in combinazione con altri protocolli e/o procedure, é tale da prevenire la commissione del reato da cui sorge la responsabilità ex d. lgsl. 231/2001*".

Per ciascuna tipologia di reato-presupposto censita vengono fissate regole comportamentali (positive o negative) cui i soggetti indicati sono vincolati, nonché vengono adottati presidi e strumenti di controllo e prevenzione.

Le prescrizioni si raccordano con le best practices del settore bancario ed i sistemi di controllo adottati dal GBCI, nonché dalla normativa interna, ancorché aventi una finalità non specificamente di prevenzione ex d.lgs. n. 231/2001.

A fattor comune si richiamano, in quanto da considerarsi protocolli specifici in riferimento al presidio di tutti i reati previsti nel catalogo, le seguenti policy emanate dal GBCI, con i rispettivi aggiornamenti:

1) Politica in materia di Risk Appetite Framework
2) Linee di indirizzo e coordinamento in materia di derivati OTC
3) Direttiva di indirizzo e coordinamento in materia di fondi prontamente disponibili e conseguenti esercizi di stress test
4) Direttiva circa le modalità di relazione con le Autorità di Vigilanza
5) Politica in materia di gestione degli incidenti
6) Politica in materia di sicurezza delle informazioni e dei rischi ICT

7) Politica di idoneità degli esponenti
8) Direttiva di coordinamento delle funzioni aziendali di controllo e flussi informativi
9) Dichiarazione consolidata non finanziaria
10) Direttiva in materia di apertura, chiusura e trasferimento delle filiali
11) Direttiva in materia di Market Risk tesa a disciplinare il complessivo framework di governo dei rischi di mercato
12) Direttiva sul regolamento delle assemblee territoriali
13) Policy per l'IT Risk Management, Self-Assessment
14) Policy di loss data collection
15) Policy per la gestione dei client condivisi
16) Direttiva in materia di Gruppo IVA in quanto soggetto passivo d'imposta collettivo
17) Politica in materia di gestione degli interventi sulle banche in regime di gestione controllata
18) Policy IRBB
19) Comunicazione di indirizzo e coordinamento in materia di decisioni di politica monetaria e strategia finanziaria
20) Manuale Contabile dei Principi Contabili e delle politiche contabili in materia di "*Consolidamento delle entità strutturate*"; "*Fondi rischi e oneri – costi legali*"; "*Attività materiali rivenienti dall'escussione di garanzie*"; "*Attività immateriali generate internamente*"; "*Operazioni di aggregazione tra entità sotto controllo comune*",
21) Politica di gestione del piano dei conti unico di Gruppo.
22) Politica fiscale
23) Politica di assetto delle funzioni aziendali di controllo
24) Politica per la gestione della continuità operativa
25) Politica per la gestione del rischio di non conformità alle norme
26) Politica in materia di conflitti di interesse nella prestazione dei servizi di investimento
27) Politica in materia di data governance
28) Politica di esternalizzazione e servizi ICT critici
29) Politica in materia di formazione assicurativa
30) Politica in materia di gestione e formazione del personale addetto ai servizi di investimento
31) Politica in materia di anagrafe di gruppo
32) Politica in materia di operazioni di maggior rilievo
33) Politica relativa al framework di Operational Risk Management
34) Politica sulla gestione delle partecipazioni
35) Politica di Product Management
36) Politica in materia di classification e Misurement ed impairment (IFRS9)

37) Politica in materia di early warning system
38) Politica di remunerazione e incentivazione
39) Politica in materia di incarichi a revisori legali o a società di revisione
40) Politica AML e Politica su Adeguata verifica della clientela a fini AML
41) Regolamento di gruppo e di governo societario

Costituiscono, altresì, protocolli specifici tutti i regolamenti e gli ordini di servizio autonomamente diramati dalla Banca tempo per tempo.

FLUSSI PERIODICI PER L'ODV 231

Al fine di rendere effettivo l'esercizio delle sue funzioni, l'Organismo di Vigilanza deve poter essere informato in merito a fatti od eventi che potrebbero ingenerare responsabilità della Banca ai sensi del D.Lgs. n. 231/2001. È necessario che sia definito ed attuato un costante scambio di informazioni tra i destinatari del Modello 231 e l'OdV stesso.

In particolare, nel Modello 231 adottato vengono individuate due tipologie di flussi informativi diretti all'OdV:

1) SEGNALAZIONI, da inviare in caso di rilevazione di gravi comportamenti illegali (frode, corruzione, etc.) o più in generale di comportamenti non corretti nella conduzione del lavoro e degli affari in violazione del Modello 231.

   Tutti soggetti coinvolti nelle attività sensibili sono, infatti, tenuti a segnalare tempestivamente all'OdV, tramite i canali informativi specificamente identificati:

   - violazioni di leggi e norme applicabili;
   - violazioni, conclamate o sospette, del Modello o delle procedure ad esso correlate o degli elementi che lo compongono;
   - comportamenti e/o pratiche non in linea con le disposizioni del Codice Etico e delle Policy adottate;
   - eventuali deroghe alle procedure decise in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.

2) FLUSSI INFORMATIVI PERIODICI, richiesti dall'ODV alle singole Funzioni aziendali coinvolte nelle attività a rischio, relativi alle notizie rilevanti ed alle eventuali criticità individuate nell'ambito dell'area aziendale di appartenenza, al fine di consentire all'Organismo stesso di monitorare l'insorgenza di attività sensibili, il funzionamento e l'osservanza del Modello nella gestione degli adempimenti dichiarativi periodici e calcolo imposte.

PARTE III

IL CATALOGO DEI REATI – Le regole ed i protocolli

Reati commessi nei rapporti con la pubblica amministrazione

Il decreto legislativo n.75 del 14 luglio 2020, oltre che ad apportare modifiche al codice penale, in ottemperanza ai criteri di armonizzazione della legislazione degli Stati membri come previsto dalla cd direttiva PIF, è intervenuto anche sulla responsabilità amministrativa da reato delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, apportando numerose modifiche al D. lgs. 231 dell'8 giugno 2001.

In particolare, rispetto ai delitti contro la pubblica amministrazione, sono state inserite nuove fattispecie di reato quali peculato, abuso di ufficio e frode nelle forniture; inasprite le sanzioni in caso di mancata adozione, presidio del modello di gestione, organizzazione e controllo previsto dalla normativa di riferimento.

In particolare, il catalogo dei reati presupposto è stato integrato, come già anticipato, con il reato di frode nelle pubbliche forniture (356 c.p.) e con il reato di appropriazione indebita o distrazione di fondi comunitari, commesso da chi "*mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale*" [7].

Rispetto a tali novità occorre osservare che la disposizione che amplia il novero dei reati presupposto di responsabilità amministrativa degli enti, inserendovi i reati di peculato, peculato per profitto dell'errore altrui e abuso d'ufficio (non specificando che deve trattarsi di fattispecie lesive degli interessi finanziari dell'Unione) andrebbe valutata alla luce della disposizione di delega che si limita a prescrivere al Governo di integrare la disciplina della responsabilità amministrativa degli enti con riguardo ai soli reati che ledono gli interessi finanziari dell'Unione europea.

Ampliando il punto di osservazione, fatta salva la discriminante dei nuovi reati inseriti che potranno essere vagliati sulla base della lesione degli interessi finanziari dell'Unione, appare comunque opportuno promuovere l'aggiornamento del MOG in un'accezione più estesa, al fine di monitorare tutti i processi aziendali in cui sia prevedibile la concretizzazione di una tale condotta (verosimilmente tutti quelli che prevedono un contatto diretto o indiretto con pubblici ufficiali o

[7] Articolo 2 della Legge 898/1986 in materia di aiuti comunitari al settore agricolo.

incaricati di un pubblico servizio) e strutturarsi, più in generale, secondo un sistema idoneo a prevenire la commissione dei reati presupposto.

Articolo 24 - Reati di malversazione e indebita percezione di erogazioni[8]:

- *Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture*

e Articolo 25 - Concussione, induzione indebita a dare o promettere utilità e corruzione:

- *Concussione (art. 317 c.p.)*[9]*, Induzione indebita a dare o promettere utilità (art. 319-quater)* [10] *, Corruzione per l'esercizio della funzione (art. 318 c.p.)*[11]*, Corruzione per un atto contrario ai doveri d'ufficio e circostanze aggravanti (artt. 319 e 319 bis c.p.)*[12]*, Corruzione in atti giudiziari (art. 319-ter c.p.)* [13]*, Corruzione di persona incaricata di un pubblico servizio (320 c.p.), Istigazione alla corruzione (art. 322), Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle C.E. e di funzionari delle C.E. e di Stati esteri (art. 322 bis c.p.)*[14]*, Traffico di influenze (art. 346-bis)* [15]

La natura imprenditoriale della Banca e il suo ruolo istituzionale comportano l'esigenza di instaurare e tenere più o meno in via continuativa relazioni e rapporti con molteplici soggetti pubblici, tra cui a titolo di esemplo: l'Agenzia delle Entrate, i Comuni ed altri enti pubblici locali, BCE, Banca d'Italia, CONSOB, U.I.F., l'INPS, INAIL, ISTAT.

Per quanto rileva ai fini del presente documento, le norme sono perlopiù finalizzate alla repressione dei fenomeni di "*frode nelle sovvenzioni*", con riferimento sia alle ipotesi di indebita captazione che a quelle di illecita utilizzazione di risorse pubbliche; in particolare, si tutela la fase dell'istruttoria del finanziamento e della sua erogazione, attraverso la repressione delle condotte di indebita captazione di erogazioni pubbliche, realizzate tramite l'esibizione di documentazione falsa o l'omissione di informazioni dovute (art. 316 ter c.p.), ovvero tramite la fraudolenta induzione in errore di terzi (art. 640 bis c.p.); nonché la fase successiva all'erogazione, punendo gli abusi consistenti nell'impiego di finanziamenti ottenuti dallo Stato, da altri enti pubblici o dalle Comunità europee per finalità diverse da quelle per la realizzazione delle quali erano stati concessi (art. 316 bis c.p.).

[8] Articoli modificati dalla L. n. 190/2012 e dalla L. 161/2017.
[9] Articolo modificato dalla Legge 69/2015.
[10] Articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015.
[11] Articolo modificato dalla Legge n. 190/2012 e Legge n. 69/2015. Da ultimo modificato dall'art. 1, comma 1, lett. n), L. 09.01.2019, n. 3 con decorrenza dal 31.01.2019.
[12] Articolo modificato dalla Legge 69/2015.
[13] Articolo modificato dalla Legge 69/2015.
[14] Articolo modificato dalla Legge n. 190/2012.
[15] Articolo aggiunto dalla Legge n. 3/2019.

Va precisato, peraltro, che la nozione di finanziamento pubblico ricomprende tutti quei rapporti in cui la temporanea creazione di disponibilità finanziarie avviene per intervento diretto o indiretto dei pubblici poteri ed in cui l'utilizzazione per il fine convenuto corrisponde ad uno specifico interesse pubblico, di volta in volta individuato. Pertanto, indipendentemente dalla denominazione assunta dalle singole erogazioni (contributi, sovvenzioni, finanziamenti ecc.), queste sono contraddistinte da due caratteristiche: l'avere per oggetto somme di denaro di provenienza pubblica (Stato, altro ente pubblico o Comunità europee) e l'essere concesse a condizioni più favorevoli di quelle di mercato, in vista del fine di pubblica utilità cui esse sono destinate.

Ne consegue che taluni esponenti aziendali e funzionari della banca, nell'espletamento delle proprie mansioni, possono trovarsi esposti al rischio di commissione di talune fattispecie di reato richiamate dagli artt. 24 e 25 del Decreto.

In considerazione della circostanza che, in ambito creditizio, i reati in esame possono configurarsi sia quando i finanziamenti sono erogati a favore della banca, sia quando la banca fa da tramite, nell'ambito di un rapporto trilaterale, della loro distribuzione ai privati destinatari dell'erogazione (ad esempio i crediti speciali o agevolati, i crediti agricoli agevolati), eventuali profili di responsabilità potrebbero essere ascritti alla Banca – a titolo di concorso – laddove questa si adoperasse od intervenisse od ancora contribuisse, in qualsivoglia maniera, alla realizzazione delle fattispecie criminose in parola.

A monte del presidio si rappresenta che tutte le fasi della procedura di richiesta e/o erogazione dei contributi, sono documentate e verificabili attraverso la pratica elettronica di fido, che consente di poter sempre ricostruire ex post le caratteristiche e le motivazioni dell'operazione ed individuare i soggetti coinvolti.

A fattor comune, qui si richiamano le indicazioni fornite dalle linee guida dell'ABI.

Ai sensi dell'art. 6 del Decreto, sono state individuate dalla Banca le attività sensibili nell'ambito delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del Decreto. Nell'ambito di dette attività sono stati valutati i profili potenziali di rischio di reato in relazione ai rapporti che la Banca intrattiene con la Pubblica Amministrazione.

Si osserva che ai fini del Modello appartengono alla Pubblica Amministrazione tutti quei soggetti, pubblici o privati, che svolgono una "funzione pubblica" o un "pubblico servizio" ai sensi degli artt. 357 e 358 del Codice Penale.

Per **funzione pubblica** si intende l'esercizio delle attività, disciplinate da norme di diritto pubblico, attinenti alla funzione legislativa, amministrativa e giudiziaria. La funzione pubblica è

caratterizzata dall'esercizio del potere autorizzativo e del potere certificativo. Colui che "*esercita una pubblica funzione legislativa, giudiziaria o amministrativa*" è qualificato, ai sensi dell'art. 357 c.p., quale "pubblico ufficiale".

Per **pubblico servizio** si intende, invece, l'esercizio delle attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'Autorità Pubblica o l'esercizio delle attività volte a garantire i diritti fondamentali della persona, quali quello alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione, etc. Il pubblico servizio è un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri autoritativi e certificativi. Colui che "*a qualunque titolo presta un pubblico servizio*" è qualificato, ai sensi dell'art. 358 c.p., quale "*persona incaricata di un pubblico servizio*".

Si prescinde, quindi, dall'esistenza di un rapporto di dipendenza con un ente pubblico, dovendosi, secondo una concezione funzionale-oggettiva, considerare tale ogni attività diretta oggettivamente al conseguimento di finalità pubbliche.

In presenza dello svolgimento di un'attività avente i requisiti predetti, la Giurisprudenza ritiene irrilevante la natura della normativa che disciplina il rapporto. Essa attribuisce rilievo anche alla prestazione di fatto di un pubblico servizio.

Le principali aree di rischio in generale

I rapporti con la pubblica amministrazione presentano rischi reato principalmente nei seguenti processi:

1. **Negoziazione, stipulazione ed esecuzione di contratti/convenzioni con la PA:**
   - 1.1. Allorquando la Banca decida di partecipare a procedure indette da soggetti pubblici per l'affidamento di servizi, quali:
     - 1.1.1. Servizio di tesoreria enti, che comprende tutti gli adempimenti amministrativi che le diverse normative impongono alla banca tesoriera (es: acquisizione dei documenti contabili dell'ente, predisposizione del consuntivo di bilancia, ecc.);
     - 1.1.2. Altri servizi bancari (conto corrente, deposito titoli, ecc) o ad essi accessori (collocamento polizze assicurative, ecc), oppure prodotti di cash management (bonifici, assegni, MAV/RAV, RI.BA, carte, ecc);
     - 1.1.3. Attività relative all'erogazione del credito e al rilascio di garanzie verso gli enti pubblici;
     - 1.1.4. Adempimenti legati alla finanza di progetto;
     - 1.1.5. Attività di monitoraggio sull'andamento dei crediti concessi all'ente pubblico, allorquando si offre o promette denaro o altra utilità ad un pubblico ufficiale e/o

un terzo intermediario per non fare emergere il deterioramento della qualità creditizia del cliente al fine di ottenere la stipula di un accordo commerciale con il medesimo ente.

1.1.6. Attività che comportino un lucro grazie ad informazioni/dichiarazioni false, lacunose o riservate (per es: un parere di consulenza non corretto mirato a spingere l'ente pubblico al compimento di un'operazione di finanza straordinaria lucrosa per la banca e non conveniente per l'ente), che potrebbero produrre imputazioni di truffe ai danni dello Stato. Ciò per esempio:

1.1.6.1. nella classificazione a default di crediti agevolati, eventualmente anche in concorso con il richiedente, omettendo o alterando i dati per non perdere un beneficio o un'erogazione;

1.1.6.2. durante l'erogazione del servizio di tesoreria, se si presenta una rendicontazione falsa all'ente occultando somme di denaro incassate o riportando pagamenti mai effettuati, al fine di lucrare sulle commissioni/interessi sulle operazioni;

1.1.6.3. effettuando un rinnovo contrattuale di una linea di credito giustificato da un fittizio deterioramento della situazione economica e finanziaria dell'affidato, a condizioni particolarmente remunerative per la Banca e lesive degli interessi della controparte.

2. Relazioni istituzionali e rapporti con le Autorità di Vigilanza;

3. Esecuzione di provvedimenti dell'autorità giudiziaria, nonché gestione dei pignoramenti presso terzi:

3.1. Le attività poste in essere per l'esecuzione delle richieste e delle disposizioni dell'A.G. o da organi dalla stessa delegati sono soggette al rischio corruttivo (corruzione attiva/traffico di influenze illecite). In particolare:

3.1.1. Acquisizione e trasmissione interna della richiesta dell'A.G. e delle relative risposte;

3.1.2. Richieste di testimonianze, sommarie informazioni e consegna di documentazione bancaria;

3.1.3. Affiancamento dell'ispezione della polizia giudiziaria;

3.1.4. Modalità e tempistica di acquisizione/trasmissione dei provvedimenti di sequestro /blocchi dei rapporti e di dissequestro;

3.1.5. Esecuzione di disposizioni relative a sequestri e/o apposizione del fermo sui rapporti di conto corrente, cassette di sicurezza, titoli di credito e altri rapporti oggetto di sequestro;

3.1.6. Adempimenti inerenti al Fondo Unico di Giustizia;

3.1.7. Pratiche di pignoramento che comprendono anche quelli esattoriali o derivanti da disposizioni giudiziarie.

4. Gestione delle indagini finanziarie e dei rapporti con l'anagrafe tributaria.

Descrizione dei Rischi in relazione ai reati contenuti nell'articolo 24

Le principali aree aziendali della Banca risultate esposte a potenzialità commissiva dei reati di cui all'art. 24 del Decreto, sono:

- *Consiglio di Amministrazione*
- *Comitato Esecutivo*
- *Direzione Generale*
- *Area Governo Operativo*
- *Legale e Affari societari*
- *Fiscale e Tributario*
- *Amministrazione*
- *Incassi e Pagamenti*
- *Crediti*
- *Area Controlli*
- *Sistemi Informativi*
- *Marketing*
- *Consulenti, Collaboratori esterni e Outsourcers.*

In generale, le attività e i processi potenzialmente esposti alla realizzazione dei reati-presupposto della specie risultano:

- *Gestione dei rapporti e relazioni con la P.A. e le Autorità di Vigilanza*
- *Gestione delle verifiche, ispezioni, controlli e accertamenti da parte delle Autorità*
- *Formazione finanziata, agevolazioni e provvidenze al Personale*
- *Gestione della Tesoreria,*
- *Omaggistica e spese di rappresentanza*
- *Gestione del patrimonio mobiliare e immobiliare della banca*
- *Gestione delle gare per appalti pubblici.*
- *Richiesta e gestione di licenze, autorizzazioni, concessioni*
- *Gestione Agevolazioni ex legge n. 488/1992 c.s.m. e legge n. 311/2004*
- *Istruttoria ed erogazione di "crediti" e gestione delle garanzie*
- *Gestione del Personale*
- *Stipula e gestione di contratti e convenzioni*
- *Attività di natura legale, amministrativa, fiscale*
- *Pianificazione operativa e controllo di gestione*
- *Gestione dei Sistemi informatici (hardware e software) e telematici*
- *Gestione contenzioso*
- *Gestione dei crediti, di qualsiasi natura (anche in sofferenza o recupero forzoso) verso*

- *soggetti privati e pubblici*
- *Gestione dei rapporti con Partners, Consulenti*
- *Conferimento ed esecuzione di mandati professionali a periti, legali, valutatori CTP*
- *Gestione degli acquisti con Fornitori di servizi e di opere, Outsourcers, Appaltatori e subappaltatori*
- *Gestione rapporti con Società del GBCI, con Parti correlate e con altre BCC*

Con specifico riferimento all'articolo 24, come anticipato nella parte generale, le fattispecie di reato presupposto espressamente richiamate sono quelle relative ai reati peculiari dell'impresa, ovvero di manifestazioni tipiche di comportamenti illeciti rinvenibili nell'attività imprenditoriale. Dunque, riscontrabile negli ambiti che determinano l'attività in sinergia con la Pubblica Amministrazione o comunque attraverso un rapporto diretto con quest'ultima, che può verificarsi anche in maniera episodica. Sono quelle condotte criminose caratterizzate da un'induzione in errore degli apparati dello Stato, cui fa seguito un indebito profitto (interesse e/o vantaggio).

Trattandosi di norme finalizzate alla repressione dei fenomeni di "frode nelle sovvenzioni", con il conseguente illecito utilizzo di risorse pubbliche, parte dei rischi sono individuabili essenzialmente nell'ambito del processo del credito a favore della clientela, dalla fase dell'istruttoria del finanziamento alla fase successiva all'erogazione. Per quanto riguarda l'istruttoria del finanziamento, rilevano le condotte fraudolente, realizzate tramite l'esibizione di documentazione e/o informazioni false o l'omissione di informazioni dovute (art. 316-*ter* c.p., art. 137 TUB), ovvero tramite la fraudolenta induzione in errore di terzi (art. 640-*bis* c.p.). In relazione alla fase successiva all'erogazione, vengono a rilievo, invece, gli abusi relativi all'impiego di finanziamenti ottenuti dallo Stato, da altri enti pubblici o dalla Comunità Europea, per finalità diverse da quelle per la realizzazione delle quali tali contributi sono stati concessi (art. 316-*bis* c.p.).

Nella malversazione, invece, assume rilievo la mancata destinazione del finanziamento ricevuto per le finalità di interesse pubblico che ne abbiano giustificato l'erogazione.

Al riguardo si rilevano anche profili di responsabilità a carico della Banca, in quanto soggetto obbligato, con riferimento al rischio di riciclaggio, il cui argomento sarà trattato nell'apposita sezione.

La Banca, nell'ambito dell'ordinaria operatività, inoltre, è solita concedere credito alla clientela, anche attraverso finanziamenti:

a) riconducibili ai crediti di firma rotativi per la partecipazione a gare d'appalto provvisorie da parte dei clienti;
b) per crediti agevolati in diversi ambiti;
c) che – a tutela della Banca – beneficiano della garanzia pubblica (MCC, Sabatini, ecc.), con il rischio che la stessa Banca, in ipotesi, potrebbe concorrere nel reato commesso dai clienti con riferimento:

- alla rendicontazione della destinazione dei finanziamenti, allo scopo di ottenere da questi ultimi la riduzione o l'estinzione dei finanziamenti concessi agli stessi,
- all'attestazione per vera di falsa documentazione prodotta dai clienti, nel caso di presentazione delle domande di agevolazione per i mutui, laddove la banca favorisca la presentazione di domande pur conoscendo la mancanza dei requisiti del presentatore, in modo da ridurre il suo rischio per l'affidamento concesso.

Rilevano, per altro verso, i rischi riguardanti:

d) finanziamenti, diretti o indiretti, a favore della Banca, qualora la stessa dovesse beneficiare di risorse pubbliche in casi di ristrutturazione e/o ricostruzione di punti operativi (per esempio in caso di calamità), ovvero nel caso di finanziamenti conseguiti per favorire piani di formazione per il personale dipendente e per gli amministratori;

e) l'alterazione o contraffazione del bilancio d'esercizio, al fine di aggiudicarsi i contratti ad evidenza pubblica per la cui stipulazione è prevista la presentazione del bilancio medesimo o per altre finalità illecite, ovvero per l'aggiudicazione/rinnovo di servizi di tesoreria e cassa in favore di Enti Pubblici, nonché di attestazioni relative alle quote di assunzione di categorie protette.

f) Concorso nella condotta illecita di ente pubblico per mantenere vincolate fraudolentemente somme libere allo scopo di ottenere le somme presenti sulle contabilità speciali;

g) Alterazione, contraffazione dei dati comunicati in occasione della gestione del servizio di incasso pensioni, in concorso con il cliente (erede), omettendo di comunicare all'ente pensionistico il decesso del cliente e incamerare le somme. Quindi potendosi configurare l'erogazione di pensioni a soggetti non aventi diritto.

h) Alterazione, contraffazione dei dati comunicati in occasione di versamenti obbligatori di natura fiscale, tributaria o contributiva (es. facendo risultare alcuni dipendenti come appartenenti a categorie protette.

i) Alterazione del software di trasmissione in via telematica, con la conseguente alterazione dei dati contenuti in un database protetto oppure un software di proprietà della P.A., nel caso, per esempio, trasmissione delle segnalazioni di Vigilanza[16].

j) Alterazione dei dati nelle attività aziendali che prevedono l'accesso nei confronti di sistemi informativi gestiti dalla PA, quali, a titolo esemplificativo:

[16] Il reato potrebbe configurarsi nel caso in cui – per esempio – essendo scaduto il termine per l'invio dei dati all'Autorità di Vigilanza, il sistema viene alterato in modo da far risultare che la trasmissione sia avvenuta nel termine prescritto.

- la partecipazione a procedure di gara che prevedono comunque una gestione informatica, quindi l'alterazione di registri informatici della PA per far risultare esistenti condizioni essenziali per la partecipazione: iscrizione in albi, ecc.;
- la presentazione in via informatica alla P.A. di istanze e documentazione di supporto, al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc.) di interesse aziendale, laddove contenenti attestazioni/certificazioni non veritiere in merito all'esistenza di condizioni e/o requisiti essenziali;
- la modifica in via informatica dei dati fiscali e/o previdenziali di interesse dell'azienda (es. modelli 770), già trasmessi alla P.A.

Regole di carattere generale

Tutti i Destinatari del Modello, come individuati dalla Parte Generale, adottano regole di comportamento conformi ai principi di seguito elencati, nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili e strumentali, al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione rilevanti per la Banca e previsti dal Decreto.
In generale, si stabiliscono i seguenti principi di comportamento per le attività sensibili relative ai reati di cui agli artt. 24 e 25 del Decreto.
A fattor comune, oltre a quanto finora descritto e qualora non dovesse individuarsi nei regolamenti e disposizioni di specifici processi, nell'ottica di prevenire la commissione dei reati nei confronti della P.A. sono fissate le seguenti prescrizioni obbligatorie:

- ✓ i rapporti in nome e per conto della Banca con esponenti della P.A. devono essere tenuti esclusivamente da soggetti legittimati e allo scopo autorizzati; i collaboratori esterni devono aver ricevuto un incarico espresso formalizzato con specifico atto/contratto;
- ✓ i Consulenti esterni, gli Outsourcers, i Partners che intermedino o supportino la Banca nella tenuta dei rapporti con la P.A. devono essere selezionati e individuati in modo trasparente e con parità di trattamento, (modalità di identificazione, condizioni di pagamento, ecc.), conformemente alla normativa aziendale vigente;
- ✓ deve essere informato con nota scritta il Consiglio di Amministrazione, nonché l'Organismo di Vigilanza, di ogni criticità di rilievo o conflitto d'interesse configurantesi nel contesto del rapporto con la P.A., affinché vengano assunti gli opportuni provvedimenti;
- ✓ l'erogazione dei servizi istituzionali o di supporto a favore di Soggetti pubblici - anche convenzionati - e/o di loro rappresentanti ed esponenti, deve essere resa in condizioni di parità di trattamento rispetto al privato;

- ✓ gli Esponenti aziendali e coloro che occupano ruoli di responsabilità nella funzione di controllo e supervisione devono porre particolare attenzione nell'espletamento delle verifiche e segnalare prontamente eventuali irregolarità o anomalie all'Organismo di Vigilanza;
- ✓ i soggetti responsabili della redazione e trasmissione, per via informatica o telematica, alle Autorità di Vigilanza e ai Soggetti pubblici di report, informative (periodica, "ad evento" o su richiesta), rendiconti, ecc., dovranno essere a ciò formalmente incaricati e dovranno conformarsi alle specifiche prescrizioni definite nella Sezione relativa ai reati informatici dei presenti Protocolli e dalla normativa interna;
- ✓ ogni corrispondenza o invio di documentazione a funzionari pubblici deve essere trasmessa, in via preferenziale, mediante sistemi di posta elettronica certificata, con archiviazione (informatica o cartacea) della relativa documentazione.

Prescrizioni comportamentali

Tutti i Destinatari del Modello, come individuati dalla Parte Generale, adottano regole di comportamento conformi ai principi di seguito elencati, nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili e strumentali indicate nel paragrafo precedente, al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione rilevanti per la Banca e previsti dal Decreto.

In generale, si stabiliscono i seguenti principi di comportamento per le attività sensibili relative ai reati di cui agli artt. 24 e 25 del Decreto.

In particolare, è fatto a ciascuno divieto di:

- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, anche acquisite al di fuori della propria realtà professionale, al fine di influenzarne le decisioni, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del settore, erogazione di contributi/finanziamenti pubblici e/o simili informazioni;
- instaurare e mantenere rapporti con pubblici ufficiali e/o incaricati di pubblico servizio in rappresentanza o per conto della Banca, in mancanza di apposita delega o procura;
- offrire denaro o altra utilità a Pubblici Ufficiali o incaricati di Pubblico Servizio o organi o funzionari dell'Autorità Giudiziaria, inclusi i familiari degli stessi, al fine di influenzarne la discrezionalità, l'indipendenza di giudizio o per indurli ad assicurare un qualsiasi vantaggio alla Banca, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del

settore e/o erogazione di contributi/finanziamenti pubblici e/o simili informazioni, ovvero agevolare eventuali processi nell'ambito del contenzioso che vede coinvolta la banca;

- riconoscere, in favore di fornitori o collaboratori esterni, o loro familiari, che operino nei confronti della Pubblica Amministrazione in nome e per conto della banca, compensi indebiti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione o dazione di denaro o altra utilità a un pubblico funzionario dell'Autorità Giudiziaria, o suoi familiari, nel caso in cui la banca sia parte di un procedimento giudiziario;
- conferire incarichi professionali, dare o promettere doni, danaro, o altri vantaggi a chi effettua gli accertamenti e le ispezioni, autorità pubbliche ovvero ad organi dell'Autorità Giudiziaria e/o di Polizia Giudiziaria;
- ricorrere a forme di contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze, pubblicità, configurino, invece, forme di doni o regalie verso pubblici funzionari, loro familiari, enti e autorità pubbliche; presentare dichiarazioni, comunicazioni o documenti contenenti informazioni non veritiere, fuorvianti o parziali alla Pubblica Amministrazione, ovvero omettere informazioni, al fine di ottenere provvedimenti favorevoli dalla Pubblica Amministrazione (ad es. per ottenere il rilascio di concessioni o autorizzazioni, finanziamenti pubblici);
- agevolare la clientela nella destinazione a finalità diverse da quelle per le quali vengono concessi contributi, sovvenzioni o finanziamenti o altra erogazione dello stesso tipo ottenuti dallo Stato o da altro ente pubblico o dall'Unione Europea.
- porre in essere comportamenti tali da integrare le fattispecie di reato sopra indicate, o idonei ad agevolarne la realizzazione, ovvero ad impedirne la rilevazione;
- procedere alla erogazione del compenso, di acconti e rimborsi spesa senza fare ricorso a sistema tracciabile e senza previa verifica dell'esattezza e tempestività della prestazione e di ricezione di regolare fattura;

È fatto, altresì, espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino gli estremi di un reato o di comportamenti corruttivi, come:

- esercitare forme di pressione, inganno, suggestione o captazione della benevolenza del funzionario pubblico, ovvero assecondare suoi comportamenti surrettizi o di induzione a dare o promettere alcunché, tali da influenzare le determinazioni del soggetto pubblico;

- effettuare - direttamente o indirettamente - elargizioni in denaro, ovvero attribuire o anche promettere utilità[17] a favore di pubblici ufficiali o ad incaricati di pubblico servizio (italiani o stranieri) e loro familiari;
- distribuire od offrire omaggi e regali al di fuori di quanto previsto dalla specifica normativa interna adottata dalla banca.
- accordare o offrire vantaggi di qualsiasi natura o forme di ospitalità, anche mediante accollo di spese di rappresentanza, ovvero atti di liberalità (es. sponsorizzazioni di eventi), ad esponenti della P.A. o loro familiari, in violazione della normativa interna;
- effettuare prestazioni, o riconoscere compensi in favore di dipendenti, dirigenti, Amministratori di enti pubblici, società o enti non profit, o onorari a favore di Collaboratori esterni (es. consulenti, Outsourcers, ecc.), che non trovino adeguata giustificazione nel contesto del rapporto contrattuale intercorrente con essi;
- effettuare dichiarazioni non veritiere ad Organismi pubblici nazionali o comunitari al fine di conseguire erogazioni, contributi o provvidenze pubbliche per la banca, ovvero per la clientela o terzi;
- accettare la richiesta o la sollecitazione, anche per interposta persona, di denaro o altra utilità dal funzionario pubblico in rapporto con la Banca, ovvero da un soggetto terzo a lui in qualsiasi modo collegato;
- ricercare, o instaurare illecitamente, relazioni personali di favore, di influenza, di ingerenza – anche con esponenti di società private, fornitrici di beni e di servizi - capaci di condizionare, direttamente o indirettamente, la tenuta del rapporto o l'esito della procedura.

Principali presidi organizzativi e gestionali

In tale ambito, oltre ai presidi di carattere generale, che disciplinano gli aspetti etico comportamentali, la Banca adotta specifiche procedure aziendali, in relazione ai singoli processi sensibili, che definiscono con chiarezza i ruoli ed i compiti delle Funzioni responsabili.
In riferimento alle ipotesi di malversazione e, quindi, alle attività riguardanti la gestione dei finanziamenti agevolati a favore della clientela - punti a), b), e c) -, attraverso il Regolamento del credito, il regolamento interno ed il regolamento dei poteri delegati, la Banca ha definito protocolli volti a indicare:

[17] Per esempio, nell'erogazione dei servizi di credito, concedendo linee di credito o garanzie a condizioni di particolare favore, ovvero mediante cancellazione di posizioni debitorie o, ancora, facendo ottenere finanziamenti o interventi agevolativi in difetto dei presupposti di legge.

- le regole per la gestione delle richieste presentate dalle imprese, in termini di verifica della loro completezza, regolarità ed esistenza dei presupposti per l'ottenimento dei finanziamenti agevolati;
- compiti e responsabilità delle unità organizzative coinvolte nelle attività.
- l'attività di controllo finalizzata a garantire l'adeguatezza e la conformità alle disposizioni normative, esterne ed interne.

Al riguardo i responsabili, rispettivamente, dell'Area Crediti e del Servizio Monitoraggio e Gestione NPLs, nell'ambito delle rispettive competenze provvedono ad assicurare flussi informativi verso l'OdV - con periodicità semestrale - circa i soggetti beneficiari e le eventuali situazioni di insoluto.

In riferimento ai punti da d) a h), avuto anche riguardo al fatto che trattasi di rischi rientranti nell'ambito dei rapporti con la Pubblica Amministrazione, taluni presidi sono regolati nel Regolamento del processo Tesoreria enti, in special modo le attività attinenti alla partecipazione ai bandi di gara per il servizio di tesoreria, nel quale sono indicate le regole sia per la gestione delle offerte economiche e tecniche, necessarie per la partecipazione a procedure ad evidenza pubblica, sia per la successiva gestione. In particolare, sono previsti i seguenti presidi:

- la procedura operativa che disciplina le modalità di gestione della Tesoreria, dall'incasso delle somme dai contribuenti fino all'erogazione e rendicontazione all'Ente;
- la regolamentazione dei compiti e delle responsabilità delle varie unità organizzative coinvolte;
- la segregazione funzionale, con particolare riferimento allo svolgimento delle seguenti attività:
  - individuazione degli Enti, raccolta della documentazione con la valutazione del loro merito creditizio e del ritorno economico dell'iniziativa e predisposizione della documentazione necessaria per la partecipazione ai bandi di gara;
  - invio della documentazione predisposta per la partecipazione ai bandi di gara;
  - ricezione degli ordinativi di incasso e pagamento (accertamento/ordinazione) e loro imputazione in procedura (lavorazione);
  - gestione della liquidità (incassi/pagamenti);
  - contabilizzazione delle operazioni;
  - gestione amministrativa e rendicontazione all'Ente e alla Banca d'Italia;

- la predisposizione di attività di controllo e supervisione finalizzate a garantire l'adeguatezza e la conformità al contratto e alle disposizioni di legge in materia di incasso e riversamento delle somme.

Ulteriori presidi sono disciplinati nel regolamento del credito, attraverso specifici iter istruttori ed autorizzativi, oltre agli ordinari poteri di delega e firma.

Inoltre, sono predisposti presidi autorizzativi e di controllo nell'ambito del regolamento sugli incassi e pagamenti, con riferimento in particolare al punto g), tenendo presente che il processo deve essere svolto in maniera trasparente e documentabile, nel rispetto delle seguenti specifiche misure comportamentali e di controllo:

- è vietato destinare, in tutto o in parte, le somme ricevute dall'INPS per scopi diversi dalla corresponsione dei ratei pensionistici ai soggetti beneficiari; in caso di somme non riscosse, ovvero restituite dal beneficiario, è obbligatorio restituirle all'INPS secondo le indicazioni contrattuali;
- è obbligatorio comunicare all'INPS le variazioni intervenute circa i soggetti beneficiari delle quali I.B. venga a conoscenza (es. decesso, aggiornamento IBAN, ecc.);
- attivazione di un periodico flusso informativo rivolto all'OdV che riporti eventuali criticità insorte nella tenuta dei rapporti con l'INPS.

Sul punto il responsabile dell'Ufficio Portafogli, Incassi e Pagamenti deve assicurare report informativo all'OdV, con cadenza annuale, nel quale andranno indicate anche le posizioni restituite all'INPS con le relative motivazioni e con la specifica giustificazione documentale acquisita, con eventuali indicazioni di attività di recupero avviate dalla banca nei confronti dei clienti.

Con riferimento, infine, ai presidi riguardanti le ipotesi di frode informatica, avuto riguardo al fatto che l'elemento soggettivo di riferimento, diversamente dal reato di accesso abusivo, prevede l'accesso a un sistema informatico al fine di alterarne i contenuti, si richiamano le disposizioni di vigilanza a cui seguono, in particolar modo, le verifiche del Collegio Sindacale e della società incaricata alla revisione, fermo restando gli adempimenti disciplinati nell'ambito del sistema dei controlli interni, che affida a ciascuna funzione aziendale di controllo l'onere delle verifiche anche in tali ambiti, specialmente riguardo ai profili di compliance. A proposito di tale ultimo aspetto, si richiama in questa sede anche il sistema di controllo e gestionale dell'outsourcer informatico al quale è stato esternalizzato il sistema informativo.

Valgono, per quanto di attinenza, i presidi di controllo nell'ambito dell'IT Risk Assessment che annualmente la banca è tenuta ad effettuare anche in termini di sicurezza ed efficienza del sistema informativo, che qui deve intendersi integralmente richiamato.

Descrizione dei Rischi contenuti nell'articolo 25

Anche in questo caso, rilevano i reati che hanno come presupposto l'instaurazione di rapporti e/o lo svolgimento di attività correlati ad una pubblica funzione o a un pubblico servizio.
Tenuto conto dei rapporti che la Banca intrattiene con Amministrazioni Pubbliche, anche con riguardo al Servizio di tesoreria e di cassa, considerato inoltre che la Banca opera in area geografica in cui non sempre risultano garantite adeguate condizioni di trasparenza, le aree di attività ritenute più specificamente a rischio sono:

1) La partecipazione a procedure di gara indette da enti pubblici, per l'affidamento di appalti, di forniture o di servizi, di concessioni, di partnership o di altre operazioni simili, caratterizzate dal fatto di essere svolte in un contesto potenzialmente competitivo, intendendosi tale anche un contesto in cui, pur essendoci un solo concorrente in una particolare procedura, l'ente appaltante avrebbe avuto, tuttavia, la possibilità di scegliere anche altre imprese presenti sul mercato.
2) La partecipazione a procedure di negoziazione diretta per la prestazione, in favore della Pubblica Amministrazione o di altri enti pubblici, di servizi, riservati o in regime di concorrenza, tra cui l'aggiudicazione, il rinnovo e la gestione del servizio di Tesoreria Enti.
3) La gestione delle risorse finanziarie di Tesoreria.
4) La gestione dei contributi e dei finanziamenti statali, nonché la gestione dei finanziamenti agevolati.
5) La gestione delle assunzioni e delle collaborazioni, in relazione alle richieste di assunzioni agevolate o per contratti di formazione con finanziamenti pubblici.
6) L'attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società partecipate o controllate dallo Stato, nonché gli appalti di lavori, che, pur non prevedendo alcun contatto con la Pubblica Amministrazione, sono potenzialmente strumentali alla realizzazione di fattispecie di reato contro la stessa.
   Tali attività, peraltro, costituiscono situazione di particolare attenzione specialmente in relazione ad acquisti di natura immateriale, tra cui consulenze commerciali, amministrativo-legali, collaborazioni a progetto, sponsorizzazioni e attività di sviluppo di software e servizi IT.
7) La partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego.
8) La richiesta di provvedimenti amministrativi occasionali, di autorizzazioni, licenze e concessioni per lo svolgimento di attività strumentali a quelle tipiche della Banca, quali ad

esempio, la corruzione del tecnico del Comune per ottenere licenze edilizie ovvero certificati di agibilità.

9) I rapporti con le Autorità indipendenti e di Vigilanza e altri organismi di diritto pubblico, nonché il rilascio di informazioni alla Pubblica Amministrazione.
10) I rapporti con i pubblici ufficiali e gli incaricati di pubblico servizio relativamente agli adempimenti fiscali, tributari e previdenziali.
11) I rapporti con l'Autorità Giudiziaria, con la polizia giudiziaria, con i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale, nonché nelle indagini di carattere penale.
12) Omaggi, spese di ospitalità e rappresentanza.
13) Rapporti con le organizzazioni politiche e sindacali.
14) Affidamento di incarichi di consulenza, specialistici e professionali.
15) Affidamento di lavori e fornitura di beni e servizi ovvero acquisizione di beni o servizi presso società o professionisti vicini ad esponenti della P.A. allo scopo di ottenere favori o altra utilità.
16) Partecipazioni in società partecipate e/o controllate da enti pubblici.
17) La selezione e l'assunzione del personale.
18) La formazione finanziata da erogare a favore del personale
19) Le iniziative non profit e sponsorizzazioni.
20) La concessione e gestione di finanziamenti agevolati alla propria clientela (contributi, finanziamenti pubblici, crediti agrari agevolati) in assenza dei presupposti di legge.

Principali presidi organizzativi e gestionali

Nei rapporti con la Pubblica Amministrazione, oltre ai presidi di carattere generale, che disciplinano gli aspetti etico comportamentali, anche con riferimento alla gestione degli omaggi, delle donazioni e delle liberalità, la Banca, adotta specifiche procedure aziendali, in relazione ai singoli processi sensibili, che definiscono con chiarezza i ruoli ed i compiti delle Funzioni responsabili della gestione dei rapporti con la Pubblica Amministrazione.

In linea generale, la Banca assicura il presidio attraverso le disposizioni riportate nei regolamenti "*Infrastrutture e Spese*", "*Poteri delegati e di firma", "Regolamento del credito*" che comprendono, per quanto rileva nel caso di specie:

a) la separazione di responsabilità tra chi avvia un pagamento e chi lo approva (es. il responsabile produzione richiede l'acquisto e il responsabile amministrativo ne ordina il pagamento);

b) la definizione di livelli gerarchici con responsabilità crescenti in modo che il pagamento di transazioni elevate sia affidato a livelli gerarchici elevati (es. coerenza dei poteri di spesa rispetto alle soglie dei poteri di firma conferiti ovvero la rispondenza degli importi previsti da contratti quadro/ordini di acquisto con i poteri di firma stabiliti;

c) la verifica che il pagamento per il lavoro o i servizi effettuati siano autorizzati secondo i pertinenti livelli di responsabilità, ad esempio che il pagamento sia autorizzato a fronte della effettiva prestazione;

d) per alcune casistiche, la richiesta di almeno due diverse funzioni sulle approvazioni di pagamento;

e) l'obbligo di conservazione della documentazione di supporto appropriata che garantisca adeguata tracciabilità del flusso autorizzativo (ad es. sulla sequenza preventivo-fattura-pagamento)

f) l'attuazione di un riesame gestionale periodico delle transazioni finanziarie significative e attuazione di audit finanziari periodici e indipendenti;

g) procedure per l'approvvigionamento differenziate a seconda dell'oggetto dell'acquisizione (lavori, beni, servizi, consulenze etc.), delle soglie di valore del contratto e della natura delle controparti (pubblica o privata);

h) procedure di selezione di appaltatori, sub-appaltatori, fornitori e consulenti;

i) previsione di supervisione e di autorizzazione di livelli gerarchici/funzionali adeguati nel caso di operazioni straordinarie, di deroghe e/o proroghe che possono determinare rischi di corruzione significativi.

Inoltre, i suindicati regolamenti prevedono:

1) L'attribuzione di poteri e deleghe di spesa e del relativo monitoraggio, allo scopo di conseguire la migliore trasparenza nella relativa gestione.
2) L'obbligo in capo all'ufficio contabilità, prima di procedere a qualsiasi pagamento, di:
    a. effettuare il controllo formale sui documenti di spesa e sulle relative autorizzazioni;
    b. acquisire la preventiva autorizzazione del Direttore Generale o, in caso di assenza, del Vicedirettore Generale o altra funzione appositamente delegata.
3) Regole:

a. per la gestione dei contenziosi, al fine di evitare la realizzazione di condotte che potrebbero favorire la BCC o danneggiare la controparte in un processo civile, penale o amministrativo.

b. per la predisposizione ed approvazione del bilancio d'esercizio, al fine di consentire adeguata verifica circa la sussistenza dei requisiti previsti, anche in relazione all'ipotesi di aggiudicazione di contratti aventi evidenza pubblica, per la cui stipulazione è prevista la presentazione del bilancio medesimo.

c. volte ad impedire condotte illecite a favore di amministratori e/o funzionari pubblici o loro familiari, tale da indurre i primi a comportamenti omissivi, realizzabili mediante la:

   i. cancellazione di eventuali posizioni debitorie;

   ii. concessione di linee di credito o garanzie, a condizioni di particolare favore o senza esigerne la restituzione;

   iii. assegnazione di titoli in forma gratuita e/o a condizioni più favorevoli rispetto a quelle di mercato.

   iv. gestione non trasparente delle locazioni e compravendite attive e passive.

Inoltre, valutati i rapporti ed i possibili legami intercorrenti con i pubblici amministratori presenti nel territorio della Banca, ovvero avuto riguardo alla possibile inferenza di questi ultimi in attività ricadenti nel territorio della Banca o a favore di clienti della banca, valgono a tutela dei rischi relativi ai reati in trattazione i presidi strutturati:

- nella regolamentazione antiriciclaggio, con riferimento alle attività di verifica ai fini della individuazione di eventuali condotte criminose funzionali al rischio di riciclaggio, adeguati ed aggiornati alle disposizioni di tempo in tempo emanate dalle competenti Autorità, ivi compresi i presidi sulle buone prassi in materia di Persone Politicamente Esposte (PEP);
- nella regolamentazione in materia di soggetti collegati di cui alle disposizioni di vigilanza di Banca d'Italia, ai sensi della Circolare 263/2006;
- nel regolamento del credito, dove sono indicati specifici iter autorizzativi.

Particolare attenzione viene rivolta alle attività che la Banca - per dimensione, struttura e competenza territoriale - svolge in via prevalente, ovvero:

a) Servizio di tesoreria e di cassa per Comuni e Enti pubblici locali.
b) Gestione dei diversi finanziamenti agevolati, anche con riguardo agli affidamenti e/o crediti di firma.

Riguardo al punto a), si fa riferimento ai presidi previsti nel Regolamento del processo Tesoreria enti, nel quale sono definite le regole sia per la gestione delle offerte economiche e tecniche, necessarie per la partecipazione a procedure ad evidenza pubblica, sia per la successiva gestione. In particolare, sono previsti i seguenti presidi:

- la procedura operativa che disciplina le modalità di gestione della Tesoreria, dall'incasso delle somme dai contribuenti fino all'erogazione e rendicontazione all'Ente;
- la definizione dei compiti e delle responsabilità delle varie unità organizzative coinvolte, attraverso specifici protocolli interni declinati: i) nel regolamento interno d'istituto; ii) nel regolamento del credito; iii) nel regolamento dei poteri e deleghe.
- la segregazione funzionale, con particolare riferimento allo svolgimento delle seguenti attività:
  - individuazione degli Enti, raccolta della documentazione con la valutazione del loro merito creditizio e del ritorno economico dell'iniziativa e predisposizione della documentazione necessaria per la partecipazione ai bandi di gara;
  - invio della documentazione predisposta per la partecipazione ai bandi di gara;
  - ricezione degli ordinativi di incasso e pagamento (accertamento/ordinazione) e loro imputazione in procedura (lavorazione);
  - gestione della liquidità (incassi/pagamenti);
  - contabilizzazione delle operazioni;
  - gestione amministrativa e rendicontazione all'Ente e alla Banca d'Italia;
- le attività di controllo e supervisione, finalizzate a garantire l'adeguatezza e la conformità al contratto e alle disposizioni di legge in materia di incasso e riversamento delle somme;
- ai fini della sicurezza fisico-logica, procedure informatiche con adeguati profili utenti e la tracciabilità delle risorse aziendali incaricate della gestione delle somme;
- le modalità di predisposizione e archiviazione della documentazione di corrispondenza con l'Ente;
- indirizzi operativi, ai fini del corretto pagamento degli emolumenti dei dipendenti degli enti pubblici, in ottemperanza al D. Lgs. 27 gennaio 2010 n. 11 (PSD) e successive modificazioni.

In riferimento alle attività riguardanti la gestione dei finanziamenti agevolati, la Banca, attraverso il regolamento del credito ed in particolare attraverso alle disposizioni attuative, ha definito protocolli contenenti:

- le regole per la gestione delle richieste presentate dalle imprese, in termini di verifica della loro completezza, regolarità ed esistenza dei presupposti per l'ottenimento dei finanziamenti agevolati;
- i compiti e le responsabilità delle unità organizzative coinvolte nelle attività.
- l'attività di controllo e supervisione finalizzata a garantire l'adeguatezza e la conformità alle disposizioni normative, esterne ed interne.

Posto che tutti i destinatari del presente devono attenersi a quanto previsto nel Codice Etico, nelle procedure e nei protocolli definiti, considerata la struttura gerarchica e funzionale della Banca, le relazioni con i rappresentanti della Pubblica Amministrazione, intesa in tutte le sue possibili articolazioni, devono essere ispirate alla rigorosa osservanza delle norme e non possono in alcun modo compromettere l'integrità e la reputazione aziendale. A tal riguardo, l'assunzione di impegni e la gestione dei rapporti di qualsiasi genere con rappresentanti della P.A. e/o enti di rilevanza pubblica sono riservate esclusivamente alle figure e funzioni aziendali a ciò preposte e autorizzate. Per quanto rileva, qui si richiama il regolamento infrastrutture e spese e dei poteri delegati.

Parimenti, riguardo ai rapporti con organizzazioni politiche e sindacali, la Banca non eroga contributi di alcun genere, direttamente o indirettamente, a partiti politici, movimenti, comitati ed organizzazioni politiche e sindacali, né a loro rappresentanti o candidati.

Per altro verso, considerato che le iniziative no profit e le sponsorizzazioni rientrano nella discrezionalità aziendale secondo le comuni pratiche di business, si rinvia ai presidi disposti nell'ambito del regolamento infrastrutture e spese, dove le attività in discorso sono disciplinate nel rispetto delle procedure e degli iter autorizzativi vigenti. In ogni caso, tra gli aspetti da considerare nella scelta delle proposte cui aderire, è fatto obbligo prestare attenzione verso ogni possibile conflitto di interessi, sia di ordine personale che aziendale. Secondo criteri di ragionevolezza e di proporzionalità, rispetto all'entità dell'impegno economico previsto per la banca devono inoltre essere preventivamente accertati, a cura della funzione aziendale "process owner", la natura e la rilevanza dell'iniziativa, l'identità ed il profilo reputazionale dei destinatari della sponsorizzazione o della contribuzione (promotori, organizzatori, ecc.), e inoltre deve essere verificato il concreto svolgimento dell'iniziativa stessa ed in particolare la sua coerenza con il programma proposto alla banca.

Riguardo agli incarichi di consulenza, specialistici e professionali, l'iter di selezione del professionista da incaricare deve rispettare i criteri di professionalità, trasparenza, imparzialità, economicità ed efficacia. A tal fine, le procedure aziendali attuano i suddetti criteri, regolando

dettagliatamente taluni processi, quali ad esempio quelli riguardanti le stime immobiliari e le consulenze legali.

Per gli incarichi diversi da quelli disciplinati da specifiche policy, devono essere assicurate almeno le seguenti modalità fondamentali:

a) laddove in relazione all'oggetto dell'incarico sia giustificata la prevalenza dell'intuitu persona come criterio di scelta, previa motivazione della necessità di affidamento dell'incarico, si procede all'ingaggio di uno specifico professionista. In tali circostanze, la funzione aziendale "*process owner*" assicura - tramite adeguata istruttoria - che il professionista selezionato abbia i requisiti di onorabilità, standing, reputazione, affidabilità, profilo organizzativo, abilitazioni, qualifiche tecnico-professionali e competenze necessari per lo svolgimento dell'incarico;

b) negli altri casi, sempre previa motivazione della necessità dell'affidamento dell'incarico, seguendo per quanto possibili criteri di rotazione, si procede a scegliere il professionista attraverso il confronto competitivo tra più candidati aventi caratteristiche idonee allo svolgimento dell'attività da affidare, sempre assicurando il possesso dei requisiti come sopra indicati;

c) in tutti i casi, le funzioni aziendali competenti devono accertare che non sussistano per il professionista incompatibilità o conflitto di interessi;

d) i contratti e/o accordi stipulati con i professionisti selezionati devono indicare con esaustività, chiarezza e adeguato dettaglio le prestazioni richieste e i criteri di maturazione dei corrispettivi pattuiti;

e) l'iter di selezione dei professionisti, i contratti ed accordi con essi stipulati e le prestazioni rese devono essere documentati e giustificati.

Allo stesso modo, nel caso di affidamento di lavori o nel caso di forniture di beni e servizi, la selezione dei fornitori deve essere effettuata nell'osservanza dei criteri di trasparenza, tracciabilità, pubblicità, libera concorrenza, non discriminazione, parità di trattamento e rotazione sulla base di criteri oggettivi legati alla competitività ed alla qualità dei prodotti e dei servizi richiesti.

Le procedure aziendali attuano i suddetti criteri, regolando dettagliatamente i processi in materia.

A fattor comune devono essere assicurati i seguenti obblighi fondamentali:

a) adottare criteri di valutazione oggettivi e trasparenti nella selezione delle eventuali aziende fornitrici;

b) osservare e rispettare, nei rapporti di fornitura, le disposizioni di legge applicabili e le condizioni contrattualmente previste;

c) ispirarsi ai principi di correttezza e buona fede nella corrispondenza e nel dialogo con i fornitori, in linea con le più rigorose pratiche commerciali;

d) l'esigenza di perseguire il massimo vantaggio competitivo per la banca deve assicurare in ogni caso l'adozione, da parte dei suoi fornitori, di soluzioni operative in linea con la normativa vigente e, più in generale, con i principi in materia di tutela della persona, della salute e sicurezza dei lavoratori e dell'ambiente.

Ai fini del presidio degli adempimenti di natura contabile, ogni operazione o transazione deve essere correttamente registrata nel sistema di contabilità aziendale, secondo i criteri indicati dalla legge e dai principi contabili applicabili.

Ogni operazione o transazione deve essere autorizzata, verificabile, legittima, coerente e congrua. Affinché la contabilità risponda ai requisiti di verità, completezza e trasparenza, per ogni operazione deve essere conservata agli atti un'adeguata e completa documentazione di supporto dell'attività svolta, in modo da consentire:

a) accurata registrazione contabile;
b) l'immediata determinazione delle caratteristiche e delle motivazioni alla base dell'operazione medesima;
c) l'agevole ricostruzione formale cronologica dell'operazione;
d) la verifica del processo di decisione, di autorizzazione e di realizzazione, nonché l'individuazione dei vari livelli di responsabilità.

Ciascun dipendente è, pertanto, tenuto a collaborare per quanto di propria competenza – affinché ogni fatto relativo alla gestione della banca sia correttamente e tempestivamente registrato nella contabilità. Ciascuna registrazione contabile dovrà riflettere esattamente ciò che risulta dalla documentazione di supporto. Pertanto, sarà compito di ciascun dipendente fare in modo che la documentazione di supporto sia facilmente reperibile ed ordinata.

Infine, con riferimento al presidio rispetto al rischio della commissione del reato di traffico di influenze, la Banca impone a tutti i collaboratori, fornitori di servizi e a tutte le terze parti che operano in nome e per conto della stessa, il divieto di intrattenere rapporti informali con appartenenti alla pubblica amministrazione, per conseguire obiettivi o risultati a favore della banca medesima. Qualsiasi rapporto, che a qualunque titolo coinvolge la pubblica amministrazione, in via diretta o indiretta, dovrà essere concordato preventivamente con i responsabili della banca e disciplinato nello specifico contratto o affidamento di incarico, avendo

cura di specificarvi che gli obiettivi perseguiti sono svincolati da qualsiasi forma di remunerazione. Particolare attenzione va risposta nei casi di affidamenti di incarichi a persone rientranti nella qualifica di PEP, ovvero seppur non rientranti in tale qualifica, ricoprono o hanno ricoperto incarichi pubblici a qualsiasi livello, che andranno opportunamente evitati, fatti salvi casi di specificità professionale non diversamente adottabili. È fatto sempre divieto il pagamento in contanti di qualunque attività seppure l'importo rientri nei limiti previsti dalla normativa sul riciclaggio per tempo vigente.

In tale ambito:

- dovrà essere assicurata la tracciabilità documentale delle attività effettuate, affinché possano essere ricostruiti con certezza tutti i tipi di rapporti intercorsi con i funzionari della pubblica amministrazione;
- ove applicabile, andranno osservate e assicurate le norme sulla trasparenza imposte alla pubblica amministrazione;
- la violazione della presente disposizione comporta l'immediata risoluzione del contratto eventualmente esistente.

Il divieto di cui al precedente punto opera anche nei confronti di tutti i dipendenti e dei singoli componenti del CdA e della Direzione Generale, nonché dell'Organo di controllo. Qualsiasi rapporto con rappresentati della P.A. per le finalità istituzionali dovrà essere autorizzato preventivamente dal CdA formalmente riunito in seduta. La presente disposizione non si applica alle ordinarie attività previste per gli adempimenti connessi al contratto di gestione del servizio di tesoreria e/o di cassa, rispettivamente per gli enti locali e gli istituti scolatici.

Il responsabile della funzione che conferisce l'incarico a terzi dovrà assicurare:

- una puntuale due diligence sulla terza parte, nonché l'analisi del razionale e la verifica di congruità e di effettività dell'attività da affidare alla terza parte;
- il continuo monitoraggio delle attività, avendo cura di:
  - acquisire adeguata documentazione con periodicità non superiore al trimestre;
  - fornire report informativi complessivi alla Direzione Generale, al CdA e all'OdV, con periodicità almeno semestrale.

In quanto compatibili si osservano le disposizioni a presidio del rischio di riciclaggio, con riferimento alle attività e buone prassi con le Persone Politicamente Esposte, nonché le disposizioni sulle politiche di remunerazione e quelle riguardanti i soggetti collegati.

Da ultimo:

È fatto obbligo organizzare e tenere (almeno su base annua) moduli di formazione delle risorse aziendali gestori di processi sensibili rispetto ai reati del Decreto.

A tal proposito, oltre al rispetto delle suddette prescrizioni, la U.O. responsabile della formazione e la U.O. responsabile/incaricata dell'ufficio risorse umane, ognuno per la parte di rispettiva competenza:

- in sede di rendicontazione dei dati e dei costi consuntivati, in base all'oggetto del finanziamento/contributo, devono verificare che tutte le spese risultino documentate, garantendone la tracciabilità;
- per lo svolgimento di attività ad opera di un service esterno provvedono alla stipulazione di appositi contratti/accordi, ove sia previsto che il soggetto fornitore ha l'obbligo di conformarsi alle prescrizioni del Codice Etico e, per quanto ad esso applicabile, del Modello ex. d.lgs. 231/2001 adottato dalla banca;
- provvedere ad un periodico flusso informativo a favore dell'OdV, con cadenza semestrale, con evidenza dei contributi ricevuti per le attività formative, nonché il numero dei partecipanti rispetto a ciascuna tipologia di attività formativa, assicurando esplicitamente l'OdV della effettiva partecipazione ai corsi da parte dei dipendenti.

Per assicurare la segregazione funzionale:

a) la U.O. ufficio personale predispone la documentazione necessaria per l'istanza di contributi/finanziamenti pubblici e della documentazione di rendicontazione del loro utilizzo;
b) l'Ufficio contabilità provvede alla contabilizzazione e gestione finanziaria dei contributi ottenuti;
c) il Tutor per la formazione verifica la documentazione prodotta (fabbisogni, prospetti, dichiarazioni e documenti vari).

Articolo 24-bis – Rischi in relazione ai delitti informatici e trattamento illecito dei dati

Come anticipato nella parte generale, I reati-presupposto richiamati dall'art. 24-bis, d.lgs. n. 231/2001 possono essere suddivisi, sulla base del bene giuridico da essi tutelato, in tre categorie. Nella prima categoria vanno ricondotti i reati contro la riservatezza informatica di cui agli artt. 615-ter, 615-quater, 617-quater e 617-quinquies c.p.. Nella seconda vanno ricompresi i reati contro la sicurezza informatica, contemplati agli artt. 615-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies c.p.. La terza categoria ha ad oggetto i reati informatici contro la fede pubblica di cui agli artt. 491-bis c.p. e 640-quinquies c.p..

Tra i reati contro la riservatezza informatica un ruolo centrale assume la fattispecie di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p., che si configura come un c.d. reato ostacolo, in quanto è volta a punire condotte prodromiche o preparatorie alla commissione di più gravi reati informatici (intercettazioni o danneggiamenti di dati o di sistemi informatici, frodi informatiche, ecc.). Il delitto in esame punisce il fatto di introdursi o di mantenersi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

La consumazione del delitto di accesso abusivo ad un sistema informatico o telematico si ha con l'introduzione in un sistema informatico o telematico protetto, vale a dire con la effettiva instaurazione di un dialogo logico con l'elaboratore, in violazione della volontà del titolare ovvero in mancanza di titolo autorizzativo. Ad integrare il reato non basta dunque il mero "inserimento" delle credenziali (login) necessarie per poter accedere al sistema informatico, ma occorre che il soggetto agente riesca ad "autenticarsi". Due sono le tipologie di condotte che vengono punite dall'art. 615-quater c.p.:

- la prima ha ad oggetto i comportamenti non autorizzati che consistono nel "far entrare" nella propria sfera di signoria parole chiave (password), codici di accesso ovvero altri mezzi (ad es. software o dispositivi tecnici) idonei a consentire l'accesso ad un sistema informatico altrui, protetto da misure di sicurezza ("si procura" o "riproduce");
- la seconda concerne le condotte che si sostanziano nel "mettere a disposizione" di terzi i menzionati "oggetti" materiali ("procura ad altri", "diffonde", "comunica" ovvero "consegna"). Il legislatore ha altresì punito la condotta, ulteriormente prodromica, del "fornire" istruzioni o indicazioni idonee a far entrare nella sfera di signoria altrui ovvero ad agevolare a terzi il conseguimento di mezzi o dispositivi idonei ad accedere abusivamente ad un sistema informatico.

Con riferimento ai reati contro la sicurezza informatica, mediante l'introduzione dell'art. 615-quinquies c.p., che ha subito significative modifiche a seguito dell'entrata in vigore della l. n.

48/2008, il legislatore ha voluto punire un ampio ventaglio di condotte prodromiche e preparatorie alla commissione dei più gravi reati di danneggiamento di dati, di informazioni o di programmi informatici (artt. 635-bis, 635-ter c.p.) ovvero di sistemi informatici o telematici (artt. 635-quater e 635-quinquies c.p.). Le condotte tipiche devono avere, quindi, ad oggetto "apparecchiature, dispositivi o programmi informatici". Mancando, però, ogni riferimento all'intrinseca dannosità o pericolosità dei "dispositivi" che devono essere oggetto delle condotte - di per sé "neutre" - di "procurarsi", "produrre", "diffondere", "importare", "distribuire" o "cedere", il contenuto d'offesa oggetto della norma incriminatrice viene fatto poggiare esclusivamente sul fine specifico di "danneggiare" illecitamente un sistema informatico o telematico oppure i dati in essi contenuti od ancora di "favorire l'interruzione", totale o parziale, o "l'alterazione del funzionamento" di un sistema informatico o telematico.

Infine, riguardo ai reati contro la fede pubblica, l'art. 491-bis c.p. riconduce il falso informatico che ha ad oggetto un documento informatico pubblico avente efficacia probatoria alle disposizioni sulle falsità in atti. Per documento informatico, la cui originaria definizione contenuta nell'art. 491-bis c.p. è stata opportunamente soppressa dall'art. 3, l. n. 48/2008, deve intendersi, in base alla nozione extra-penale offerta dall'art. 1, lett. p), d.lgs. 7.3.2005, n. 82 (c.d. "Codice dell'Amministrazione Digitale"), "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*". Ad essere tutelati sono soltanto i documenti informatici pubblici dotati di valenza probatoria.

Recenti studi criminologici dimostrano come molti dei comportamenti illeciti realizzati mediante l'utilizzo abusivo delle nuove tecnologie siano da attribuire ai c.d. insider, vale a dire a dipendenti infedeli[18]. Pertanto sono state /e vengono costantemente) individuate – anche attraverso l'intervento dell'outsourcer informatico - le vulnerabilità dei device, dei database e dei Server aziendali rispetto a possibili abusi, attacchi o minacce provenienti sia dall'interno (inside attacks) che dall'esterno (outside attacks), per adottare, anche in conformità alle best practise in materia di cyber security, efficaci misure di sicurezza di tipo fisico (hardware) e "logico" (software) per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati trattati e garantire, al contempo, l'affidabilità e la continuità dei servizi erogati. In definitiva, l'organizzazione aziendale si è dotata di una efficace policy sulla sicurezza informatica , che, nel rispetto dei limiti imposti dalla normativa in materia di privacy, prevede in particolare un sistema di auditing per la registrazione e l'archiviazione dei file di log relativi alle attività svolte mediante i sistemi informatici dai soggetti che operano all'interno della banca, apposite procedure di

[18] Si pensi, ad es., ai sempre più frequenti casi di accesso abusivo a sistemi informatici, di danneggiamento di dati e di sistemi informatici, di spionaggio industriale o politico realizzati mediante intercettazioni informatiche, ecc.

autenticazione dei dipendenti che utilizzano i device aziendali, nonché precise regole per il corretto utilizzo della posta elettronica, delle reti e dei dispositivi aziendali, così da evitare o ridurre il rischio che al suo interno vengano posti in essere comportamenti illeciti mediante l'utilizzo delle nuove tecnologie. Nondimeno si richiama in questa sede l'affidamento di compiti aggiuntivi ai fini dei controlli alla neocostituita U.O. Ufficio controlli interni cui tratta la comunicazione di direzione n. 15/2021 del 2/7/2021.

Si aggiunge che, attraverso l'approvazione della legge n. 238/2021 – in vigore dal 1° febbraio 2022 - per l'adeguamento alla direttiva n. 2013/40/UE, relativa agli attacchi contro i sistemi di informazione, taluni reati contenuti nel presente articolo sono stati modificati nella rubrica e nel loro contenuto.

L'esigenza di tale modifica scaturisce dal fatto che gli attacchi informatici su larga scala possono causare notevoli danni economici, sia attraverso l'interruzione dei sistemi di informazione e delle comunicazioni e sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati. Da qui la Direttiva UE chiede di particolare sensibilizzazione delle imprese (innovative) con riguardo alle minacce relative a tali attacchi e alla loro vulnerabilità agli stessi, in conseguenza della loro crescente dipendenza dal corretto funzionamento e dalla disponibilità dei sistemi di informazione, e della disponibilità, spesso limitata, di risorse da dedicare alla sicurezza delle informazioni.

Inoltre, posto che la comunicazione di informazioni può agevolare una migliore comprensione delle minacce attuali e future, contribuendo così a una più idonea e mirata formulazione di decisioni sulla lotta e la prevenzione degli attacchi contro i sistemi di informazione, la norma prevede che gli Stati membri trasmettano informazioni sul modus operandi degli autori dei reati a Europol e al suo Centro europeo per la lotta alla criminalità informatica, ai fini dell'effettuazione di valutazioni delle minacce e di analisi strategiche in merito alla criminalità informatica, conformemente alla decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di Polizia (Europol).

Descrizione dei Rischi in relazione ai reati contenuti nell'articolo 24-bis

In relazione ai delitti informatici e di trattamento illecito di dati, le aree di attività ritenute maggiormente a rischio, sono:

- rispetto ai reati informatici, le comunicazioni della Banca, mediante canali diretti o indiretti (internet, extranet, collegamenti dedicati, ecc.…), nei confronti di clienti, fornitori, dipendenti, Pubblica Amministrazione, Autorità di Vigilanza, banche e aziende di servizi, tramite l'utilizzo improprio o illegale di sistemi informatici, dispositivi hardware e infrastrutture IT aziendali;

- rispetto al reato di falsità in un documento informatico pubblico o avente efficacia probatoria, quelle relative al processo di gestione degli archivi informatici della Banca, che contengono i dati per la gestione dei rapporti con clienti, dipendenti, fornitori, attività soggette a vigilanza di autorità pubbliche in base a discipline di settore.

In considerazione dell'ampio spettro di aree potenzialmente a rischio, risultano sensibili tutti i processi IT riconducibili alla sicurezza informatica ed in particolare:

- la gestione della sicurezza fisica dei sistemi IT.
- la gestione della sicurezza logica, con particolare attenzione al controllo accessi a sistemi informativi e rete dati (rete aziendale, internet, extranet) e alla crittografia dei dati e/o del canale di comunicazione (ad esempio infrastrutture firewall, Reti private virtuali, ecc.), con la precisazione che tale attività viene svolta da società in outsourcing che è direttamente responsabile della sicurezza, come da contratto di riferimento ed in rispetto degli obblighi in materia di esternalizzazione di funzione aziendale importante;
- sviluppo e attuazione di sistemi di monitoraggio e revisione per la prevenzione e individuazione di attività non autorizzate/illecite sulla rete, sistemi e banche dati aziendali.
- la gestione delle principali procedure residenti nel sistema informatico a supporto del processo del credito, individuabili nelle seguenti:
  - gestione elettronica delle pratiche di fido;
  - gestione fidi e garanzie;
  - gestione poteri di erogazione del credito;
  - sistema di classificazione del rischio di credito;
  - monitoraggio rischi di credito (SARWEB, GRIG, PEG, Profilo Cliente, tabulati sconfini, rate in mora ecc. ed altri applicativi);
  - cruscotto direzionale.
  - Il sistema di gestione della firma grafometrica.

Più in particolare, l'art. 7 della legge 18 marzo 2008, n. 48 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero*" ha introdotto nel Decreto l'art. 24-bis[19] per i reati di:

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

La fattispecie riguarda l'alterazione e/o contraffazione di documenti informatici pubblici o privati, aventi efficacia probatoria (ad esempio attestazioni di pagamento di F23 e F24 online,

[19] In vigore dal 5/4/2008.

ordini elettronici di acquisto/vendita titoli, ecc), procurando alla banca un ingiusto profitto. La norma sancisce che i reati di falso in atto pubblico ed in scrittura privata (definiti con riferimento a documenti tipicamente cartacei) trovano applicazione anche quando la condotta illecita abbia ad oggetto "documenti informatici".

In banca la formazione di un documento informatico falso o falsificazione di un documento informatico pubblico o privato avente efficacia probatoria al fine di procurare a sé o ad altri un vantaggio attiene anche all'ambito del processo contabilità, bilancio e segnalazioni di vigilanza, nonché del processo relativo agli accertamenti bancari e alle segnalazioni all'Agenzia delle Entrate. In quest'ultimo caso, parte del processo è esternalizzato per gli adempimenti di natura informatica, rimanendo in capo alla Banca – segnatamente all'Area Operativa e alle U.O. da questi dipendenti – la responsabilità di convalidare i dati da trasmettere.

Oltre a quanto sopra, di seguito alcune delle ipotesi suscettibili di interesse e vantaggio della banca, che possono dare origine alle responsabilità di cui al D.lgs. 231/01:

a) rilascio elettronico di CUD intenzionalmente non corrispondenti al vero e alle disposizioni normative in materia;
b) apposizione di una data diversa dal reale pagamento di F23 e F24 on line;
c) alterazione delle disposizioni impartite dalla clientela per via informatica o nelle registrazioni informatiche di tali disposizioni (es. accettazione a trattamenti tutelati dalla privacy o in questionari antiriciclaggio e servizi intermediazione, etc.);
d) falsificazione nella fatturazione o utilizzo di fatture di cui si conosce la falsità, quest'ultimo caso anche con riferimento al processo del credito e segnatamente al servizio di anticipazione;
e) falsificazione di ordini di acquisto e vendita titoli elettronici o telefonici;
f) false attestazioni in relazione ai requisiti per l'ottenimento di finanziamenti agevolati da parte della banca e dei clienti nel caso in cui tali attestazioni dovessero essere rappresentate in documenti informatici;
g) utilizzo di documenti informatici di cui si conosce la falsità, pur non avendo partecipato alla falsificazione;
h) alterazione della documentazione presentata in giudizio (es. in sede di revocatoria), ove supportata da "documenti informatici" (indirettamente, anche l'alterazione dei supporti informatici che poi, stampati, sono presentati in giudizio sotto forma di documenti).

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

Fatto salvo quanto esposto nella parte generale circa taluni orientamenti giurisprudenziali, la norma punisce chiunque si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, anche nel caso in cui supera i limiti dell'eventuale originaria autorizzazione o protraendosi dopo la revoca del consenso o la richiesta di uscita.

In sintesi, la tipologia di reato, che si traduce nella violazione del sistema informatico protetto, può concorrere anche alla commissione del reato di frode informatica, che si differenzia quest'ultimo – come anche in precedenza spiegato – per la specifica finalità dell'accesso al sistema informatico al fine di alterarne i contenuti.

Con riferimento al reato di cui all'articolo 615-ter, sotto il profilo applicativo sono ipotizzabili i seguenti rischi, seppur non esaustivi:

a) accesso senza titolo utilizzando una password assegnata ad altra persona, ad una banca dati / information provider;
b) accesso e/o permanenza ad una piattaforma di sistema senza titolo o in violazione alle regole definite dal titolare dei diritti;
c) riproduzione/copia non autorizzata di programmi o notizie tramite l'accesso al sistema operativo di fornitori / clienti;
d) accesso abusivo ad informazioni di concorrenti conservate su database nell'ambito di servizi prestati o a mezzo di server condivisi;
e) utilizzo abusivo di una rete swift, rete bancomat o simili;
f) accesso ad informazioni di terzi conservate su sistemi informatici in occasione di malfunzionamenti dei sistemi (es. lettura di movimentazione di conti di clienti di concorrenti grazie a problemi nel server esterno comune).
g) Accesso ai dati del computer da restituire e/o HD esterni utilizzati per back-up locali;
h) Accesso ad internet per collegamenti ai siti pedopornografici

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)[20]

La norma punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa,

[20] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti codici, parole chiave o altri mezzi idonei all´accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Si tratta di una condotta prodromica a quella sanzionata dall'art. 615-ter, la cui punibilità viene anticipata sino al momento antecedente a quello dell'accesso. Si ritiene che i casi applicativi siano riconducibili a:

a) condivisione di password, licenze, codici di accesso a sistemi informatici e telematici, e database;
b) condivisione di chiavi e carte per l'accesso ai locali ove sono custoditi sistemi;
c) diffusione di codici per l'attivazione di programmi;
d) fornitura di strumenti atti a consentire l'accesso a sistemi e reti (es. particolari programmi di decriptazione o hardware specifico);
e) nel caso di alienazione/restituzione dei pc, inefficace cancellazione dei dati per mancata validazione dell'applicativo che quindi consentirebbe l'accesso da parte di soggetti non autorizzati;
f) nell'ambito del processo di manutenzione, installazione e utilizzo di SW di controllo e/o di monitoraggio da remoto;
g) download ed upload di documenti protetti dal diritto d'autore, anche attraverso la rimozione della protezione dei supporti informatici e loro duplicazione;
h) Firme digitali abusive;
i) disegno dell'architettura di rete che intenzionalmente e strutturalmente consenta l'accesso e utilizzo abusivo;
j) sottrazione di credenziali per l'accesso a banche dati esterne, protette da misure di sicurezza, allo scopo di ottenere informazioni commerciali o confidenziali.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) [21]

Si configura il reato allorquando qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso

[21] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

pertinenti ovvero di favorire l´interruzione, totale o parziale, o l´alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Al riguardo si evidenzia che, in linea generale, la norma mira a contrastare i casi di diffusione dei virus informatici, ma estende, per altro verso, la sua applicabilità alla complessiva attività volta a danneggiare l'integrità e la funzionalità dei sistemi informatici e telematici e delle informazioni ivi contenute. È il caso per esempio:

a) dell'attività di spamming attraverso la pubblicizzazione di prodotti tramite e-mail senza l'autorizzazione del destinatario o la creazione dei programmi necessari per farlo.
b) dell'introduzione deliberata di codici malevoli all'interno di banche dati esterne allo scopo di compromettere la confidenzialità delle stesse, arrecando un danno reputazionale ai concorrenti;
c) dell'introduzione nella sala server per la violazione delle banche dati e la conseguente alterazione dei contenuti.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [22]

La norma punisce chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi; la stessa norma punisce anche chiunque rivela al pubblico, in tutto o in parte, mediante qualsiasi mezzo di informazione, il contenuto delle comunicazioni così intercettate, impedite o interrotte.

Fatte salve le configurazioni di reato previste da altre normative, quali la privacy, i casi in cui si potrebbe configurare un interesse ed un vantaggio per la banca attengono alla fraudolenta intercettazione di conversazioni telefoniche, di comunicazioni informatiche o e-mail, quali:

a) informazioni rilasciate tra cliente ed operatore intercettate da altro operatore e da questi, o da altri, diffuse nel caso di raccomandazioni su strumenti finanziari quotati;
b) informazioni industriali di terzi e competitor intercettate su reti e servicer condivisi;
c) l'intercettazione da parte di terzi in azienda di informazioni trasmesse ad un dipendente "di fiducia" da parte di un cliente.

[22] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [23]

La norma estende la sanzionabilità alle attività prodromiche al reato di cui all'art. 617-quater, laddove vi sia installazione di apparecchiature (i.e. software) a ciò preposte. Quindi essa punisce chiunque, 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 ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, salvi i casi consentiti dalla legge.
Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio.

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

È il caso di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.
Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio.

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.)

Si persegue colui che commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio.

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

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

[23] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio.

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

La norma punisce i casi di cui all'articolo 635-quater qualora diretti a sistemi informatici o telematici di pubblica utilità.

Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio.

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

Il reato punisce il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Elemento costitutivo della fattispecie di reato è la qualifica di "certificatore di firma elettronica" in capo all'agente.

Non si ravvedono ipotesi che possano concretizzarsi in banca o quantomeno che possa realizzarsi un interesse o un vantaggio, posto che la Banca non svolge la funzione di Autorità Certificatore, pur utilizzando il sistema di firma grafometrica.

Presidi organizzativi e gestionali

In premessa, occorre precisare che anche la mitigazione di una criticità rappresenta un miglioramento, essendo ormai chiaro a tutti che il "rischio zero" non esiste.

A presidio delle possibili ipotesi di reato, come sopra indicate, la Banca garantisce la compliance – anche ai fini dell'osservanza delle disposizioni di vigilanza previste dalla Circolare 285/2013 di Banca d'Italia - in tema di sicurezza informatica attraverso i seguenti documenti di governo:

1) Policy aziendale di sicurezza informatica costituisce un insieme di obiettivi, principi di sicurezza e pratiche che la Banca recepisce nelle proprie procedure. L'ambito di applicazione riguarda le informazioni contenute nei software applicativi, software di sistema, database, sistemi hardware e nell'infrastruttura di rete gestita dall'outsourcer ICT principale e in via residuale da ulteriori fornitori terzi. Le disposizioni e le indicazioni in essa contenute si applicano a tutte le unità organizzative della Banca e sono conosciute, comprese e attuate da tutto il personale interno e dalle terze parti che svolgono le proprie attività nell'ambito dei processi della Banca e/o di contratti di fornitura con la stessa, sia che tali attività siano svolte presso le aree ed i locali della Banca stessa, sia che siano svolte presso altre sedi. Inoltre, la

Policy è redatta, oltre che sulla base delle suindicate disposizioni, anche sulla base dei seguenti standard e best practise internazionali:

- ISO/IEC 27001:2013 "Information technology— Security techniques — Information security management systems — Requirements.
- ISACA Control Objectives for Information and related Technology (COBIT) 5.0.

2) Il processo di analisi del rischio informatico nel quale sono descritte le fasi del processo di analisi del rischio informatico, declinando operativamente il documento "*Metodologia di analisi del rischio informatico*", con particolare attenzione ai flussi informativi utilizzati e a quelli prodotti dall'attività di analisi del rischio informatico e alle fasi di interazione tra la Banca e l'outsourcer ICT principale. Al riguardo si evidenzia che il processo di analisi del rischio informatico integra, per gli aspetti relativi all'Information Technology le normative e i regolamenti dell'outsourcer ICT e della Banca, in particolare in riferimento alla Banca: il Risk Appetite Framework (RAF), che fornisce il quadro di riferimento per la determinazione della propensione al rischio della Banca e il modello dei Rischi Operativi. Inoltre, il documento identifica le fasi e gli attori coinvolti nella valutazione del rischio informatico e nell'attuazione degli eventuali trattamenti necessari per la riduzione del rischio ad un livello accettabile.

3) Documento sulla metodologia di analisi del rischio informatico, con lo scopo di definire i principi e le regole per la valutazione, la gestione, il controllo e il reporting dei rischi informatici per la Banca. Tale metodologia:

   a) si applica alle categorie di rischio che impattano sul sistema informativo e sulle risorse ICT, che possono comportare perdite economiche, di reputazione e di quote di mercato per la Banca;

   b) recepisce le linee guida emanate a suo tempo nell'ambito di progetti di categoria sul tema ed è in linea con la metodologia di gestione del rischio della Banca;

   c) è redatta in conformità con quanto richiesto dal 15° Aggiornamento della Circolare 263/2006 emanata da Banca d'Italia (ora 285/2013) ed in coerenza con la policy di sicurezza informatica.

   d) è allineata all'analoga metodologia di gestione del rischio informatico utilizzata dall'outsourcer BCC Sistemi Informatici S.p.A.

4) Il documento relativo alla governance ICT ed il modello organizzativo, nel cui ambito sono definiti ruoli e responsabilità, anche in coerenza con il Regolamento Generale d'Istituto, secondo quanto previsto dal 15° aggiornamento della Circolare 263/2006, con particolare riferimento ai seguenti ambiti:

   - Governance ICT

- Gestione del rischio informatico;
- Sicurezza informatica;
- Data Governance,

avendo in considerazione il fatto che il modello organizzativo considera la struttura della Banca in ambito ICT, ovvero un full-outsourcing del sistema informativo aziendale che prevede attività in banca principalmente inerenti al coordinamento ed al monitoraggio delle attività operative svolte dall'outsourcer.

5) La procedura per la gestione dei cambiamenti per definire le attività necessarie alla gestione dell'insieme delle strutture tecnologiche ed applicative che costituiscono i sistemi informativi della Banca, con l'obiettivo di garantire la riservatezza, l'integrità e la disponibilità delle informazioni. L'ambito di applicazione riguarda le modifiche, evolutive e correttive, al software applicativo, al software di sistema, al database, alla schedulazione, ai sistemi hardware e all'infrastruttura di rete gestito dall'outsourcer ICT principale e in via residuale da ulteriori fornitori esterni.

6) La procedura per la gestione degli incidenti di sicurezza che occorrono sull'insieme delle strutture tecnologiche ed applicative che costituiscono i sistemi informativi della Banca, con l'obiettivo di minimizzare l'impatto di eventi avversi sui processi bancari e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti. L'ambito di applicazione riguarda gli incidenti al software applicativo, al software di sistema, al database, alla schedulazione, ai sistemi hardware e all'infrastruttura di rete gestito dall'outsourcer ICT principale e in via residuale da ulteriori fornitori esterni.

7) Il regolamento per la gestione del processo di firma grafometrica, nel cui ambito sono disciplinati sia gli aspetti normativi e sia tecnici, nonché sono disciplinate le principali misure tecniche e organizzative su cui si basa la soluzione e la descrizione della procedura organizzativa per la gestione dell'intero processo presso la rete di vendita e nell'ambito delle U.O. di back office. Allegato a tale documento segue la relazione tecnica e organizzativa rilevante ai fini del presidio di cui alla delibera del garante n. 513 del 12 novembre 2014, ai fini del trattamento biometrico dei clienti.

Si aggiungono:

8) Un sistema di reportistica dettagliato destinato agli organi apicali da parte di ciascun responsabile di processo, riunito nel documento denominato "Governance ICT – Flussi";

9) La Policy di Data Governance, inquadrata nel più generale standard di Data Governance della Banca, che ha l'obiettivo di descrivere i requisiti, i principi ed i processi adottati al fine di

garantire che i dati aziendali siano adatti agli scopi per i quali sono utilizzati, protetti ed affidabili a tutti i livelli dell'organizzazione ed in tutte le funzioni e posizioni. La policy si pone i seguenti obiettivi:

a) fornire al CDA e a tutte le strutture deputate al governo dei dati le indicazioni per l'esercizio dei propri ruoli e responsabilità necessari alla gestione del dato come asset strategico;

b) garantire che tutte le parti coinvolte nella governance dei dati siano responsabili per il mantenimento ed il successo nelle attività a loro assegnate.

10) La Policy di Data Quality, anch'essa inquadrata nel più generale standard di Data Governance della Banca, che ha l'obiettivo di descrivere la struttura ed i modelli di gestione della qualità dei dati adottati per adempire alle richieste di Banca d'Italia contenute nelle disposizioni di vigilanza. Al riguardo si evidenzia che la gestione della qualità dei dati è l'insieme dei modelli, metodologie e strumenti volti ad assicurare che le informazioni contenute nel sistema informativo aziendale abbiano un livello di affidabilità adeguato a garantire la gestione dei rapporti con la clientela e/o a supportare le attività di governo e di rendicontazione esterna (adempimenti obbligatori normativi). A tal fine la Banca ha definito il proprio modello di governo delle informazioni e delineato l'impianto metodologico, organizzativo, procedurale e strumentale attraverso un:

- **Modello metodologico** per la gestione della qualità dei dati aziendali, in cui sono normate e definite le dimensioni di analisi della qualità, le metriche di valutazione correlate, le modalità di applicazione dei pesi e delle soglie, necessarie ad impostare efficacemente i controlli;
- **Modello organizzativo**: che indica ruoli e responsabilità dei differenti attori coinvolti a vario titolo nei processi di gestione della qualità dell'informazione, come descritto nel documento di definizione dello standard di Data Governance;
- **Modello procedurale:** che descrive il funzionamento dei processi di gestione della qualità dei dati, indipendentemente dagli ambiti di applicazione:
  - Progettazione, Realizzazione e Avvio degli apparati di controllo;
  - Esercizio degli Apparati di Controllo e conseguenti azioni correttive;
  - Regia e monitoraggio del sistema.
- **Modello architetturale**: che delinea e descrive le tipologie di controllo, le regole per la determinazione dei punti di innesto sui processi di estrazione ed elaborazione dati e le componenti logiche dell'architettura di riferimento.

11) Banca d'Italia, con l'emissione della Circolare n. 263 – 15° aggiornamento di luglio 2013, ha richiesto alle Banche la definizione e l'adozione di uno Standard di Data Governance. A tal fine, la Banca riconoscendo il valore derivante da una corretta gestione dei dati che, oltre a produrre immediati effetti sulla sicurezza delle informazioni e sul rispetto degli obblighi normativi, può contribuire alla riduzione dei costi e degli errori dovuti alla bassa qualità delle informazioni, si è dotata di uno standard di Data Governance funzionale ad una gestione efficace ed efficiente dei dati aziendali, in cui si definisce quanto segue:

- il quadro normativo ed i requisiti regolamentari in ambito Data Governance considerati per la redazione dello standard;
- il perimetro di applicazione dello standard di Data Governance, inclusa la componente di Data Quality;
- i ruoli e le responsabilità delle funzioni coinvolte nell'utilizzo, gestione e controllo delle informazioni aziendali;
- gli obiettivi, le linee guida, i principi, i processi ed i controlli;
- i Key Performance Indicator (KPI), volti a valutare e monitorare il raggiungimento degli obiettivi della Data Governance;
- le modalità di comunicazione e training previste al fine di rendere le risorse della Banca consapevoli delle tematiche e delle proprie responsabilità in ambito Data Governance.

Da ultimo, si richiama in questa sede:

12) Il Disciplinare interno sull'uso della posta elettronica e di internet.

13) Il sistema dei controlli interni, nel cui ambito si evidenzia il regolamento e l'applicativo informatico di controllo in materia di circolazione delle informazioni in ambito bancario e tracciamento delle operazioni bancarie (di cui al Provvedimento Generale del Garante per la protezione dei dati personali del 12 maggio 2011), dove è prevista l'adozione di specifiche misure di sicurezza per il trattamento di dati personali della clientela al fine di garantire il rispetto dei princìpi in materia di protezione dei dai personali in ordine ai temi della "circolazione" delle informazioni riferite ai clienti in ambito bancario e della "tracciabilità" delle operazioni bancarie effettuate dai dipendenti delle banche (sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, c.d. inquiry).

14) Attività di formazione e sensibilizzazione del personale sui temi specifici della sicurezza informatica nell'ambito di progetti di categoria.

Protocolli Specifici

In premessa, occorre precisare che anche la mitigazione di una criticità rappresenta un miglioramento, essendo ormai chiaro a tutti che il "rischio zero" non esiste.

Oltre ai protocolli esistenti e già citati in precedenza con riferimento ad altre fattispecie di rischio, la Banca provvede a mappare attori, ruoli e responsabilità, incaricando una U.O. che funge da punto di riferimento per tutte le attività legate alla sicurezza informatica, ossia il responsabile dell'Ufficio Organizzazione. Il profilo ricopre ruolo di responsabilità. Ed a tal fine ha visibilità su tutti i processi chiave ed è in grado di relazionarsi adeguatamente con le diverse figure aziendali.

Peraltro, tale U.O. è sempre in grado di assicurare i seguenti parametri: (i) l'elemento di sistema, (ii) chi vi accede (iii) perché vi accede, (iv) come vi accede e (v) da dove vi accede. Quindi viene anche conseguentemente adottata la politica dei privilegi minimi, ovvero ogni figura aziendale può avere accesso solo alle informazioni che gli sono necessarie e per il tempo necessario.

Al riguardo, la Banca tiene conto del fatto che il «Fattore Umano» rappresenta il primo e più grave rischio per la Sicurezza, posto che le misure tecnologiche da sole non bastano, pertanto, ritiene essenziale la strada della formazione periodica e dell'informazione puntuale su rischi emergenti, perché motiva i collaboratori e crea competenza, consapevolezza e collaborazione. A tal fine occorre mantenere alta l'attenzione di tutti i collaboratori sulle molteplici tipologie di rischio che si incontrano nell'attività lavorativa e nella vita privata.

E ancora. Il percorso di conformità al GDPR rappresenta l'occasione per mappare in modo sistematico i trattamenti di dati personali che avvengono in azienda e attuare misure organizzative e tecnologiche di protezione e mitigazione dei rischi.

Inoltre, la banca ha predisposto e adottato i seguenti strumenti:

- Politiche di sicurezza e Privacy, diffuso tra le funzioni aziendali e consegnato a tutti i neoassunti al momento della sottoscrizione del contratto;
- L'individuazione di risorsa nell'ambito del Servizio Organizzazione preposta alla sicurezza informatica, con funzioni di Security Manager, responsabile, peraltro, della gestione delle principali procedure residenti nel sistema informatico a supporto del processo del credito, il quale si interfaccia con il corrispondente Security Manager dell'outsourcing, mediante sistema di autenticazione con chiave hardware.
- Audit periodici sul sistema informatico;

Misure tecniche e tecnologiche quali:

- URL Filtering;
- Gestione dei Proxy;
- Spam Monitoring;
- Installazione e aggiornamento di sistemi antivirus e firewall.

La banca ha – inoltre - adottato le seguenti misure:

- Protocolli organizzativi specifici destinati a regolamentare l'acquisto di software e l'approvvigionamento di altri beni protetti da proprietà intellettuale.
- Monitoraggio su software, programmi e applicazioni informatiche, dove sono definite le regole per l'utilizzo degli strumenti informatici aziendali e le attività di controllo su software, programmi, applicazioni informatiche installate su tali dispositivi, al fine di verificare che non vengano scaricate applicazioni potenzialmente utili alla commissione di attività illecite e / o contrarie alle disposizioni aziendali definite (es. manomettere il sistema informatico di terzi, accedere impropriamente al sistema dei pagamenti interno per finanziare la commissione di reati 231).
- Controllo sicurezza su accesso a sistemi, dove sono definiti criteri e regole di autorizzazione per l'accesso ai sistemi informatici aziendali; tali accessi vengono costantemente monitorati in termini di utenti che vi accedono e attività consentite. Vengono inoltre implementate adeguate misure di sicurezza che impediscano l'accesso al sistema informativo da parte di terzi non autorizzati (dotazione di firewall).
- Monitoraggio periodico sugli amministratori di sistema, nel cui ambito vengono attuate specifiche attività di controllo sull'attività degli amministratori di sistema e su software, programmi e applicazioni presenti sui loro dispositivi informatici.

Flussi informativi a favore dell'OdV

Il responsabile dell'Ufficio Organizzazione assicura flussi informativi – su base semestrale e/o all'occorrenza – riguardo ai risultati dei controlli riguardanti l'intero comparto, sia quelli effettuati in via diretta e sia quelli desunti dalle attività di verifica di tutte le funzioni aziendali di controllo, rilevabili nelle attività di raccordo cui provvede la U.O. incaricata all'Ufficio Controlli.

Articolo 24-ter - Delitti di criminalità organizzata

L'art. 2 della Legge 15 luglio 2009, n. 94 "*Disposizioni in materia di sicurezza pubblica*" ha introdotto nel decreto l'art. 24 ter[24] per i seguenti reati:

1) Associazione per delinquere (art. 416, comma 6 c.p.), ossia per la commissione dei reati di cui agli artt. 600, 601 e 602 di cui in precedenza
2) Associazione di tipo mafioso (art. 416 bis c.p.)[25]
3) Scambio elettorale politico-mafioso (art. 416 ter c.p.)
4) Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.)
5) Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 309/90)[26]
6) Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91)
7) Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o parti di esse, di esplosivi, di armi clandestine nonché di armi comuni da sparo, escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, comma 2, lettera a), numero 5 c.p.p.).

Descrizione dei Rischi in relazione ai reati contenuti nell'articolo 24-ter

Va evidenziato che, sotto il profilo oggettivo, seppure la Banca operi in territorio particolarmente esposto a rischio criminalità organizzata, si ritiene improbabile la realizzazione di un ipotetico accordo criminale fra il personale (dirigenti e/o Operatori) per procurare all'associazione (e quindi alla Banca) interessi o vantaggi con la commissione di autonomi reati fine.

Purtuttavia, le attività potenzialmente a rischio, per tali intendendosi le operazioni finanziarie con soggetti terzi o comunque operazioni sospette, individuate con riferimento alle sopra citate normative, fermo restando che le medesime, per rilevare ai fini della normativa 231/01 debbono essere poste in essere da apicali o subordinati nell'interesse o a vantaggio dell'azienda, sono:

- la gestione di operazioni che per caratteristiche, entità o natura o per qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, inducano a ritenere – in base agli elementi a disposizione ed utilizzando

[24] In vigore dall'8/8/2009.
[25] Articolo modificato dalla Legge n.69/2015.
[26] Comma 7-bis aggiunto dal D. Lgs. n. 202/2016.

la normale diligenza – che il denaro, i beni o le utilità oggetto delle operazioni medesime possano provenire da delitto;

- operazioni attuate con persone di cittadinanza non comunitaria nel territorio dello Stato italiano, ovvero con persone straniere che non hanno titolo di residenza;
- intrattenimento di rapporti con soggetti coinvolti in procedimenti giudiziari di natura penale, in particolare in veste di imputati, testimoni o di persone informate dei fatti;
- gestione delle risorse finanziarie della banca (incassi e pagamenti);
- gestione delle carte di credito corporate, note spese e anticipi;
- i rapporti con la P.A. collegati alla richiesta e fruizione di finanziamenti o benefici erogati dallo Stato, la Comunità Europea e altri Enti pubblici locali, nazionali o comunitari;
- gestione dei rapporti con l'amministrazione della giustizia nell'ambito o in occasione di procedimenti giudiziari di natura civile, amministrativa, tributaria e penale, che coinvolgano la banca;
- gestione di procedure per l'ottenimento di fondi o contributi da parte delle PP.AA. italiane o comunitarie;
- selezione, assunzione e gestione del personale;
- gestione di sponsorizzazioni;
- gestione di dotazioni e utilità aziendali (es. pc, autovetture etc.);
- gestione dei rapporti con l'amministrazione della giustizia nell'ambito o in occasione di procedimenti giudiziari di natura giuslavoristica che coinvolgano la banca;
- gestione dei rapporti con i fornitori di beni e/o servizi (consulenze o prestazioni d'opera).

Regole di carattere generale

Gli organi sociali della Banca ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate. In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- realizzare correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività di gestione delle risorse finanziarie;
- monitorare e tener traccia della provenienza e dell'impiego dei flussi finanziari, dei beni e delle altre risorse aziendali, nonché delle operazioni compiute in relazione ad essi;

- prestare attenzione e controllo su operazioni che per caratteristiche, entità o natura o per qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, inducano a ritenere – in base agli elementi a disposizione ed utilizzando la normale diligenza – che il denaro, i beni o le utilità oggetto delle operazioni medesime appaiano di provenienza delittuosa.

In particolare, si indicano i seguenti principi generali di comportamento, i dati e le informazioni su clienti, fornitori e consulenti sono completi e aggiornati, in modo da garantire la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica del loro profilo;

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella presente Modello.

Protocolli specifici

Oltre alle regole generali di organizzazione individuate nel presente documento - che sono applicate in via generale in relazione a tutte le attività sensibili individuabili ai sensi del Decreto e che devono informare i presenti principi speciali oltreché i relativi protocolli e procedure aziendali - sono stati identificati, i seguenti principi specifici di comportamento, quali misure di prevenzione e controllo, che saranno meglio specificati, ove del caso, negli ulteriori protocolli e procedure aziendali richiamate:

- La selezione dei fornitori locali in generale è effettuata tramite una comparazione economica di diverse proposte pervenute da fornitori diversi.
- La scelta dei fornitori in genere è effettuata dall'Area/Ufficio competente, previa verifica della loro affidabilità e reputazione sul mercato, nonché la verifica della loro assenza dalle liste utilizzate a fini di prevenzione del rischio di riciclaggio.
- È predisposto un elenco dei fornitori qualificati della banca costantemente aggiornato, in modo da garantire sempre la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica periodica del loro profilo.
- Sono stabilite idonee modalità di raccolta e conservazione della documentazione relativa al processo di selezione, valutazione e gestione del fornitore, dell'appaltatore o comunque della controparte contrattuale e di verifica dei requisiti di reputazione, onorabilità e affidabilità.

Flussi informativi a favore dell'OdV

Annualmente il responsabile del servizio infrastrutture e spese produce report all'OdV con l'elenco dei fornitori e delle controparti commerciali in genere con cui la Banca intrattiene

rapporti. L'OdV, nell'ambito della propria attività di vigilanza, può richiedere copia della documentazione di supporto all'attività di valutazione e selezione effettuata dalla banca.

Parimenti, il Local Data manager e i referenti per la gestione delle verifiche tributarie, precontenzioso e contenzioso, nonché il referente per le attività esternalizzate per tali servizi, rispettivamente e per la parte di ciascuna competenza, assicureranno flussi informativi annuali e/o all'occorrenza in merito alle attività da ciascuno gestite ed in merito ai controlli effettuati.

A fattor comune, per ciascun processo sensibile, il Responsabile Interno deve:

- tenere a disposizione dell'OdV ogni eventuale documentazione di supporto;
- segnalare all'OdV e richiedere la sua assistenza per ogni situazione che si ritenga non conforme alle regole aziendali in materia o laddove si evidenzi comunque una situazione di anomalia.

Articolo 25-bis - Reati di falsità in monete, in carte di pubblico credito e in valori di bollo e in strumenti o segni di riconoscimento

Le norme relative a tale tipologia di reato sono finalizzate a tutelare la fede pubblica.

Come spiegato nella parte generale, le fattispecie di reato suindicate sono configurabili perlopiù nell'ambito di realtà imprenditoriali appositamente strutturate per svolgere attività economiche illecite.

Nella fattispecie sono previsti i seguenti reati:

1) Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
2) Alterazione di monete (art. 454 c.p.)
3) Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
4) Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
5) Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.) e uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
6) Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
7) Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
8) Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
9) Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art.473 c.p.).

Le condotte relative ai suindicati articoli possono essere distinte in:

i. contraffazione, ossia produzione di valori da parte di chi non è autorizzato, in modo da ingannare il pubblico e, quindi, ledere gli interessi tutelati dalla norma;
ii. alterazione, ossia modifica delle caratteristiche materiali o formali di valori genuini, volta a creare l'apparenza di un valore monetario diverso;
iii. introduzione, che consiste nel far giungere nel territorio dello Stato valori altrove contraffatti;
iv. detenzione, che rappresenta la disposizione, a qualsiasi titolo, dei valori contraffatti o alterati;

v. spendita e messa in circolazione di valori contraffatti o alterati, ossia utilizzare come mezzo di pagamento o far uscire dalla propria sfera di custodia, a qualsiasi titolo, i valori contraffatti o alterati;

vi. acquisto o ricezione di valori falsificati da parte di un contraffattore o di un intermediario al fine di metterli in circolazione.

Descrizione dei Rischi in relazione ai reati contenuti nell'articolo 25-bis

Con riferimento ai rischi, si ritiene che in relazione alle tipologie dei reati di falsità in monete, in carte di pubblico credito e in valori di bollo, non appare ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti della Banca pongano in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio della Banca stessa, fatti di falsificazione e di alterazione di monete, di valori di bollo o di carta filigranata in uso per la fabbricazione di carte di pubblico credito.

Parimenti, non si ritiene, inoltre, probabile che siano commessi, nell'interesse o a vantaggio della Banca, i reati di spendita e introduzione nello Stato di monete falsificate da parte degli operatori delle Filiali, poiché:

- le modalità di realizzazione del reato appaiono tali da procurare un vantaggio economico esclusivamente al dipendente che lo commette;
- i falsi statisticamente rilevati rappresentano una minima percentuale sul totale dei flussi movimentati.

Trattasi, in sostanza, di reati di difficile realizzazione che, tuttavia, l'ABI ha ipotizzato, limitatamente ad alcune fattispecie, come realizzabili nel caso in cui la Banca non fornisca ai dipendenti apparecchiature o mezzi di riconoscimento che consentano l'identificazione delle monete falsificate.

Regole di carattere generale

La Banca in ogni caso profonde le dovute energie nella prevenzione e repressione dei reati di falso ed a richiamare l'attenzione dei dipendenti sul puntuale rispetto delle procedure di controllo dei valori trattati, prevedendo tra l'altro - in caso di sospetta falsità - l'immediato ritiro dalla circolazione.

Gli organi sociali della banca ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate. In coerenza con le procedure aziendali, i medesimi hanno l'obbligo di:

- vigilare sui processi di approvvigionamento;
- agire con clienti e fornitori in modo trasparente e collaborativo, nel rispetto della normativa vigente;
- essere in grado di garantire al cliente che i prodotti e i servizi forniti siano in possesso di tutte le caratteristiche e le qualità promesse e dichiarate;
- rispettare la proprietà industriale di terzi nello svolgimento delle attività di ricerca e sviluppo, di marketing e di tutte le attività che comportano l'utilizzo di loghi e marchi;
- informare le proprie azioni all'ottenimento di risultati competitivi che premino la capacità, l'esperienza e l'efficienza evitando qualsiasi azione diretta ad alterare le condizioni di corretta competizione.

In coerenza con il Codice Etico e le procedure aziendali, agli organi sociali della banca ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti è inoltre espressamente fatto divieto di:

- contraffare, alterare marchi o segni distintivi ovvero di brevetti, modelli e disegni ovvero usarli senza una preventiva analisi di anteriorità;
- commercializzare prodotti con marchi e/o segni distintivi alterati o contraffatti.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste dal presente Modello.

Protocolli Specifici

Valgono a presidio del rischio le regole e gli adempimenti indicati nel regolamento "*Regolamento per la gestione e il trattamento del contante*" e il "*Regolamento di cassa*".

Flussi informativi a favore dell'OdV

Per ciascun processo sensibile, il Responsabile Interno deve:

- tenere a disposizione dell'OdV ogni eventuale documentazione di supporto;
- segnalare all'OdV e richiedere la sua assistenza per ogni situazione che si ritenga non conforme alle regole aziendali in materia o laddove si evidenzi comunque una situazione di anomalia.

Ciascun responsabile di area territoriale produrrà report semestrale sulle attività previste nei suddetti regolamenti e sui rispettivi controlli effettuati nel periodo di riferimento.

Parimenti il responsabile della cassa centralizzata per i valori in bianco fornirà report semestrale in merito alla gestione dei valori in bianco e di ogni tipologia di controllo che ha effettuato nel periodo.

Articolo 25-bis.1 - Delitti contro l'industria e il commercio

Le fattispecie criminose sono funzionali alla repressione delle frodi commerciali e industriali, il cui scopo è quello di disincentivare politiche aziendali volte ad alterare la concorrenza in danno di consumatori.

Di seguito l'elenco dei reati:

1) Turbata libertà dell'industria o del commercio (art.513 c.p.)
2) Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.)
3) Frodi contro le industrie nazionali (art. 514 c.p.)
4) Frode nell'esercizio del commercio (art. 515 c.p.)
5) Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
6) Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
7) Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.)
8) Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.)

Avuto riguardo alla specificità dell'attività svolta dalla Banca, non si ritiene possibile la realizzazione di alcuno dei reati previsti dalla normativa in questione.

Regole di carattere generale

Gli organi sociali della banca ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- vigilare sui processi di approvvigionamento;
- agire con clienti e fornitori in modo trasparente e collaborativo, nel rispetto della normativa vigente;
- essere in grado di garantire al cliente che i prodotti e i servizi forniti siano in possesso di tutte le caratteristiche e le qualità promesse e dichiarate;
- rispettare la proprietà industriale di terzi nello svolgimento delle attività di ricerca e sviluppo, di marketing e di tutte le attività che comportano l'utilizzo di loghi e marchi;

- informare le proprie azioni all'ottenimento di risultati competitivi che premino la capacità, l'esperienza e l'efficienza evitando qualsiasi azione diretta ad alterare le condizioni di corretta competizione.

In particolare, è fatto divieto di attuare comportamenti tali da far sì che siano commercializzati prodotti:

- con caratteristiche differenti rispetto a quanto rappresentato ai consumatori sia sulla confezione del bene, sia attraverso campagne pubblicitarie;
- utilizzando marchi o brevetti di proprietà industriali di terzi;
- che riportino indicazioni o denominazione non corrispondenti all'effettiva origine, provenienza e qualità.

Protocolli Specifici

Il coinvolgimento della Banca – in via del tutto astratta – potrebbe scaturire nell'ambito di attività di sponsorizzazioni, il cui processo appare ben presidiato attraverso le regole indicate nel regolamento "*Infrastrutture e spese*".

Ai fini della prevenzione dei reati richiamati dall'art.25-bis.1, costituisce, altresì, protocollo di prevenzione indirizzato a tutte le Unità Organizzative il regolamento relativo al rischio di non conformità alla normativa Antitrust cui tratta la delibera AGCM n. 25411 del 1° aprile 2015, adottata dalla banca in data 15/7/2015, nonché a policy del GBCI diramate nel tempo.

Flussi informativi a favore dell'OdV

I responsabili della Direzione Marketing e dell'Ufficio Organizzazione provvedono annualmente e/o all'occorrenza ad informare l'OdV dell'esito delle attività compiute e degli eventuali controlli effettuati come disciplinato nel sopracitato regolamento.

Articolo 25-ter Reati societari

L'art. 3 del decreto legislativo 11 aprile 2002, n. 61, nell'ambito della riforma del diritto societario ha introdotto l'art. 25 ter[27] per le seguenti ipotesi di reato:

False comunicazioni sociali (art. 2621 c.c.)[28] - Fatti di lieve entità (art. 2621-bis c.c.) - False comunicazioni sociali in danno dei soci o dei creditori (art. 2622) [29]

Il reato di false comunicazioni sociali consiste nella condotta posta in essere da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, consapevolmente espongono nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società, in modo concretamente idoneo ad indurre altri in errore. Esso si consuma con la sola esposizione di fatti non rispondenti al vero nei bilanci, nelle relazioni o in altre comunicazioni sociali ovvero con l'omissione di informazioni la cui comunicazione è obbligatoria per legge.

In banca il reato può verificarsi qualora vengano esposti nei bilanci, nelle relazioni o nelle comunicazioni sociali fatti materiali non veritieri, ovvero vengano omesse informazioni obbligatorie relative alla situazione economica, patrimoniale e finanziaria per ingannare i soci o il pubblico. Non sembra rilevare, di converso, le informazioni di tipo "qualitativo", inidonee ad alterare in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della banca.

Potrebbe anche verificarsi il caso in cui vengano ricevuti versamenti estemporanei a parziale copertura di sofferenze - soprattutto quando è un garante a fare il versamento - senza talvolta decurtare le somme percepite dal totale della sofferenza, al fine di non far conoscere l'informazione ad altre banche esposte, accantonando l'importo in un fondo a parte.

Altro rischio che potrebbe rilevare è rappresentato dalla sottostima delle svalutazioni delle sofferenze quale manovra di bilancio.

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

Ai fini della responsabilità della società, rileva soltanto l'ipotesi prevista dal secondo comma dell'art. 2625 c.c.., ossia qualora la condotta abbia causato un danno ai soci.

[27] In vigore dal 16/4/2002.
[28] Articolo modificato dalla Legge n. 69/2015.
[29] Articolo modificato dalla Legge n. 69/2015.

Il reato di impedito controllo consiste nella condotta posta in essere dagli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alla società di revisione. È il caso, per esempio, quando al socio viene ostacolato/impedito l'esercizio del diritto di ispezionare i libri sociali (libro soci e libro adunanze assembleari), oppure quando la Banca omette il deposito presso la sede sociale del progetto di bilancio nei termini previsti dal codice.

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

Ai fini della salvaguardia della solidità patrimoniale della società, il reato di indebita restituzione dei conferimenti consiste nella condotta posta in essere dagli amministratori, che fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

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

La norma mira a salvaguardare la capacità finanziaria delle società.
Il reato consiste nella condotta posta in essere dagli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

La fattispecie, tuttavia, appare di difficile realizzazione, non essendo ravvisabile un interesse o un vantaggio per la Banca.

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

Il reato consiste nella condotta posta in essere dagli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali della società di appartenenza (c.d. "azioni proprie") o della società controllante, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La fattispecie in oggetto sembra di difficile realizzazione non essendo ravvisabile un interesse o un vantaggio per la banca.

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

La norma è diretta a tutelare i creditori delle società commerciali sia dal punto di vista della capacità finanziaria che dal punto di vista della permanenza del soggetto debitore. Il reato consiste nelle azioni di riduzioni del capitale sociale o fusioni e scissioni con altre società, cagionando danno ai creditori e/o alla medesima società.

Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)[30]

È il caso, per esempio, di delibera di operazioni da parte del Consiglio di Amministrazione con il voto favorevole dell'amministratore in conflitto di interesse, oppure l'esposizione di dati idonei a pregiudicare i diritti dei creditori sociali in occasione di operazioni straordinarie (riduzioni del capitale sociale, fusione, scissione).

La fattispecie di reato prevede che dalla violazione dell'obbligo di comunicazione derivino danni alla società o a terzi.

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

Il reato si configura allorquando gli amministratori ed i soci conferenti che formano od aumentano il capitale sociale in modo fittizio, ponendo in essere almeno una delle seguenti condotte:

- attribuzione di azioni o di quote sociali per somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- rilevante sopravvalutazione dei conferimenti di beni in natura o di crediti;
- in caso di trasformazione, rilevante sopravvalutazione del patrimonio della società.

La fattispecie sembra di difficile realizzazione non essendo ravvisabile un interesse o un vantaggio per la Banca.

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

La norma è diretta a salvaguardare la difesa della massa dei creditori nella fase della liquidazione (volontaria o coatta amministrativa) della società.

Il reato consiste nella condotta posta in essere dai liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori.

È il caso per esempio della ripartizione di beni sociali tra i soci prima del pagamento dei creditori, in concorso con liquidatori o altri, oppure la ripartizione tra i soci dell'avanzo di liquidazione che andrebbe devoluto ai fondi mutualistici

Corruzione tra privati (art. 2635 c.c.)[31]

La norma è diretta a tutelare la correttezza dei rapporti tra la società ed altri enti o società private) al fine di prevenire e reprimere gli accordi illeciti tra privati.

[30] Articolo aggiunto dalla Legge n. 262/2005.
[31] Articolo aggiunto dalla L. n. 190/2012; modificato dal D.Lgs. n. 38/2017.

Il reato punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, nonché coloro che svolgono funzioni direttive e le persone sottoposte alla direzione o alla vigilanza di uno dei suindicati soggetti, che - anche per interposta persona - sollecitano o ricevono, per se o per altri denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

Il comma 3 dell'art. 2635, rilevante ai sensi dell'art. 25-ter del d.lgs. 231/01, estende la punibilità al corruttore, o all'interposta persona, che dà o promette denaro o altra utilità a uno dei soggetti sopra menzionati.

Il reato potrebbe realizzarsi nell'ambito della gestione dei rapporti diretti con i fornitori ed in particolare nelle operazioni di acquisto: gli esponenti aziendali potrebbero, anche per interposta persona, infatti, dare o promettere denaro o altra utilità ad un soggetto apicale o ad un soggetto sottoposto alla sua direzione o vigilanza di un'azienda fornitrice per accordi illeciti con lo stesso finalizzati a transazioni economiche vantaggiose per la banca e svantaggiose per l'azienda fornitrice.

Istigazione alla corruzione tra privati (art. 2635-bis) [32]

Il reato sanziona la condotta di chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, anche per interposta persona, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

Ai fini della consumazione del reato, è sufficiente l'offerta o la promessa dell'utilità, oppure con la sollecitazione della promessa o dazione, mentre è irrilevante il verificarsi o meno del fine a cui è preordinata l'istigazione.

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

Il reato di illecita influenza sull'assemblea consiste nella condotta posta in essere da chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé od altri un ingiusto profitto. Il reato si consuma, ad esempio, attraverso:

- la presentazione di documenti o informazioni false, fuorvianti, o comunque decettive;
- la simulazione o la fraudolenta predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea, anche in concorso con altri;

[32] Articolo aggiunto dal D.Lgs. n. 38/2017.

- l'esecuzione di atti (simulati o fraudolenti) tali da far convergere la maggioranza assembleare verso tesi precostituite;
- la rappresentazione all'assemblea di improbabili prospettive di sviluppo nella loro attuabilità, allo scopo di ottenere dei voti per una rielezione o per la realizzazione di operazioni straordinarie;
- l'utilizzo improprio delle deleghe per costituire maggioranza assembleare;
- la gestione delle deleghe al di fuori di quanto previsto nello statuto o nei regolamenti assembleari (es. le deleghe sottoscritte e validate con indicazione in bianco del delegato);
- il caso in cui gli amministratori, temendo di non essere rieletti, fanno partecipare all'assemblea soggetti non soci che votano a loro favore;
- la maliziosa convocazione assemblea in date "scomode";
- le dichiarazioni mendaci e reticenti degli amministratori finalizzate ad influenzare il voto dell'assemblea.

Aggiotaggio (art. 2637 c.c.)

Il reato consiste nella condotta posta in essere da chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi societari.

La norma mira ad evitare pratiche scorrette volte alterare il valore di strumenti finanziari non quotati o comunque non negoziabili in mercati regolamentati.

Il reato in esame si realizza nel caso di:

- divulgazione, ossia comunicazione ad un numero indeterminato di persone, di fatti materiali non rispondenti al vero;
- compimento di operazioni simulate, includendo in tale nozione sia le operazioni che le parti non abbiano inteso in alcun modo realizzare, sia quelle che presentino un'apparenza difforme rispetto a quelle effettivamente volute.

È il caso, per esempio, di diffusione di notizie false da parte dei soggetti "apicali" o "sottoposti":

i. sul titolo di una piccola società non quotata partecipata dalla Banca, che abbia per effetto un incremento nell'acquisto da parte della clientela dei titoli emessi dalla società stessa con conseguente incremento del valore della partecipazione;

ii. sul titolo di una piccola società non quotata dislocata nell'area di operatività della Banca che abbiano per effetto l'alterazione nel comportamento dell'investitore con conseguente incremento dell'operatività in raccolta ordini o negoziazione in conto proprio;

iii. finalizzate a menomare la fiducia del pubblico circa la stabilità patrimoniale di altre banche presenti nella zona di competenza della BCC.

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

Il reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza punisce amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari e liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di Vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, espongono fatti materiali non rispondenti al vero - ancorché oggetto di valutazioni - sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero occultano con altri mezzi fraudolenti fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, al fine di ostacolare l'esercizio delle funzioni di vigilanza.

La norma punisce, inoltre, qualsiasi forma di ostacolo consapevole alle funzioni delle medesime Autorità pubbliche di Vigilanza, anche realizzato attraverso l'omissione delle comunicazioni a queste dovute.

L'ostacolo si realizza in due ipotesi:

a) nel caso in cui taluni dei suindicati soggetti, al fine di ostacolare l'attività delle autorità pubbliche di vigilanza:
   - espongano, in occasione di comunicazioni alle autorità pubbliche di vigilanza, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero
   - occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che erano tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi;
b) nel caso in cui la condotta, anche omissiva, degli stessi soggetti, indipendentemente dal fine perseguito, ostacoli effettivamente l'attività dell'autorità di pubblica vigilanza.

Si fa osservare che la norma non specifica quali siano le "*autorità pubbliche di vigilanza*" destinatarie della tutela penale e potendosi individuare opposti orientamenti: i) l'uno ne limita

l'applicabilità alle sole "*authorities*" di settore in senso stretto, quali Consob, Banca d'Italia, Isvap, UIF, ecc, ii) l'altro, del quale si trova traccia nelle linee guida di talune associazioni di categoria, estende la nozione in commento a qualunque soggetto pubblico che detenga poteri di natura ispettiva o di controllo. Al riguardo, la scelta della Banca orienta i propri presidi sul tema indipendentemente dall'autorità ed in ossequio alla tutela della norma verso qualsiasi destinatario, rientrando peraltro nel logico percorso di legalità che la banca profonde nell'attività istituzionale.

Tanto premesso, in banca il reato potrebbe essere commesso in occasione di comunicazioni sugli adempimenti previsti da norma di legge (ad esempio: segnalazioni di vigilanza, legge sull'usura, disposizioni in tema di trasparenza, vigilanza cooperativa, etc) o regolamenti o in occasione di ispezioni o verifiche delle Autorità di Vigilanza (Consob, Banca d'Italia, Ministero delle Attività Produttive), attraverso:

a) L'esposizione di fatti materiali non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria della BCC;

b) L'occultamento con mezzi fraudolenti, in tutto o in parte, fatti che si sarebbero dovuti comunicare;

c) L'ostacolo consapevole nei confronti delle funzioni delle Autorità pubbliche di vigilanza, anche omettendo le comunicazioni dovute alla predetta Autorità;

d) L'alterazione o contraffazione della documentazione e dei dati:

   i. comunicati a Monte Titoli in occasione degli adempimenti previsti da norma di legge o regolamenti (sistema di gestione accentrata);

   ii. relativi agli adempimenti previsti dalla normativa in materia di igiene e sicurezza sul lavoro, nonché dalla normativa previdenziale (ad esempio le comunicazioni relative agli obblighi assuntivi della BCC nei confronti delle categorie protette, comunicazioni per i fondi pensione);

   iii. trasmessi al Garante della Privacy al fine di indurre in errore circa il rispetto degli adempimenti previsti dalla normativa in materia di privacy;

   iv. comunicati alle Autorità Fiscali/Amministrative (Ministero delle Finanze ed altri Enti con capacità impositiva, Registro delle Imprese) in occasione degli adempimenti previsti da norma di legge o in occasione di ispezioni o verifiche (ad esempio nel caso in cui la BCC richieda un rimborso IVA sulla base di documentazione contraffatta);

   v. Segnalazioni alla UIF

e) L'alterazione, la contraffazione o l'omissione della segnalazione dei rapporti e/o risposte a quesiti inerenti alle indagini finanziarie.

Descrizione dei rischi in relazione ai reati societari di cui all'articolo 25-ter

Per riepilogare, le aree di attività ritenute esposte a rischio rappresentative, pertanto, di situazioni che necessitano particolare attenzione, sono le seguenti:

1) Redazione del bilancio, della relazione sulla gestione e di altre comunicazioni sociali.
2) Operazioni societarie che possono incidere sulla integrità del capitale sociale e del patrimonio.
3) Attività soggette a vigilanza di autorità pubbliche in base alla disciplina di settore.
4) Gestione dei rapporti con i soci e la Società di revisione;
5) Gestione delle attività di comunicazione (presentazioni societarie, organizzazione e gestione eventi pubblici, etc.);
6) Gestione dei rapporti con la clientela;
7) La trasmissione di dati in via informatica a soggetti pubblici, ad esempio all'Agenzia delle Entrate o agli Enti previdenziali o assicurativi, o comunque la elaborazione e la trasmissione di documenti aventi efficacia probatoria;
8) Selezione ed assunzione di personale dipendente;
9) Gestione dei rapporti con i fornitori;
10) Gestione delle sponsorizzazioni;
11) Gestione delle risorse finanziarie, i cui principi sono individuati nel regolamento dei poteri aziendali;
12) La modifica dolosa dei dati contabili presenti sul sistema informatico, al fine di:
    a. creare una falsa rappresentazione della situazione patrimoniale, economica e finanziaria mediante l'inserimento di voci di bilancio inesistenti o di valori difformi da quelli reali;
    b. generare riserve occulte o fondi "neri".
13) La disapplicazione dei criteri dettati dalla legge e dei principi contabili riguardanti la sopravvalutazione o sottovalutazione delle poste di bilancio.
14) La gestione dei rapporti con il Collegio Sindacale e con la società incaricata alla revisione legale, al fine di impedire od ostacolare il controllo da parte del Collegio stesso.
15) La gestione degli adempimenti con la Monte Titoli SpA.
16) La gestione degli adempimenti normativi in materia del lavoro e in materia di Privacy.
17) La predisposizione dei prospetti per la sollecitazione all'investimento.

18) Le operazioni in pregiudizio dei creditori con riferimento alla riduzione del capitale, fusione e scissione.
19) La predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea.
20) La gestione dei rapporti con le Autorità di Vigilanza, con particolare riguardo all'esposizione di fatti sulla situazione economica, patrimoniale e finanziaria.
21) La gestione dell'informativa verso l'esterno per quanto attiene a tutte le attività riguardanti il rispetto delle normative.

Principali presidi organizzativi e gestionali

Regole di carattere generale

Gli organi sociali della banca ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate. In coerenza con le procedure aziendali, i medesimi hanno l'obbligo di:

- attuare correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, onde fornire una informazione veritiera e completa sulla situazione economica, patrimoniale e finanziaria della Società; in particolare è fatto divieto di:
  - rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, fuorvianti o, comunque, non rispondenti alla realtà;
  - omettere dati o informazioni imposti dalla legge e dai regolamenti sulla situazione economica, patrimoniale e finanziaria;
  - rispettare le disposizioni di legge, i principi contabili e le regole aziendali, ponendo la massima attenzione, professionalità ed accuratezza, nella acquisizione, elaborazione, valutazione ed illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali;
  - assicurare il regolare funzionamento degli organi sociali, agevolando e collaborando con il Collegio Sindacale. In particolare, è fatto divieto di:
    - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o comunque che

ostacolino lo svolgimento dell'attività di controllo e di revisione da parte dei soci o delle funzioni di controllo;

- determinare o influenzare l'assunzione delle deliberazioni dell'Assemblea, attraverso atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- osservare scrupolosamente le norme a tutela dei creditori e della integrità ed effettività del capitale sociale;
- assicurare la tempestiva formalizzazione delle attività assembleari e degli altri organi societari; la regolare formazione, tenuta e conservazione di tutta la rilevante documentazione societaria, contabile e fiscale. Pertanto, è fatto divieto di tenere comportamenti che, mediante il mancato tempestivo aggiornamento della documentazione, la mancata corretta conservazione o l'occultamento dei documenti impediscano, alle autorità ed agli organi di vigilanza di effettuare le dovute attività di controllo.

Va infine fatto osservare, con particolare riferimento al reato di corruzione tra privati, che le regole organizzative funzionali alla minimizzazione di tali rischi possono essere mutuate da quelle già ampiamente sviluppate in materia di prevenzione di fatti di corruzione pubblica, ritenute funzionali a garantire:

- la trasparenza della gestione economica e finanziaria;
- la segmentazione ed autonomia delle funzioni aziendali deputate alla sponsorizzazione e promozione commerciale, alla regolazione contrattuale, al pagamento e alla fatturazione delle spese;
- la tracciabilità dei processi decisionali e di gestione e la conseguente definizione dei soggetti responsabili di ciascuna procedura.

Protocolli Specifici

La banca – in quanto aderente al GBCI - si è dotata di una serie di strumenti, procedure e protocolli operativi di carattere generale in materia di gestione delle attività amministrative e finanziarie.

Oltre ai presidi che disciplinano gli aspetti etico-comportamentali, nonché i presidi previsti dalle leggi e normative di riferimento, vengono individuati i seguenti specifici presidi, in relazione alle tipologie di reati, attraverso singoli regolamenti di processo e protocolli volti a verificarne nel continuo l'osservanza:

1) revisione del Bilancio da parte di primaria società di Revisione, alla quale è affidato il controllo contabile sulla Società ai sensi dell'art. 2409-bis del Codice civile;

2) riunioni periodiche dell'Organismo di Vigilanza/Collegio Sindacale e la Società di Revisione. Tali riunioni si tengono quantomeno una volta all'anno in prossimità della riunione del CdA prevista per l'approvazione del Bilancio.

3) L'applicazione e la gestione degli adempimenti previsti dalle Istruzioni di Vigilanza della Banca d'Italia e dalle Delibere della Consob, in materia di bilancio, nonché da quelli previsti dalle autorità fiscali e amministrative.

4) L'attuazione degli adempimenti previsti nel Regolamento Assembleare, nonché delle indicazioni della categoria delle Banche di Credito Cooperativo e della neocostituita Capogruppo in materia di assemblee ordinarie e straordinarie, diramate di anno in anno.

5) Il confronto giornaliero, a cura della funzione Back Office, circa la corrispondenza dei dati riportati nel sistema informatico da ICCREA Banca con quelli analoghi riportati dall'outsourcing BCC SI, riguardanti l'accentramento presso Monte Titoli SpA degli strumenti finanziari di propria emissione, significando che gli ulteriori adempimenti sono demandati a ICCREA Banca, a cui è stato conferito contrattualmente l'incarico di gestione.

6) L'attuazione degli adempimenti previsti nella regolamentazione di Vigilanza, con particolare riferimento all'informativa al pubblico, in cui sono chiaramente indicati ruoli e responsabilità delle funzioni aziendali nelle varie fasi del processo. Nelle suindicate disposizioni è previsto l'obbligo di pubblicazione di informazioni riguardanti l'adeguatezza patrimoniale, l'esposizione ai rischi e le caratteristiche generali dei sistemi preposti all'identificazione, alla misurazione e alla gestione dei rischi di I e II Pilastro cui è esposta la banca. L'informativa al pubblico fornisce, con l'obiettivo di rafforzare la disciplina di mercato, una rappresentazione dei rischi assunti, delle caratteristiche dei relativi sistemi di gestione e controllo e dell'adeguatezza patrimoniale della banca.

7) L'adozione di regole, con previsione di competenze e responsabilità, per la predisposizione di tutte le comunicazioni/adempimenti previsti dalla normativa in materia di:

   a. igiene e sicurezza sul lavoro, nonché dalla normativa previdenziale da effettuare alle autorità competenti;

   b. privacy e/o in occasione di ispezioni o verifiche del Garante Privacy e dall'AGCM.

8) Presidi finalizzati al rafforzamento del sistema di controllo e governo contabile, ai sensi della Legge 28 dicembre 2005 n. 262 sulla "*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*", per il raggiungimento degli obiettivi di assurance sui processi contabili della Banca, tra cui:

a. l'individuazione dei responsabili della struttura esecutiva tecnica, per la redazione dei documenti contabili societari, nelle figure del Direttore Generale e del Capo Contabile (Responsabile dell'Amministrazione), i quali peraltro, unitamente al Presidente del CdA, al Presidente del Collegio Sindacale e alla società incaricata alla revisione legale, risultano direttamente responsabili delle segnalazioni di vigilanza alla Banca d'Italia;

b. la redazione di apposite procedure, che prevedono compiti e responsabilità della struttura organizzativa, con relativa separazione funzionale, nonché la formalizzazione dei controlli contabili.

9) La previsione di riunioni tra la Funzione Audit, esternalizzata alla Capogruppo Iccrea Banca, il Collegio Sindacale, la società di revisione e l'OdV.

10) L'attività di vigilanza sull'adeguatezza amministrativa e contabile, nonché l'attività di controllo contabile sul bilancio, svolta ai sensi dell'art. 2409 ter del codice civile da parte del Collegio Sindacale[33].

11) Le "*lettere di attestazione*" predisposte, da parte dei responsabili di funzione, in sede di redazione di bilancio d'esercizio e della relazione semestrale.

12) la possibilità, da parte dell'OdV di richiedere, ai responsabili delle funzioni coinvolte nei processi di formazione del bilancio, specifiche conferme in ordine all'osservanza dei principi generali di comportamento.

Inoltre, la Banca ha implementato le attuali disposizioni interne nello specifico regolamento per la gestione delle spese e delle infrastrutture.

Infine, a presidio del rischio di cui al reato di cui all'articolo 2632 c.c., la società di revisione e il Collegio Sindacale verificano, sulla base di autonoma discrezionalità e nell'ambito delle rispettive competenze, che il capitale sia stato interamente versato e che non vi sia esclusivamente una operazione contabile fittizia nell'attivo.

Flussi informativi a favore dell'OdV

Sul punto si ritiene che l'OdV nella sua composizione di Collegio Sindacale dispone di sufficienti elementi informativi periodici

[33] Come previsto dall'articolo 43 dello Statuto e ai sensi dell'art. 52, comma 2 bis, del D. Lgs. 32/2007, il controllo contabile è demandato al Collegio Sindacale.

Articolo 25-quater - Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali

La commissione di simili delitti nell'interesse della Banca o comunque a suo vantaggio appare difficilmente ravvisabile.

Tuttavia, nella fattispecie, potrebbe essere possibile che vengano instaurati rapporti con clienti che perseguano, direttamente o quali prestanome, finalità di terrorismo, sovversione o eversione dell'ordine costituzionale, agevolandoli (inconsapevolmente) nella realizzazione dei loro criminosi obiettivi. Tali norme tendono, infatti, a punire non solo fattispecie di costituzione di associazioni terroristiche e/o sovversive, ma anche qualsiasi ipotesi di fiancheggiamento o sostegno alle stesse attraverso la messa a disposizione di risorse finanziarie – sia mediante erogazioni liberali sia nell'ambito dello svolgimento dell'attività societaria tipica – nonché di mezzi di trasporto, rifugi o sedi logistiche.

Per quanto precede, tenuto conto della numerosità dei rapporti che la Banca intrattiene quotidianamente con la propria clientela retail e business, e, soprattutto delle prescrizioni normative che individuano, nel conseguimento di un interesse o vantaggio anche indiretto per l'ente, una possibile fonte d'imputabilità, sono state individuate le seguenti potenziali aree di attività a rischio:

1) Servizi finanziari erogati alla clientela, in particolare servizi bancari a vario titolo che la Banca potrebbe fornire inconsapevolmente a soggetti o organizzazioni terroristiche, nonché coinvolti in attività illecite lesive della persona o della personalità individuale.
2) Altri servizi che la Banca potrebbe fornire a soggetti o organizzazioni correlate a frange terroristico/eversive.

Oltre ai presidi di carattere generale, la Banca ha provveduto ad identificare i seguenti presidi, in relazione allo specifico ambito di reati di terrorismo ed eversione dell'ordine democratico:

1) Controlli previsti, in relazione ai servizi finanziari della Banca, mediante la gestione dell'Anagrafe Negativa (banca dati che mette in relazione i nominativi dei soggetti collegati al finanziamento del terrorismo internazionale con i nominativi dei clienti della Banca) e le attività connesse alle evidenze ditale Anagrafe.
2) Politiche e procedure aziendali con particolare riguardo alle misure di sicurezza relative al controllo degli accessi alle aree aziendali.
3) L'espletamento di adeguate attività di verifica dei requisiti dei fornitori nell'ambito del processo acquisti di beni e servizi.

4) Tutti i presidi strutturati e declinati nell'ambito della regolamentazione a presidio del rischio di riciclaggio.

Articolo 25-quater.1 - Pratiche di mutilazione degli organi genitali femminili

L'articolo 8 della Legge del 9/01/06 n. 7 ha aggiunto l'art. 25 quater1 e riguarda il divieto delle pratiche di mutilazione genitali femminili di cui all'art. 583 bis c.p.[34].

Non si ritiene ravvisabile in Banca tal genere di ipotesi di reato.

[34] In vigore dal 2/2/2006.

Articolo 25-quinquies - Delitti contro la libertà e personalità individuale

Il novero dei delitti contro la personalità individuale è stato introdotto dall'art. 5 della Legge 11/08/2003 n. 228, che ha aggiunto nel Decreto l'art. 25-quinquies[35], modificato ulteriormente con l'art. 10 della Legge 6/2/2006 n. 38[36], con riferimento agli articoli contenuti nel Libro II capo III del Codice penale, specificamente:

1) Riduzione o mantenimento in schiavitù e servitù (art. 600 c.p.)
2) Prostituzione minorile (art. 600-bis c.p.)
3) Pornografia minorile (art. 600-ter c.p.)
4) Detenzione o accesso a materiale pornografico (art. 600-quater c.p.) [37]
5) Pornografia virtuale (art. 600-quater.1)
6) Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
7) Tratta di persone (art. 601 c.p.)
8) Acquisto o alienazione di schiavi (art. 602 c.p.)
9) Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)
10) Adescamento di minorenni (art. 609-undecies c.p.) [38]

La fattispecie in esame è diretta a reprimere le ipotesi di illecito arricchimento conseguito attraverso le attività connesse alla tratta di persone, al c.d. "turismo sessuale", ovvero a fatti di pedopornografia.

Da ultimo, la norma è stata riformata, in aderenza alla direttiva europea n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che, per quanto qui rileva, ha introdotto un nuovo comma all'articolo 600-quater dove si sanzione anche chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto.

Inoltre, attraverso la modifica dell'articolo 609-undecies sono state introdotti aumenti di pena nei seguenti casi:

---

[35] In vigore dal 7/9/2003.

[36] In vigore dal 2/3/2006.

[37] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

[38] Articolo e rubrica modificata dalla Legge n. 238/2021 "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*", in vigore dal 1° febbraio 2022.

1) se il reato è commesso da più persone riunite;
2) se il reato è commesso da persona che fa parte di un'associazione per delinquere e al fine di agevolarne l'attività;
3) se dal fatto, a causa della reiterazione delle condotte, deriva al minore un pregiudizio grave;
4) se dal fatto deriva pericolo di vita per il minore.

Tali norme puniscono, altresì, chiunque induca alla prostituzione una persona minorenne, sfrutti o adeschi minori per realizzare esibizioni pornografiche o produrre materiale pornografico e chiunque organizzi o propagandi iniziative turistiche volte allo sfruttamento della prostituzione minorile (c.d. turismo sessuale). Inoltre, è punito chiunque commercia, vende acquista ovvero procura o tratta organi o parte di essi, prelevati da persona vivente; è, altresì, punito anche chi ne organizza o pubblicizza i relativi viaggi ovvero diffonde, anche per via informatica, annunci tesi a tale scopo.

È il caso, per esempio, seppure di difficile realizzazione non essendo ravvisabile un interesse o un vantaggio per la BCC, della diretta o indiretta erogazione di finanziamenti con la consapevolezza della destinazione dei medesimi al fine di compiere reati contro la personalità individuale.

Parimenti si può ipotizzare il rischio della diretta o indiretta elargizione o raccolta di fondi a associazioni/enti, con la consapevolezza che vengono utilizzati per le condotte criminose in trattazione, nonché il (remoto) rischio di finanziamento a favore di agenzie di viaggi, clienti della Banca, nell'ipotesi di iniziative turistiche volte allo sfruttamento della prostituzione minorile, nonché rapporti con persone sottoposte a procedimenti penali specifici.

Da ultimo, sebbene in linea generale la Banca non si avvale di personale fornito attraverso il sistema del lavoro interinale, viene valutato il rischio che essa possa usufruire di servizi da parte di fornitori che utilizzano personale non correttamente inquadrato sulla base della normativa in vigore del comparto, al fine di contenere il costo del servizio (per esempio il caso del servizio di pulizie).

Valgono al riguardo i presidi riportati nella regolamentazione del credito, delle infrastrutture e spese, nonché nella regolamentazione a presidio del rischio di riciclaggio e finanziamento al terrorismo.

Si richiamano, altresì sul punto, le disposizioni contenute nel regolamento infrastrutture e spese, nonché i presidi previsti per l'affidamento di incarichi a terze parti.

Il responsabile dell'ufficio infrastrutture e spese ed economato assicurerà:

- che sia previsto contrattualmente la possibilità per la banca di effettuare verifiche sul personale impiegato dalla controparte e che questa garantisca che l'assunzione del personale, anche straniero, avvenga su base di regolari contratti di lavoro;
- i necessari e puntuali controlli nel corso della gestione del personale impiegato nelle attività gestite dalle terze parti, avendo cura di verificare, nel caso di dipendenti stranieri, la documentazione circa i permessi di soggiorno, nonché la relativa validità durante il prosieguo del rapporto di lavoro; verificherà, altresì, la sussistenza dei requisiti normativi di regolarità della controparte tramite l'acquisizione della documentazione prevista dalla legge (es: DURC).

Flussi informativi a favore dell'OdV

Il responsabile dell'ufficio infrastrutture e spese ed economato fornisce – fatte salve casistiche particolari - semestrali flussi informativi all'OdV sull'andamento delle attività in argomento e sul risultato dei periodici controlli.

Articolo 25-sexies - Delitti di abuso di informazioni privilegiate e di manipolazione del mercato

In relazione alla disciplina sul Market Abuse (Parte V Titolo I bis, Capo II del T.U.F.), è stato introdotto nel Decreto l'art. 25 sexies[39] per i reati di:

1) Abuso di informazioni privilegiate (insider trading) di cui all'art. 184 del TUF, ove l'asimmetria informativa portata, appunto, dalla conoscenza di informazioni privilegiate, permette di effettuare migliori scelte, rispetto ad altri investitori operanti sul medesimo mercato.
2) Manipolazione del mercato, di cui all'art. 185 del TUF, che si configura nei confronti di colui che diffonde informazioni false o ingannevoli o realizza operazioni simulate o altri artifizi, che concretamente risultano idonei a provocare l'alterazione del prezzo degli strumenti finanziari.

Inoltre, l'ipotesi di responsabilità amministrativa a carico degli enti per illeciti amministrativi, in materia di abusi di mercato è prevista anche dall'articolo 187-quinquies del TUF, che impone il pagamento di una somma pari all'importo della sanzione amministrativa irrogata ai sensi degli artt. 187 bis e 187 ter del TUF.

In sintesi, la norma punisce tre condotte criminose, riferibili coloro che abbiano accesso alle informazioni privilegiate in ragione della propria professione, della partecipazione al capitale dell'emittente, ovvero della partecipazione ad organi di amministrazione, direzione o controllo dello stesso (c.d. insider "primari").

I beni giuridici che la norma intende tutelare sono l'integrità dei mercati finanziari regolamentati e la protezione e l'accrescimento della fiducia degli investitori.

Sono punite le seguenti condotte:

1) acquistare, vendere o compiere altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando informazioni privilegiate (c.d. trading);
2) comunicare informazioni privilegiate ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio (c.d. tipping);
3) raccomandare o indurre altri, sulla base delle informazioni privilegiate, al compimento di taluna delle operazioni su strumenti finanziari (c.d. tuyautage).

[39] In vigore dal 12/5/2005.

Il reato in esame è punito qualora attenga a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato, mentre sono escluse dall'ambito di applicazione dell'art. 184 TUF le "*operazioni attinenti alla politica monetaria, alla politica valutaria o alla gestione del debito pubblico compiute dallo Stato italiano, da uno Stato membro dell'Unione europea, dal Sistema europeo delle Banche centrali, da una Società centrale di uno Stato membro dell'Unione europea, o da qualsiasi altro ente ufficialmente designato ovvero da un soggetto che agisca per conto degli stessi*", nonché le "*negoziazioni di azioni, obbligazioni e altri strumenti finanziari propri quotati, effettuate nell'ambito di programmi di riacquisto da parte dell'emittente o di società controllate o collegate, e operazioni di stabilizzazione di strumenti finanziari che rispettino le condizioni stabilite dalla CONSOB con regolamento*".

A seguito delle recenti modifiche legislative, è stato ampliato l'ambito soggettivo della fattispecie, rendendo punibile anche l'insider da reato, cioè la condotta di colui che, essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose, attui una delle condotte rilevanti.

Ai sensi dell'art. 181, TUF, per "*informazione privilegiata*" si intende un'informazione che ha carattere preciso, che non è stata resa pubblica e che concerne, direttamente o indirettamente uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti ovvero su sui prezzi di strumenti finanziari derivati connessi.

Descrizione dei rischi in relazione ai reati societari di cui all'articolo 25-sexies

In relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato (c.d. *"Market Abuse"),* nell'ambito della gestione finanziaria della Banca, sono state individuate le seguenti attività a rischio:

1) Impiego dei fondi provenienti dalla raccolta da parte della clientela privata, tenuto conto degli importi delle singole transazioni e del livello di liquidità del mercato dei titoli di Stato. Si tratta in particolare della teorica possibilità di alterare il prezzo degli strumenti finanziari oggetto di compravendita.
2) Impiego delle eccedenze di liquidità della Banca che possono essere investite in titoli obbligazionari, depositi fiduciari, depositi bancari e operazioni di pronti contro termine su titoli di Stato Euro governativi.
3) Operazioni in strumenti derivati a copertura dei rischi finanziari connessi ai flussi di cassa e alle attività e passività della Banca, con riferimento al potenziale reato di manipolazione del mercato mediante l'utilizzo improprio degli strumenti derivati impiegati per la copertura.

4) Prestazione dei servizi di investimento ed in particolare il servizio di:
   - collocamento di strumenti finanziari;
   - ricezione e trasmissione ordini al partner di riferimento.

Le suddette attività risultano potenzialmente esposte sia in relazione al reato di manipolazione del mercato - mediante la possibile diffusione di informazioni false o fuorvianti su un emittente o su un titolo - sia a quello di abuso di informazioni privilegiate, mediante il rilascio di informazioni privilegiate.

Relativamente al collocamento di strumenti finanziari si evidenzia, tuttavia, che il rischio di commissione dei reati di *Market Abuse* risulta contenuto, considerate le caratteristiche standard delle operazioni (condizioni di offerta e di prezzo esplicitate sulla documentazione di offerta; parità di accesso dei sottoscrittori alle informazioni riguardanti il titolo in emissione; assenza di un mercato secondario sul titolo, ecc.).

Per quanto concerne l'attività di ricezione e trasmissione ordini, il rischio potenziale risulta marginale, tenuto conto delle caratteristiche della clientela e degli esigui volumi operativi di acquisto e vendita di titoli.

Vengono individuati gli ulteriori seguenti rischi:

a) Acquisito/vendita o compimento di altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando informazioni privilegiate detenute in ragione della propria qualità di membro di organi di amministrazione, direzione o controllo della società, della partecipazione al capitale della medesima, dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio, ovvero a motivo della preparazione o esecuzione di attività delittuose;

b) comunicazione di tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;

c) raccomandazione o induzione di altri, sulla base di tali informazioni al compimento di taluna delle operazioni indicate nella lettera a).

Tali casistiche sono rappresentative delle seguenti ipotesi:

a) comunicazione al di fuori dell'orario di lavoro da parte dei soggetti "apicali" o "sottoposti" dell'informazione privilegiata a terzi che abbia per effetto l'incremento dell'operatività dei servizi di investimento della BCC;

b) raccomandazione a terzi, da parte dei soggetti "apicali" o "sottoposti" in possesso di informazione privilegiata, che abbia ad effetto l'incremento dell'operatività dei servizi di investimento della BCC;

c) il personale della banca potrebbe venire a conoscenza di informazioni privilegiate anche attraverso un cliente che sia insider di una società e che compia operazioni rilevanti sui titoli della medesima.

d) diffusione di notizie false da parte dei soggetti "apicali" o "sottoposti" sul titolo di una piccola società quotata sedente nell'area di operatività della BCC che abbiano per effetto l'alterazione delle quotazioni del titolo che comportano l'incremento del valore dei titoli stessi presenti nel portafoglio di proprietà della BCC (185 e 187 ter TUF);

e) diffusione di notizie false da parte dei soggetti "apicali" o "sottoposti" sul titolo a ridotto flottante di una piccola società quotata partecipata dalla banca nel rispetto dei limiti di Vigilanza che abbiano per effetto un incremento nell'acquisto da parte della clientela dei titoli emessi dalla società stessa con conseguente incremento del valore della partecipazione.

Infine, si ritiene che anche lo sviluppo di nuovi strumenti finanziari possa rappresentare un'ulteriore area a rischio, considerato che la diffusione di informazioni concernenti uno o più emittenti potrebbe influire sulla formazione dei prezzi degli stessi.

Con riferimento alle principali aree di rischio connesse con i reati di market abuse, si individuano di seguito i principali processi sensibili che presentano connotazioni specifiche e peculiari.

Instaurazione, sviluppo delle relazioni commerciali con soggetti pubblici e privati

Tale processo presenta particolare profilo di rischio durante lo svolgimento, ad esempio, delle seguenti attività: (i) sviluppo dei rapporti commerciali, (ii) erogazioni di prodotti del credito, (iii) operazioni di project financing, (iv) investimenti su strumenti finanziari quotati per conto della clientela e attività di corporate finance, (v) attività di consulenza in materia di investimenti.

I reati in esame potrebbero sussistere qualora indipendente, nell'ambito dell'esecuzione di mandati di consulenza per operazioni di finanza straordinaria e/o nell'ambito delle attività di sviluppo delle relazioni commerciali, acquisisca informazioni confidenziali e riservate e raccomandi o induca terzi, sulla base delle medesime informazioni, al compimento di operazioni di compravendita di strumenti finanziari nell'interesse della banca.

Pianificazione strategica finanziaria, gestione dei relativi investimenti

Tale processo si riferisce al processo di predisposizione del piano strategico pluriennale e al processo di pianificazione finanziaria e le attività connesse di realizzazione dei relativi

investimenti. I reati in esame potrebbero sussistere qualora un dipendente comunichi informazioni di carattere privilegiato attinenti al piano strategico ad altri soggetti, ovvero diffonde all'esterno informazioni non veritiere attinenti a dati relativi al piano finanziario.

- **gestione del portafoglio di proprietà**

Il processo è caratterizzato dallo svolgimento della gestione del portafoglio bancario e del portafoglio di negoziazione di vigilanza, con riferimento all'impiego della liquidità della banca.

Si sostanzia nelle seguenti macro-attività:

- gestione del portafoglio dei titoli di Stato
- gestione del rischio tasso di interesse/rischio cambio/rischio paese tramite l'utilizzo di derivati;
- strutturazione di operazioni di investimento verso terze parti;
- operazioni di cartolarizzazioni;
- attività di trading sui titoli di Stato o titoli garantiti dallo Stato, compresa la negoziazione dei relativi derivati di copertura.

I reati in esame potrebbero sussistere qualora un dipendente, nell'interesse a vantaggio della banca, nell'ambito della gestione del portafoglio di competenza eseguisse operazioni di investimento della liquidità della Banca sfruttando abusivamente un'informazione privilegiata (ad esempio raccolta nell'ambito dello svolgimento di altre attività da parte delle strutture di business).

- **gestione delle operazioni sul capitale/straordinarie e adempimenti societari.**

Il processo è caratterizzato dallo svolgimento delle seguenti attività:

- pianificazione, gestione e deliberazione delle operazioni sul capitale sociale;
- operazioni aventi ad oggetto l'acquisto e/o la dismissione e/o la permuta di quote di partecipazione in società terze;
- operazioni straordinarie societarie (es: operazioni di fusione, conferimenti, trasformazioni, liquidazioni, cessioni/acquisizioni di rami di azienda chiusa);
- Convocazione e verbalizzazione delle riunioni assembleari del consiglio di amministrazione.

I reati in esame potrebbero sussistere qualora un dirigente/funzionario/dipendente della banca, nell'ambito dell'attività di qui sopra, acquisiscano informazioni di carattere privilegiato e:

- comunichi tali informazioni ad altri soggetti al di fuori del normale esercizio del lavoro, affinché questi compiano operazioni nell'interesse e/o a vantaggio della banca;

- raccomandi o induca altri soggetti, sulla base delle informazioni acquisite, al compimento di operazioni di acquisto e/o vendita di strumenti finanziari quotati, nell'interesse euro e/o a vantaggio della banca.

Principali presidi organizzativi e gestionali

Oltre ai presidi etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, la Banca ha adottato, con delibere del Consiglio di Amministrazione, procedure idonee per individuare le eventuali operazioni sospette, per il tramite della soluzione tecnologica SIMAD che, basandosi sull'inoltro dei flussi di dati prodotto da BCC SI SpA a ICCREA BANCA SpA, viene alimentata da una base dati di vigilanza, con soglie parametriche per l'attivazione di procedure di WARNING.

Sono stati, altresì, previsti i seguenti specifici presidi organizzativi e gestionali in relazione ai potenziali reati di Market Abuse:

1) Comitato di Direzione/Rischi, con ruolo consultivo e di supervisione della realizzazione delle strategie finanziarie e del rispetto delle linee guida operative.

2) Mandato a ICCREA BANCA S.p.A. per il monitoraggio, l'identificazione e la segnalazione delle operazioni sospette, con verifiche connesse alle specifiche previsioni della Consob, relativamente alle operazioni inoltrate e/o eseguite dalla Banca o dalla propria clientela sui mercati regolamentati. In particolare, rinviando ai dettagli riportati nel relativo contratto, ferma restando la responsabilità in capo alla Banca circa le valutazioni di merito, ICCREA BANCA SpA, a seguito di specifica analisi, provvede a comunicare a questa Banca:

   - l'assenza di operazioni sospette ovvero abusi di mercato e la conseguente archiviazione;
   - la necessità di ulteriori approfondimenti al fine di rilevare la sussistenza o insussistenza di operazioni sospette o abusi di mercato;
   - la necessità di effettuare la segnalazione alla Consob.

   La gestione delle suddette attività, in ragione delle rispettive competenze, è demandata in capo al Responsabile della Funzione di conformità e al Responsabile dell'Area Finanza, quest'ultimo è anche responsabile dell'archiviazione di tutte le segnalazioni inviate da ICCREA, a prescindere dall'esistenza o meno di operazioni potenzialmente sospette.

3) Stipula di "contratti di servizio" con le controparti bancarie, ovvero con ICCREA BANCA SpA, con BANCA INTERMOBILIARE SpA e DIRECTA SIM per le attività direttamente ad esse demandate per l'operatività in titoli e trading on-line, delle quali risultano singolarmente responsabili nei limiti delle rispettive competenze.

4) Procedure aziendali e disposizioni interne, protese alla:

- individuazione dei soggetti incaricati di gestire l'attività di comunicazione esterna;
- gestione delle informazioni rilevanti in quanto "*price-sensitive*";
- definizione di un programma di informazione/formazione periodica degli Amministratori e della Direzione in materia di informazioni price-sensitive.

Si richiama, inoltre, quanto prescritto dal Testo Unico della Finanza e dai relativi regolamenti di attuazione, anche in recepimento della Direttiva MiFID (Markets in Financial Instruments Directive) con specifico riferimento:

- all'individuazione dei soggetti in possesso di informazioni privilegiate e di quelli ad essi collegati (c.d. soggetti rilevanti) e istituzione del relativo registro;
- al monitoraggio e rilevazione delle operazioni personali eseguite dai suddetti soggetti rilevanti;
- al sistema di rilevazione (delegato a ICCREA BANCA Spa) e segnalazione di operazioni sospette in materia di Market Abuse.

Detti presidi sono riferibili anche ai rischi reato in materia di *Market Abuse* connessi alla prestazione dei servizi di investimento e sviluppo nuovi prodotti. A tali presidi si aggiungono: la procedura aziendale in materia di gestione del Profilo della Clientela, i limiti operativi previsti dalla procedura aziendale riguardante l'operatività in titoli, nonché i programmi di formazione/informazione erogati sull'argomento.

Articolo 25-septies - Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Come riportato nella sezione generale del presente documento, l'articolo 30 del D. Lgs. 9 aprile 2008 n. 81 (Testo unico sulla salute e sicurezza sul lavoro) prevede che il modello di organizzazione e di gestione idoneo ad avere efficacia esimente deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici in esso indicati e che qui devono intendersi integralmente richiamati.

In sostanza il provvedimento, integrando le norme a presidio della salute e sicurezza dei lavoratori nei luoghi di lavoro ha introdotto la punibilità dell'ente anche per i reati di natura "colposa".

Le norme in tema di prevenzione degli infortuni sul lavoro hanno la funzione primaria di evitare che si verifichino eventi lesivi dell'incolumità fisica connaturati all'esercizio dell'attività lavorativa. Il bene giuridico da tutelare è, quindi, l'integrità della persona.

Rileva nel caso di specie anche l'ipotesi in cui tali rischi siano conseguenti ad un'eventuale imprudenza e disattenzione del lavoratore. Ne consegue che il datore di lavoro è sempre responsabile dell'infortunio occorso al lavoratore, sia quando ometta di approntare le idonee misure protettive, sia quando non accerti e vigili, con prudente e continua diligenza, che il dipendente faccia effettivamente uso delle medesime. Pertanto, il compito del datore di lavoro spazia dall'istruzione dei lavoratori sui rischi di determinate attività alla predisposizione in concreto di misure mdi sicurezza e alla continua vigilanza circa il rispetto delle medesime.

Assume, dunque, rilevanza qualunque condotta (commissiva o omissiva) idonea a cagionare:

i. la morte di una persona;

ii. lesioni gravi o gravissime ad una persona.

A tal fine, si riporta che ai sensi dell'art. 583 C.P. sono lesioni "gravi":

- quelle da cui derivi una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a 40 giorni;
- quelle a cui consegua l'indebolimento permanente di un senso o di un organo.

Ai sensi della medesima disposizione. sono lesioni personali "gravissime", quelle da cui derivi:

- una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- 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 nell'uso della parola;
- la deformazione ovvero lo sfregio permanente del viso.

Descrizione dei rischi in relazione ai reati per violazione delle norme sulla tutela della salute e sicurezza sul lavoro di cui all'articolo 25-septies

Riguardo ai reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione delle norme di tutela della salute e sicurezza sul lavoro, non è possibile escludere in modo aprioristico alcun ambito di attività, dal momento che tale casistica di reati può di fatto investire la totalità delle componenti aziendali.

Per quanto si ritiene proponibile nella presente sezione, costituiscono attività a rischio:

1) La carenza o mancanza dei requisiti di sicurezza e/o di efficienza degli impianti.
2) La inadeguatezza del posto di lavoro e le attività relative alla manutenzione e gestione dei luoghi di lavoro.

3) La carente salubrità dell'ambiente di lavoro.

4) La mancata attività di prevenzione degli incendi.

5) La mancata o carente valutazione del rischio di stress da lavoro correlato nel Documento di valutazione dei rischi, il cui onere ricade sul datore di lavoro, sui dirigenti ed eventuali preposti.

6) L'omessa o non corretta adozione di misure previste dal D. Lgs. 81/08 quali:

   - formalizzazione dei documenti relativi alla valutazione dei rischi;
   - nomina scritta dei soggetti previsti dalla normativa;
   - formazione e informazione dei lavoratori;
   - definizione del piano di emergenza e di esodo ed individuazione delle squadre di emergenza;
   - installazione presidi antincendio;
   - omologazione CE delle macchine e delle attrezzature di lavoro,

   tali da determinare la responsabilità della banca in caso di decesso o lesioni gravi di un lavoratore.

Costituisce ulteriore rischio l'inosservanza delle norme e disposizioni sulla sicurezza e prevenzione dei crimini, quali ad esempio le rapine.

Principali presidi organizzativi e gestionali

Oltre ai presidi di carattere generale, che disciplinano gli aspetti etico - comportamentali che devono essere osservati, la Banca, attraverso il documento di valutazione dei rischi, di cui al D.Lgs. del 19 settembre 1994, n. 626 e successive modifiche di cui al D. Lgs. 9 aprile 2008 n. 81 ha individuato:

a) i responsabili del servizio di prevenzione e protezione;

b) i presidi organizzativi e gestionali in tema di salute e sicurezza sul lavoro, disciplinati e descritti all'interno della procedura denominata "*Sistema di gestione della salute e sicurezza sui luoghi di lavoro (SGSL)*", segnatamente:

   - l'organizzazione di un sistema strutturato di monitoraggio dei principali indicatori delle prestazioni di sicurezza, di verifica e di controllo dei processi in relazione agli indirizzi aziendali definiti;
   - la verifica e la valutazione periodica dello stato dei luoghi e dei relativi interventi migliorativi da sottoporre alla valutazione del CdA, al fine di provvedere alla revisione organica dei luoghi e dell'impatto che le relative soluzioni possono avere sulle strategie e le politiche aziendali.

A tal fine, la banca ha:

- affidato l'incarico di RSPP a professionista esterno, in possesso delle previste qualifiche e competenze;
- nominato il referente sulla sicurezza d.lgs.81/08, come da organigramma aziendale tempo per tempo in vigore;
- nominato gli addetti al servizio antincendio e primo soccorso presso ogni dipendenza.

Valgono, altresì, a presidio:

- il documento di valutazione dei rischi;
- il piano di emergenza, ove previsto.
- la rilevazione delle presenze nella fase di formazione e di esercitazione dei dipendenti
- gli attestati rilasciati per addetti antincendio e primo soccorso
- la nomina degli addetti alle emergenze
- i verbali delle riunioni periodiche
- i controlli da parte:
  i. della funzione Compliance sul rischio di stress da lavoro correlato;
  ii. del Referente interno Sicurezza;
  iii. dell'RSPP incaricato;
  iv. del medico competente.

Con riferimento alla sicurezza e prevenzione dei crimini, si rinvia alle disposizioni indicate nel "*regolamento d'Istituto*", segnatamente individuabili al capitolo "*Norme relative alle misure di sicurezza*". In tale sezione viene preso in considerazione, tra gli altri, il rischio rapine attraverso la declinazione di specifiche procedure che ciascun dipendente deve seguire ai fini della relativa prevenzione.

Protocolli specifici

Rileva, innanzitutto, il documento di valutazione dei rischi che deve contenere:

- la valutazione di tutti i rischi per la salute e la sicurezza dei lavoratori esistenti nel contesto aziendale;
- le misure di prevenzione e di protezione adottate alla luce di tale valutazione;
- il programma delle misure idonee a migliorare i livelli di sicurezza nel tempo e individuare le procedure per l'attuazione delle misure e, tra l'altro, i ruoli dell'organizzazione aziendale che devono attuarle;

- l'indicazione dei soggetti che hanno collaborato alla valutazione dei rischi (responsabile del servizio di prevenzione e protezione, rappresentante dei lavoratori per la sicurezza, medico competente);
- l'individuazione dei rischi specifici di determinate mansioni, che esigono un'adeguata formazione e specifiche capacità professionali.

Inoltre, il documento di valutazione dei rischi va immediatamente rielaborato quando:

- al processo produttivo o all'organizzazione del lavoro vengono apportate modifiche incidenti sulla sicurezza o la salute dei lavoratori;
- vengono introdotte innovazioni, soprattutto nel campo della tecnica;
- si verificano infortuni significativi;
- i risultati della sorveglianza sanitaria ne evidenziano la necessità.

Fermo quanto previsto dalle norme di riferimento, con riferimento alla sicurezza sui luoghi di lavoro, nel cui ambito sono compresi anche gli adempimenti relativi ai presidi di sicurezza relativi alla situazione sanitaria Covid-19, i preposti formalmente nominati ai sensi dell'articolo 18 del D.Lgs. 81/2008 devono:

- sovrintendere e vigilare sull'osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e
- intervenire per modificare il comportamento non conforme, fornendo le necessarie indicazioni di sicurezza, in caso di rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite, ai fini della protezione collettiva e individuale;
- interrompere l'attività del lavoratore e informare i superiori diretti, in caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza;
- interrompere temporaneamente, se necessario, l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza;
- verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;

- richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
- frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37 del D.Lgs. 81/2008.

Nel medesimo ambito, a fronte di contratti d'appalto e/o di subappalto di servizi o d'opera a terzi, fermo restando la disposizione che il datore di lavoro, ivi compresi i subappaltatori:

- cooperano all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinano gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva,

il responsabile del Servizio Infrastrutture e spese, provvede, per conto del datore di lavoro committente, alla verifica formale e sostanziale degli adempimenti previsti dall'articolo 26 D.Lgs. 81/2008, nonché provvede ad acquisire, con le formalità del caso, il nominativo o i nominativi del personale che svolge le funzioni di preposto.

Per altro verso, il tutor per la formazione, avvalendosi dell'ufficio del personale, di concerto con il RSPP incaricato e con il responsabile del Servizio Infrastrutture e Spese, deve assicurare che ciascun lavoratore riceva una formazione sufficiente ed adeguata in materia di salute e sicurezza, con particolare riferimento a:

- concetti di rischio, danno, prevenzione, protezione, organizzazione della prevenzione aziendale, diritti e doveri dei vari soggetti aziendali, organi di vigilanza, controllo, assistenza;
- rischi riferiti alle mansioni e ai possibili danni e alle conseguenti misure e procedure di prevenzione e protezione caratteristici del settore o comparto di appartenenza dell'azienda.

Le suindicate figure assicurano, altresì, tutti gli adempimenti previsti dall'articolo 37 D.Lgs. 81/2008 in materia di formazione dei lavoratori e dei loro rappresentanti, avendo cura che:

- sia assicurato l'aggiornamento biennale per i preposti in presenza e comunque ogni qualvolta sia reso necessario in ragione dell'evoluzione dei rischi o all'insorgenza di nuovi rischi;

- sia assicurato l'addestramento attraverso prova pratica per l'uso corretto e in sicurezza di attrezzature, macchine, impianti, sostanze, dispositivi, anche di protezione individuale;
- gli interventi di addestramento effettuati siano tracciati in apposito registro anche informatizzato.

Inoltre:

a) Annualmente l'RSPP deve effettuare sopralluoghi presso tutti gli edifici della Banca e redigere un verbale che viene condiviso con il Responsabile del Settore Infrastrutture e Spese (in quanto funzione a staff della Direzione Generale), il Presidente del CdA, il rappresentante dei lavoratori e della sicurezza e il medico competente per concordare gli interventi da effettuare (ad es. formazione, adozione misure di sicurezza, ...). In tale contesto vengo valutate anche le eventuali esigenze di aggiornamenti e adeguamenti del documento di valutazione dei rischi.
b) Il Personale dipendente deve riceve periodicamente la formazione necessaria prevista dalla normativa, la cui documentazione deve essere custodita presso l'Ufficio del Personale.
c) L'RSPP deve:
    a. definire il piano di emergenza e di esodo.
    b. coordinare le esercitazioni periodiche, provvedendo anche ad assicurare la partecipazione di tutto il personale almeno una volta per ogni tipologia di esercitazione, documentandone e certificandone la presenza.

Per quanto rileva, si richiama in questa sezione l'apparato sanzionatorio di cui all'articolo 55 D.Lgs. 81/2008.

Attività di verifiche da parte dell'OdV

☞ **Procedure - Approvvigionamento e gestione degli appalti**

Verificare l'adozione di specifica procedura per la gestione degli appalti nel cui ambito vengono previsti e definiti i seguenti presidi:

a) budget, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza;

b) meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro;

c) meccanismi di controllo che garantiscano l'inclusione nei contratti di appalto, subappalto e somministrazione, dei costi relativi alla sicurezza del lavoro;

d) lo scambio informativo dei rischi con le Ditte Esterne incaricate di prestazioni di servizio, e presidiare l'andamento dei lavori relativamente ai rischi d'interferenza;

e) nel caso di acquisti di servizi, anche di natura intellettuale, la Banca subordina l'attività di affidamento alla verifica preliminare delle competenze dei propri fornitori anche sulla base della sussistenza di esperienze pregresse ed eventuali requisiti cogenti (ad es. iscrizione ad albi professionali;

f) le modalità di verifica del possesso di idonei requisiti tecnico-professionali del soggetto esecutore delle lavorazioni, anche attraverso la verifica dell'iscrizione alla CCIAA;

g) l'obbligo per il soggetto esecutore delle lavorazioni di dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva;

h) l'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi rilascia la dichiarazione di conformità alle regole dell'arte;

i) con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del datore di lavoro, sono attuati specifici presidi di controllo che prevedono l'individuazione della normativa applicabile (art. 26 o Titolo IV del Testo Unico Sicurezza);

☞ **Procure e deleghe - Contratti**

Verificare che i poteri autorizzativi e di firma assegnati siano:

(i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;

(ii) chiaramente definiti e conosciuti all'interno della struttura organizzativa;

☞ **Ruoli e responsabilità - Rapporti con soggetti pubblici per la presentazione di documentazione tecnica, economica ed amministrativa**

Verificare che siano identificati i ruoli e le responsabilità di coloro che sono coinvolti nell'attività sensibile e/o intrattengono rapporti con soggetti pubblici.

☞ **Segregazione dei compiti - Adempimenti di legge**

Verificare che sia garantita l'esistenza di segregazione tra chi predispone la documentazione e le dichiarazioni e chi, dopo aver verificato la corretta compilazione, la completezza e la veridicità dei dati riportati, le sottoscrive.

☞ **Tracciabilità - Rapporti con la pubblica amministrazione per richieste autorizzative**

Accertare che siano garantiti i seguenti principi:

i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata;

ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali;

iii) le principali fasi del processo in oggetto devono essere opportunamente documentate ed archiviate presso gli uffici competenti. In particolare, i documenti necessari alla predisposizione delle domande, compresi i documenti trasmessi dalle funzioni competenti per la compilazione delle stesse, le dichiarazioni trasmesse alla Pubblica Amministrazione e le relative ricevute di invio devono essere opportunamente tracciate ed archiviate.

☞ **Procedure - Gestione delle emergenze**

Accertare che sia adottata una procedura per la gestione dell'attività sensibile in esame che preveda al suo interno i seguenti elementi essenziali:

- l'identificazione delle situazioni che possono causare una potenziale emergenza;
- definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di salute e sicurezza;
- modalità e responsabilità di gestione delle prove di emergenza, con particolare riguardo alla tipologia di emergenza (es. incendio, evacuazione, ecc.);
- pianificazione ed esecuzione delle prove di emergenza per la verifica dell'efficacia dei piani di gestione delle emergenze;
- individuazione, attraverso detti piani, dei percorsi di esodo e delle modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze.

☞ **Procedure - Gestione di incidenti non conformità e azioni correttive**

Accertare che sia adottata una procedura per la gestione dell'attività sensibile in esame che preveda al suo interno i seguenti elementi essenziali:

- deve essere garantito l'accesso delle informazioni al Rappresentante dei Lavoratori per la sicurezza (RLS);
- devono essere attuate le azioni correttive e preventive di miglioramento individuate nelle riunioni periodiche della sicurezza e approvate dal datore di lavoro, presidiandone lo stato di avanzamento e valutandone gli effetti migliorativi;

- devono essere segnalate tempestivamente eventuali criticità nella messa in atto delle misure di cui sopra;
- devono essere raccolte e valutate le segnalazioni dei Preposti;
- devono essere effettuati sopralluoghi nei quali vengono notificate eventuali non conformità e programmati gli opportuni interventi risolutivi.

☞ **Procedure - Sorveglianza sanitaria**

Accertare che sia adottata una procedura per la gestione dell'attività sensibile in esame che preveda al suo interno i seguenti elementi essenziali:

- deve essere garantita la formazione dei lavoratori della banca;
- deve essere assicurata l'attuazione della sorveglianza sanitaria;
- devono essere definite le modalità di verifica dei requisiti per quanto riguarda gli aspetti sanitari, se riscontrati in sede di valutazione del rischio, da effettuare preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore.

Flussi informativi a favore dell'OdV

Il referente interno della sicurezza, annualmente e all'occorrenza, produce report informativo all'OdV circa:

- gli attestati rilasciati agli addetti alle emergenze;
- sintesi informativa del contenuto dei verbali delle riunioni periodiche;
- il numero e l'esito dei controlli effettuati in autonomia e quelli programmati come indicati nella procedura *SGSL*;

Il RSPP – direttamente o per il tramite del Responsabile del Settore Infrastrutture e Spese - annualmente fornisce report in merito:

- ai sopralluoghi effettuati, allegando i rispettivi verbali;
- agli eventi formativi e addestramento effettuati, allegando i relativi verbali
- agli aggiornamenti effettuati sui documenti del comparto;

Il tutor per la formazione – anche per il tramite dell'incaricato all'Ufficio Personale – produce report annuale in merito:

- ai futuri periodi formativi programmati, nonché resoconto di quelli effettivamente svolti nel corso dell'anno, assicurando che tutto il personale vi abbia effettivamente partecipato;

- all'aggiornamento delle certificazioni conferite al personale.

Articolo 25-octies - Ricettazione, Riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

L'art. 63 del D. Lgs. 21 novembre 2007 n. 231, riguardante "*l'attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*", ha introdotto l'art. 25 octies[40] che estende l'ambito della responsabilità in relazione ai reati di:

1) ricettazione (art 648 c.p.), commesso, fuori dai casi di concorso nel reato, da chiunque acquista, riceve od occulta, denaro o cose provenienti da un qualsiasi delitto al fine di procurare a sé o ad altri un profitto

   Le condotte punite si sostanziano:

   - in qualsiasi attività negoziale che consenta il trasferimento del possesso del denaro o cosa da un soggetto ad un altro;
   - nel conseguire il possesso in modo diverso rispetto all'acquisto;
   - nel nascondere (anche solo temporaneamente) dopo averne avuto la disponibilità;
   - nell'intervento volto a mettere in contatto chi ha commesso il reato presupposto con chi esegue la condotta tipica della ricettazione (primi tre alinea).

   Il reato in esame si realizza qualora la Banca consapevolmente acquisti/acquisisca denaro o altri beni provenienti da un qualsiasi delitto, ovvero compia in relazione ad essi altre operazioni volte a consentire ad altri la ricettazione, traendone beneficio (es. minori costi, maggiori ricavi, retention di un cliente, etc.) o procurando ad altri un profitto.

2) riciclaggio (art. 648 bis c.p.), commesso, fuori dei casi di concorso nel reato, da chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da un delitto ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione delittuosa della loro provenienza.

   Il delitto di riciclaggio ha natura plurioffensiva. Tra i vari beni giuridici tutelati prevalgono l'amministrazione della giustizia e l'ordine economico generale.

   Il reato in esame si realizza qualora la Banca, consapevolmente, sostituisca o trasferisca denaro, beni o altre utilità provenienti da delitto, ovvero compia in relazione ad essi altre

[40] In vigore dal 29/12/2007 - modificato dalla L. n. 186/2014 e dal D.Lgs. 8 novembre 2021, n. 195 (quest'ultimo in vigore dal 15/12/2021).

operazioni (es. occultamento di taluno dei nominativi coinvolti nelle operazioni) in modo da ostacolare l'identificazione della loro provenienza delittuosa.

3) impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.), commesso, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli precedenti, da chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

4) autoriciclaggio (art. 648-ter.1 c.p.).
Con la L. 15/12/2014, n. 186, avente decorrenza dal 01/01/2015, è stato introdotto il reato di autoriciclaggio che prevede la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 per chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La norma incrimina chi avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare l'identificazione della loro provenienza delittuosa. L'articolo prevede alcune ipotesi nelle quali le sanzioni previste per il reato in esame possano essere maggiorate, ovvero, ridotte; a tal proposito il comma 5, stabilisce che la pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria, finanziaria o di altra attività professionale.

A fattor comune si evidenzia che in ragione dei suindicati reati, è previsto che il Ministero della giustizia, sentito il parere dell'UIF, formula le osservazioni di cui all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231. Ciò significa che l'UIF dovrà valutar e il grado di coinvolgimento della Banca e la corretta adozione del modello di gestione tale da escludere la colpa organizzativa e tutti i requisiti previsti ai fini delle esimenti di responsabilità.

Altresì, il legislatore italiano, con il decreto legislativo, 8 novembre 2021, n. 195,[41], dando attuazione alla direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al *riciclaggio mediante diritto penale*, è intervenuto su tale disciplina a livello domestico, apportando diverse modifiche al Codice penale.

[41] Pubblicato sulla Gazzetta ufficiale del 30 novembre 2021

Più nel dettaglio, le modifiche hanno riguardato gli artt. 9, 240-*bis*, 648, 648-*bis*, 648-*ter* e 648-*ter.1* del Codice penale.

Per quanto concerne il delitto di ricettazione, il Governo si è limitato sostanzialmente ad adeguare l'aspetto sanzionatorio del reato ritenendo la fattispecie in linea con le previsioni comunitarie, salvo che per l'estensione alle contravvenzioni quali presupposto della condotta in conformità all'art. 2 par. 1 della direttiva che descrive una nozione di "attività criminale" comprensiva di qualsiasi tipo di reato presupposto punito con pena detentiva massima superiore ad un anno e pena minima di sei mesi.

In tal direzione è stato sostituita la parola "delitto" con "reato" nel testo del terzo comma dell'art. 648 c.p. e sono stati introdotti due nuovi commi che prevedono, rispettivamente la pena della reclusione da uno a quattro anni e della multa da 300 a 6.000 euro quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi e l'aumento di pena quando il fatto sia commesso nell'esercizio di un'attività professionale. L'aggravante appena menzionata è in linea con la Direttiva anche se presenta un più ampio margine di operatività rispetto a questa: ed invero la Direttiva impone un aggravamento della pena se autore del reato è un soggetto obbligato al rispetto della normativa antiriciclaggio che abbia commesso il reato nell'esercizio della sua attività professionale; l'aggravante introdotta dal Decreto legislativo consente di aumentare la pena se il reato è commesso nell'esercizio di una attività professionale anche se l'autore non è soggetto obbligato nei sensi di cui sopra: ne consegue che l'attività professionale prevista dall'aggravante in questione non è solo quella per la quale è prevista una speciale abilitazione, ma qualsiasi attività economica o finanziaria diretta a creare nuovi beni e servizi oppure attività di scambio e di distribuzione dei beni nel mercato del consumo.

Al fine di rispettare l'esigenza di proporzionalità della pena prevista dall'art. 5 par. 1 della direttiva, il Decreto legislativo ha sostituito l'attuale capoverso dell'art. 648 riguardante il fatto di particolare tenuità, prevedendo una incidenza differenziata della circostanza a seconda che il reato presupposto sia un delitto o una contravvenzione: nel dettaglio, la pena della reclusione sino a sei anni e della multa sino a 1000 euro nel caso di danaro o cose provenienti da delitto e la pena della reclusione sino a tre anni e della multa sino a 800 euro nel caso di danaro o cose provenienti da contravvenzione.

La lett. b dell'art. 1 del Decreto legislativo fa, infine, riferimento a questa nuova ipotesi di particolare tenuità della ricettazione, prevista ora al quarto comma dell'art. 648, per escludere l'applicabilità della confisca obbligatoria.

Quanto all'art. 648 bis (riciclaggio) c.p., al fine di rendere compatibile l'attuale previsione del codice penale italiano alla nozione europea di "*attività criminosa*", il Governo ha soppresso le parole "*non colposo*" dal testo del primo comma dell'art. 648 bis c.p., estendendo ai delitti colposi i presupposti della condotta di riciclaggio e ha introdotto una disciplina sanzionatoria di minor rigore per il caso in cui il reato presupposto sia una contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi: reclusione da 2 a 6 anni e multa da 2500 a 12.500 euro.

Analoga previsione è stata introdotta dalla lettera e) dell'art. 1 all'art. 648 ter c.p.[42] – reato per il quale è, inoltre, modificato, per ragioni di coordinamento, il riferimento all'articolo 648 di cui all'ultimo comma dell'articolo 648-ter - e dalla lett. f) dell'art. 1 all'art. 648 ter. 1 c.p. (Autoriciclaggio).

Per quest'ultimo, introdotto nel nostro ordinamento già dal 2014, è stata pure operata la soppressione delle parole "*non colposo*" di seguito a "*delitto*", estendendo le condotte criminose che costituiscono reato presupposto; inoltre, è stata modificata la diminuente di cui al secondo comma, prevedendo che la pena è ridotta se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della ·reclusione inferiore nel massimo a cinque anni; infine, è stata apportata una modifica di coordinamento al terzo comma.

Su tale fattispecie, come si evince dalla relazione illustrativa, non si è ritenuto di intervenire apparendo il riferimento all'impiego "*in attività economiche, finanziarie, imprenditoriali o speculative*" in linea con quanto previsto dall'art. 3, par. 5, della direttiva che impone agli Stati membri di perseguire come reato anche le condotte poste in essere dall'autore dell'attività criminosa che ha generato i beni: ciò alla luce della consolidata interpretazione della giurisprudenza di legittimità che privilegia una nozione ampia di attività economica o finanziaria, ricomprendendo in essa anche l'ulteriore trasferimento del bene di provenienza illecita non inquadrabile in una stabile e organizzata attività economica o commerciale.

Passando alla parte operativa riguardante la struttura del MOG e come anche spiegato nella parte generale la Banca:

- ai sensi del D.Lgs. 231/2001, viene presa in considerazione come impresa ed è responsabile se i reati previsti vengono commessi dai propri vertici o dai dipendenti nell'interesse o a vantaggio della banca stessa;

[42] Impiego di denaro, beni o utilità di provenienza illecita.

- ai sensi del D.Lgs. 231/2007, è chiamata a svolgere una funzione inquadrabile tra i doveri civici di collaborazione con i pubblici poteri, ai fini della prevenzione e repressione del rischio di riciclaggio e finanziamento al terrorismo.

Le due prospettive sono, pertanto, complementari: nel momento in cui i protocolli organizzativi e il sistema di controllo garantiscono che i moduli operativi seguiti dal personale interno siano conformi a quelli prescritti ex lege, allo stesso modo essi prevengono le occasioni di verificazione di fatti di riciclaggio da parte di apicali o dipendenti. L'ampiezza della definizione amministrativa di riciclaggio conferma che le finalità preventive, sotto il profilo dell'organizzazione dell'ente, non sono limitate ai soli rischi di controparte, esogeni, bensì ineriscono anche ai fattori di rischio che originano all'interno della banca, dagli stessi soggetti che concorrono a formare l'organigramma societario. In definitiva, i due modelli di prevenzione del medesimo fenomeno criminoso, esprimono, in realtà, significative sinergie, nel senso che si integrano con i protocolli e le procedure che la banca adotta nel proprio sistema di controllo ed operativo.

Ne consegue che le policy ed i regolamenti di processo possono ben rappresentare idonei protocolli atti a prevenire i reati del genere, avendo riguardo sia alle esigenze commerciali e sia al principio di legalità che la banca ha fatto proprio e, quindi, da preservare come requisito fondamentale della crescita economica, poiché la criminalità (nelle sue conformazioni), la corruzione e l'evasione fiscale inquinano l'attività di impresa e l'occupazione, riducendo quindi la possibilità di crescita economica.

Descrizione dei rischi in relazione ai reati di cui all'articolo 25-octies

Con riferimento all'ipotesi in cui tali reati vengano commessi da operatori bancari, si ritiene, anche alla luce dell'attuale casistica, che il rischio della loro commissione sia meno elevato. Infatti, perché possano sussistere i presupposti per un eventuale responsabilità amministrativa della Banca, gli esponenti o i dipendenti dovrebbero commettere intenzionalmente detti reati nell'interesse o a vantaggio della Banca stessa. Nella storia della Banca si è verificato un solo caso oggetto di procedimento penale della specie, dove - per quanto noto – i soggetti coinvolti nella vicenda risultano aver agito per fini personali, avuto anche riguardo al fatto che una richiesta da parte della locale Procura della Repubblica di produzione del MOG vigente all'epoca, non risulta aver avuto seguito circa l'eventuale responsabilità in capo alla Banca.

A. Con riferimento al reato di ricettazione, rilevano i seguenti rischi:
   i. accettare a garanzia di un affidamento un pegno costituito da merce proveniente da un'azione delittuosa, quali opere d'arte, preziosi, o altro;
   ii. acquistare deliberatamente merce proveniente da un'azione delittuosa, nell'ambito del processo di acquisto di beni, nel caso in cui il corrispettivo offerto dai soggetti terzi

fornitori sia al di fuori di qualsiasi parametro di mercato e tale da ingenerare fondati dubbi sulla legittimità della provenienza della merce.

A tale riguardo si potrebbe configurare come attività sensibile la selezione del fornitore e stipula dei contratti di appalto per la fornitura di beni.

Ulteriori possibili occasioni potrebbero essere individuate nei seguenti casi:

iii. compravendita di opere d'arte o beni di consumo (computer, arredi, etc.);
iv. compravendita o locazione di immobili;
v. investimenti di denaro proveniente da furto o vendita di beni rubati;
vi. accoglimento di depositi in denaro provenienti da furto o dalla vendita di beni rubati;
vii. movimentazioni economiche relative ad ogni genere di rapporti bancari;
viii. servizi di prestito su pegno;
ix. acquisizione in pegno di cosa di provenienza furtiva.

B. Per quanto attiene, invece, al rischio di riciclaggio e autoriciclaggio, va fatto osservare che colpiscono la circolazione dei profitti derivati da tutti i reati. Le fattispecie si configurano come trasversali rispetto al sistema organizzativo aziendale e vengono esposti al rischio reato tutti i processi che comportano l'impiego di denaro che possono essere considerati come proventi da un reato e/o abbiano l'effetto di creare un ostacolo alla identificazione circa la provenienza illecita dei beni.

Con l'introduzione del reato di autoriciclaggio tra i reati presupposto comporta, indirettamente una estensione delle aree di rischio, poiché il profitto oggetto di autoriciclaggio può derivare dalla commissione di qualsiasi delitto, anche se non compreso nel catalogo dei reati presupposto.

Considerato il contesto in cui opera la Banca, ovvero il circuito bancario nazionale e internazionale, che per sua natura e funzione agevola lo scambio di risorse finanziarie tra soggetti diversi, la Banca è potenzialmente esposta al rischio della commissione dei suddetti reati con riferimento alle condotte della clientela, ancor più significativamente alla luce degli eventi pandemici, poiché si è registrato un repentino innesto di una nuova prospettiva del fenomeno, passando dal *money-laundering* al *money-dirtying*[43].

In sintesi, la clientela, oltre ad utilizzare il sistema finanziario per "ripulire" i beni di illecita provenienza indebitamente acquisiti, tende anche ad impiegare i beni di provenienza lecita per finalità illecite[44].

[43] Money-laundering: pulizia del danaro sporco >>> Money-dirtyng: sporcamento del danaro pulito.

[44] Fidi, contributi e fondi pubblici, redditi d'impresa, ecc…

Tenuto anche conto che il riciclaggio è una tipologia di reato trasversale a qualunque illecita attività, le aree di attività ritenute più a rischio sono connesse ai rapporti finanziari intrattenuti in qualità di intermediario finanziario con la propria clientela.
Tali rapporti sono stati così individuati:

1) erogazione di servizi finanziari alla clientela nell'ambito di rapporti continuativi (Conti correnti, Libretti di risparmio, Certificati di Deposito, Carte prepagate e Servizi ad essi collegati);
2) erogazione di servizi finanziari alla clientela occasionale.

Inoltre, rilevano i seguenti rischi:

a) Omessa o incompleta identificazione della clientela al fine di favorire consapevolmente l'operatività illecita della clientela stessa.
b) Omessa registrazione di operazioni.
c) Omissione di controlli obbligatori relativi alle singole operazioni bancarie (es.: "accertamenti bancari"), al fine di favorire consapevolmente l'operatività illecita di un cliente.
d) Omesse segnalazioni di operazioni sospette per favorire consapevolmente l'operatività illecita di un cliente.
e) Eseguire operazioni "Italia o estero" favorendo un soggetto cliente o non cliente (operazioni per cassa) nel riciclaggio di denaro o identificare in modo non corretto un cliente allo scopo di non far emergere la sua operatività.
f) In fase di monitoraggio omettere deliberatamente di rilevare aspetti riconducibili ai reati di riciclaggio o impiego di denaro di provenienza illecita.

Altri possibili scenari potrebbero configurarsi attraverso:

- la costituzione o partecipazione ad un'associazione finalizzata ad attività di riciclaggio;
- gli investimenti con il patrimonio libero;
- la vendita o locazione di immobili di proprietà della Banca;
- l'intenzionale manomissione delle transazioni finalizzate ad ostacolare l'identificazione della provenienza del denaro;
- le movimentazioni economiche relative ad ogni genere di rapporti bancari.

Con riferimento al reato di autoriciclaggio si mira sostanzialmente a punire gli evasori fiscali. Come noto, infatti, l'evasione fiscale si concretizza per lo più nel risparmio di imposte e quindi nella disponibilità di somme che si possono reinvestire in attività economiche.

Laddove, pertanto, si scoprisse che un investimento in attività imprenditoriali o finanziarie sia stato realizzato con fondi provenienti da reati tributari, potrebbe scattare la condanna per autoriciclaggio anche se non si dovessero raggiungere i limiti per la punibilità dei reati fiscali così come previsti dalle leggi in materia.

Nella valutazione dei rischi si tiene, altresì, presente i due seguenti fattori:

a) L'introduzione dell'autoriciclaggio nel catalogo 231 comporta, indirettamente, una estensione delle aree a rischio; infatti, il profitto oggetto dell'autoriciclaggio può derivare dalla commissione di qualsiasi reato, ossia anche uno di quelli non compresi nell'elenco dei reati presupposto. Particolare rilievo assume – sotto il profilo dell'interesse e del vantaggio – l'esposizione al rischio dei processi attinenti alla contabilità rilevante ai fini fiscali.

b) Il rischio di riciclaggio è per sua natura additivo, cioè ogni nuovo cliente determina un incremento dell'esposizione al rischio. Pertanto, l'unico elemento di mitigazione del rischio consiste nella capacità di identificare correttamente tutti i fattori di rischio e di applicare misure organizzative coerenti per decidere se autorizzare l'accensione del rapporto, astenersi ovvero interrompere il rapporto d'affari, nonché inoltrare una SOS.

Un'altra area di attività potenzialmente a rischio, direttamente connessa ai rapporti propri, ancorché ai rapporti con la clientela, è individuabile nella possibile violazione dell'obbligo di non aprire o mantenere anche indirettamente conti di corrispondenza con una banca di comodo di cui all'articolo 25, comma 3 del D. Lgs. 231/2007.

Principali presidi organizzativi e gestionali

La Banca, in linea con quanto previsto in ambito legislativo e dalla normativa antiriciclaggio (D.lgs. 231/07), nonché delle indicazioni e delle linee guida delle autorità competenti, identifica i seguenti specifici presidi organizzativi e gestionali:

1) con riguardo alla normativa antiriciclaggio:
   - l'adeguata verifica della clientela ordinaria o rafforzata, con conseguente adozione di procedure, informatiche e documentali specifiche e obbligatorie, disposte in capo alle diverse funzioni, per fare fronte in modo efficace alle esigenze e alle indicazioni normative.
   - la registrazione dei rapporti continuativi e delle operazioni occasionali sulla base delle disposizioni di tempo in tempo vigenti.
   - le segnalazioni delle operazioni sospette.
   - la conservazione della relativa documentazione.

- l'adozione di procedure, informatiche e documentali, strutturate su base gerarchica, incombenti sulle diverse funzioni interessate ai diversi processi, in termini di responsabilità, controlli e resoconti. Si richiamano in questa sede gli adempimenti in occasione degli interventi nelle operazioni di cessione del credito da parte della clientela, cui tratta il recente D. Lgs. 157/2021; in particolare la Banca – anche in coerenza con le disposizioni della capogruppo. – ha adottato specifiche cautele, quali, ad esempio, la previsione dell'iter istruttorio in PEF per le posizioni a rischio di riciclaggio Alto, sebbene l'operazione non rappresenti in senso tecnico un affidamento. Ciò consente di documentare tutte le valutazioni effettuate dalla linea gerarchica competente e l'intervento sulla valutazione del rischio associato alla clientela da parte del Responsabile AML della Banca. Per quanto ovvio, in ossequio alle disposizioni normativa sopra richiamate, la Banca sarà in grado di astenersi dal compiere operazioni della specie e di valutarne la conseguente segnalazione di operazione sospetta alla UIF nell'ambito della prevista collaborazione attiva.
- l'intervento nelle attività da parte del responsabile/addetto alla funzione antiriciclaggio;
- l'intervento a livello accentrato della U.O. Incassi e Pagamenti per l'inoltro dei bonifici tramite rete interbancaria, ferma restando la validazione da parte del preposto alla filiale di competenza, ovvero dell'intervento del responsabile del Servizio Finanza nel caso di importi superiori a 50.000 euro;
- la costruzione di processi aziendali che consentono la piena tracciabilità delle operazioni e delle scelte, anche con riguardo alla trasparenza dei flussi monetari interni e all'adempimento degli obblighi tributari.

Va soggiunto, quale ulteriore presidio, il ruolo, la responsabilità e il coinvolgimento nel processo della Governance, quindi del CdA, che:

a. definisce e cura l'attuazione delle procedure di gestione dei rapporti con la clientela classificata ad "alto rischio";
b. stabilisce programmi di addestramento e formazione del personale sugli obblighi previsti dalla disciplina antiriciclaggio;
c. adotta gli strumenti idonei a consentire la verifica dell'attività svolta dal personale in modo da rilevare eventuali anomalie che emergano, con particolare riferimento nei comportamenti e nei rapporti del personale con la clientela;
d. adotta sempre una visione olistica del rischio AML, cioè attenta alle interrelazioni tra i vari fattori ed elementi dell'attività svolta con riferimento a:
    i. Prodotti e servizi offerti

ii. Tipologia di clienti

iii. Canali di commercializzazione e distribuzione.

e. si assicura che venga sempre effettua la valutazione del rischio di business in modalità «customizzata», prendendo in considerazione i fattori e i rischi peculiari del business medesimo, in una logica di proporzionalità rispetto alla natura e alla dimensione della stessa Banca, considerato che non vengono offerti prodotti o servizi complessi, che hanno un'operatività prevalentemente domestica.

2) Riguardo all'operatività creditizia di trade finance, sebbene la Banca non operi e comunque non ha clienti che svolgono significative operazioni con Stati esteri, i crediti documentari rappresentano la porzione più significativa di tali servizi.

I fattori di rischio sono caratterizzati dal fatto che la banca che intermedia una transazione ha un accesso parziale alle informazioni sulla transazione stessa e sulle parti principali. Inoltre, la documentazione dell'operazione non è sempre standard e la banca può non essere dotata di sufficiente esperienza nel trattarla. Per tale ragione:

- ☞ vengono assistite operazioni con controparti già sperimentate e, perlopiù operazioni effettuate entro l'U.E. o l'Area economica europea, in particolare con paesi ove vige un regime AML adeguato alla AMLD4 e che si caratterizzano per un basso livello di violazioni a tale regime;
- ☞ viene accertato sempre che il cliente conduca effettivamente un'attività commerciale ben nota e che la transazione sia in linea con la medesima attività.

Da ultimo, quale elemento di ulteriore novità, si fa riferimento alla normativa DAC6 [45], rivolta a combattere l'elusione fiscale internazionale e la pianificazione fiscale aggressiva attraverso la prevenzione del fenomeno, che consente l'accesso alle informazioni sui redditi o sui beni detenuti all'estero attraverso lo scambio automatico[46] di informazioni sui contribuenti impegnati in attività trasfrontaliere, considerato come una componente essenziale di un

[45] Directive Administrative Cooperation – DAC6: Direttiva UE 2016/2258, recepita in Italia attraverso il D.Lgs. 100/2020. La direttiva introduce nuove regole in materia di obbligo per gli Stati Membri di scambiare in maniera automatica le informazioni sui meccanismi transfrontalieri. In particolare, impone agli intermediari (e ai contribuenti) l'obbligo di comunicare alle amministrazioni finanziarie competenti informazioni complete e pertinenti sui meccanismi fiscalmente aggressivi di natura transfrontaliera. Inoltre, la DAC7: Direttiva 2021/514, da recepire entro il 2022, ultima in ordine cronologico, estende l'obbligo della comunicazione di dati in materia fiscale anche alle transazioni di beni e servizi che vengono offerti tramite le piattaforme digitali.

46 La forma di scambio automatico delle informazioni si ha quando le autorità competenti degli Stati concordano di scambiarsi in maniera sistematica e regolare informazioni, a prescindere da una preventiva richiesta e, normalmente, per specifiche categorie di reddito.

efficace sistema di cooperazione amministrativa, allo scopo di arginare la diffusione di pratiche fiscali dannose.

Al riguardo, si richiama in questa sede che il sistema dei controlli interni della banca è chiamato anche a considerare in modo adeguato il rischio fiscale laddove esso risulta interconnesso con il rischio di riciclaggio, reputazionale e di responsabilità penale. Infatti, il sistema dei controlli interni è stato adeguato alla normativa europea DAC6 che ha introdotto in Italia obblighi specifici per intercettare meccanismi transfrontalieri soggetti a segnalazione verso l'Autorità tributaria. Per quanto ovvio la valutazione è sempre connaturata all'attività di business svolta dalla banca, tenendo anche conto che i meccanismi transfrontalieri oggetto di segnalazione possono individuarsi in ogni servizio prestato alla clientela, dalla gestione delle operazioni creditizie alla prestazione di servizi di investimento con speciale riferimento alla gestione di patrimoni o al collocamento di operazioni di cessione di crediti.

Al riguardo sono state valorizzate le strutture interne dedite alla gestione delle tematiche fiscali anche attraverso il coinvolgimento operativo delle strutture presso la capogruppo.

3) Con riguardo alla normativa sul finanziamento del terrorismo internazionale e più precisamente la gestione dell'Anagrafe Negativa, il relativo Sistema di WARNING e le attività connesse alle evidenze ditale anagrafe.
4) In materia di acquisti: procedure di acquisto, regolate dal sistema delle deleghe e dei poteri e dal regolamento Infrastrutture e spese, nonché il Codice Etico.

A fattor comune, infine, si richiamano i presidi, le regole ed i controlli indicati singolarmente nel regolamento antiriciclaggio, nel regolamento del credito e nei regolamenti dei singoli processi interessati nelle diverse operazioni.

Flussi informativi a favore dell'OdV

Al riguardo si fa riferimento alla direttiva di indirizzo e coordinamento del GBCI in materia di coordinamento delle funzioni aziendali di controllo e al relativo schema dei flussi informativi verso gli organi aziendali, tempo per tempo vigente.

Valgono, altresì, i flussi informativi rinvenienti dalle riunioni di coordinamento tra l'OdV e le funzioni aziendali di controllo ed il comitato interno rischi.

Articolo 25-octies.1 Delitti in materia di strumenti di pagamento diversi dai contanti

È evidente che tra i nuovi reati sicuramente rilevano la gestione amministrativa, la gestione degli acquisti e quella dei flussi finanziari, normalmente già mappati ai fini dei reati di riciclaggio e autoriciclaggio, con i quali le nuove fattispecie mostrano evidenti affinità.

In particolare, salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, nell'ipotesi in cui qualsiasi altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio, abbia ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente sanzioni pecuniarie.

Principali presidi organizzativi e gestionali

A fattor comune valgono i presidi organizzativi e gestionali indicati nella sezione relativa ai reati di cui all'articolo 24-bis del presente documento, come pure i presidi specificati al precedente articolo 25-octies relativamente ai reati di riciclaggio e autoriciclaggio, in quest'ultimo caso anche riguardo alle operazioni con valute virtuali, laddove la Banca ne ha contezza in via indiretta e solo attraverso l'analisi di dettaglio delle singole operazioni rilevanti ai fini del processo di adeguata verifica.

La Banca, nel caso di specie, è soggetta a diversi tipi di controllo, i quali, peraltro, risultano preminenti sia da parte della capogruppo e sia da parte dell'autorità di vigilanza.

Con particolare riferimento al comparto della monetica, la banca svolge il ruolo di collocamento e, quindi, meramente esecutrice, posto che i controlli ed il monitoraggio dell'operatività è riconducibile ad Iccrea Banca, attraverso le U.O. Issuing e Acquiring che gesticono il processo, mentre la U.O. AML ne presidia il relativo rischio.

Parimenti, riguardo al comparto dei sistemi di pagamento diversi dal contante – come declinati dalla normativa – la gestione e i controlli conseguenti sono incardinati presso l'outsourcer informatico della capogruppo.

Flussi informativi a favore dell'OdV

Per i flussi informativi in questione, si rinvia a quelli indicati nelle sezioni dei singoli specifici reati.

Articolo 25-novies - Delitti in materia di violazione del diritto d'autore

Tra i reati ivi previsti, potrebbero in astratto essere commessi nell'ambito delle attività della banca e nell'interesse di quest'ultima le fattispecie previste:

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171, c. 1 lett. a-bis e c. 3, L. 633/1941), che sanziona chiunque metta a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere,

un'opera di ingegno protetta o parte di essa, con un aggravio di pena nel caso in cui l'opera altrui non sia destinata alla pubblicazione o nel caso in cui vi sia usurpazione della paternità dell'opera, ovvero deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore;

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio**[47] (art. 171-bis, L. 633/1941) che punisce chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);
- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171-ter, L. 633/1941) che punisce l'abusiva duplicazione, trasmissione, riproduzione o diffusione di altre opere protette dal diritto d'autore;
- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171-septies, L. 633/1941): «1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:
  - ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
  - salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge»;
- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171-octies, L. 633/1941): «1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi. visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio;

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità».

Descrizione dei rischi in relazione ai reati di cui all'articolo 25-novies

A seguito del recepimento delle direttive 96/9/CE e 91/250/CEE rientrano nella disciplina del diritto d'autore anche i programmi per elaboratore e le banche di dati. Con il decreto legislativo 6 maggio 1999 n. 169 l'Italia ha attuato la direttiva 96/9/CE relativa alla tutela giuridica delle banche dati. Esse sono definite normativamente nel sistema italiano come una raccolta di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo[48] e la durata dei diritti del costitutore sulla banca dati è di quindici anni decorrenti dal 1° gennaio dell'anno successivo alla data del completamento della banca dati.

La scelta effettuata dal legislatore italiano di includere le banche dati tra le opere protette dalla "*Legge sul Diritto d'Autore*" è dovuta al carattere di originalità che può assumere un insieme di dati raccolti secondo criteri specifici e con un eventuale scopo, costituendo in tal modo una creazione intellettuale al pari di un software o di una qualsiasi altra opera multimediale.

Tuttavia, con riguardo alla tipologia di reati previsti nella presente sezione, si ritiene come potenziale rischio possibile - dalla cui attività la banca ne potrebbe trarre un beneficio economico - sono:

- l'abusiva duplicazione, al fine di installare programmi per elaboratore soggetti alle norme sul diritto d'autore sui PC dell'azienda,
- l'utilizzo di software con numero di licenze superiore a quelle acquistate.

Principali presidi organizzativi e gestionali

In linea generale, in tale specifico settore, la Banca ricorre all'adozione di modelli preventivi fondati sulla concentrazione delle funzioni informatiche in unità funzionali ovvero organi unici, in outsourcer ed interni all'azienda, cui compete la gestione esclusiva del sistema informativo aziendale (ivi comprese le operazioni di manutenzione e aggiornamento), nonché l'approvvigionamento delle risorse informatiche (ad es. software e applicazioni) per l'intero assetto organizzativo. La concentrazione di tali funzioni informatiche garantisce maggiori prestazioni "prevenzionistiche" in termini di capacità di controllo e rivelazione delle prassi comportamentali di tipo endemiche, capaci di degenerare in violazioni (penalmente rilevanti) del copyright. La conformazione della struttura aziendale all'obiettivo preventivo, attraverso la

[48] Cfr. punto 9 – art. 2 Legge n. 633/41 TU Diritto d'Autore e ss.

previsione di un'area interna autonoma, dedicata ai "sistemi informativi", peraltro, risulta complementare all'adozione di un modello organizzativo che assicuri un'efficace procedimentalizzazione delle c.d. attività informative, mediante la definizione delle singole procedure aziendali, valorizzando quanto più possibile la sinergia con l'ulteriore obiettivo di prevenzione dei reati commessi mediante l'impiego di mezzi informatici o della rete internet[49].

Oltre ai presidi di carattere generale, che disciplinano gli aspetti etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, la Banca, allo scopo di evitare ogni possibile illecito uso da parte degli utenti, consente le funzioni di installazione sui singoli PC esclusivamente in capo all'amministratore di sistema nell'ambito dell'ufficio Organizzazione, dove il responsabile ricopre anche il ruolo di Security Manager. Questi provvede anche a verificare la corrispondenza del numero di licenze con il numero delle macchine possedute.

Parimenti, le piattaforme e gli applicativi utilizzati per il tramite di servizi gestiti in outsourcing, le società fornitrici assicurano l'autenticità dei software installati suoi pc aziendali. Si citano a titolo di riferimento gli applicativi gestionali di BCC SI, di Iccrea e Sinergia (quest'ultima anche per la videoconferenza), nonché i sistemi di interrogazione delle banche dati di cui la Banca fa ordinario utilizzo per le varie interrogazioni.

Va, infine, precisato che la banca ha aderito ad un progetto di acquisizione di applicativi di office automation attraverso la capogruppo le cui licenze sono interamente tutelati (per esempio Office 365).

Ad ogni buon conto, gli organi sociali, i dirigenti ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- vigilare sui processi di approvvigionamento dei beni protetti da proprietà intellettuale;
- rispettare la proprietà intellettuale di terzi nello svolgimento di attività, ivi comprese quelle di comunicazione o marketing, che possano comportare l'utilizzo di opere soggette al diritto d'autore;

Inoltre, è fatto divieto di:

- copiare i programmi software di proprietà della Società installati sui computer aziendali;

[49] Cfr. artt. 24, 24-bis, 25-quater, 25-quinquies, c. 1, lett. c, d.lgs. n. 231/2001

- installare sui computer aziendali software non autorizzati dall'Ufficio competente;
- installare o copiare opere tutelate dal diritto d'autore su un numero di apparecchi superiore rispetto al numero di licenze acquistate;
- installare o copiare opere tutelate dal diritto d'autore non munite di contrassegno SIAE o con contrassegno contraffatto (ad esempio libri, riviste, cd, etc.);
- riprodurre (in modo permanente o temporaneo, totale o parziale), tradurre, adattare, trasformare, distribuire software di proprietà di terzi acquisiti in licenza senza preventiva autorizzazione;
- riprodurre, nei documenti della banca, immagini, contenuti, oggetti protetti dal diritto d'autore senza apposita autorizzazione dei legittimi proprietari.

Protocolli Specifici

Oltre ai protocolli esistenti e già citati in precedenza con riferimento ad altre fattispecie di rischio, che qui si intendono per richiamati, la Banca ha predisposto e adottato (anche per il tramite di outsourcer) i seguenti strumenti:

- Politiche di sicurezza e Privacy – Dipartimento IT, diffuso tra le funzioni aziendali e consegnato a tutti i neoassunti al momento della sottoscrizione del contratto.
- Procedura per la gestione dei rapporti con la P.A., con riferimento alla trasmissione di documenti informatici aventi efficacia probatoria.
- Audit periodici sul sistema informatico.
- misure tecniche e tecnologiche quali:
  - URL Filtering;
  - gestione dei Proxy;
  - Spam Monitoring;
  - installazione e aggiornamento di sistemi antivirus e firewall;
  - protocollo sul processo di gestione della comunicazione.
- **Monitoraggio su software, programmi e applicazioni informatiche**: dove sono definite le regole per l'utilizzo degli strumenti informatici aziendali e le attività di controllo su software, programmi, applicazioni informatiche installate su tali dispositivi, al fine di verificare che non vengano scaricate applicazioni potenzialmente utili alla commissione di attività illecite e / o contrarie alle disposizioni aziendali definite (es. manomettere il sistema informatico di terzi, accedere impropriamente al sistema dei pagamenti interno per finanziare la commissione di reati 231).

- **Controllo sicurezza su accesso a sistemi**: dove vengono definiti criteri e regole di autorizzazione per l'accesso ai sistemi informatici aziendali; tali accessi vengono costantemente monitorati in termini di utenti che vi accedono e di attività consentite. Inoltre, sono state implementate adeguate misure di sicurezza che impediscono l'accesso al sistema informativo da parte di terzi non autorizzati (dotazione di firewall).
- **Monitoraggio periodico sugli amministratori di sistema**: al riguardo vengono poste in essere specifiche attività di controllo sull'attività degli amministratori di sistema e su software, programmi e applicazioni presenti sui loro dispositivi informatici.

Flussi informativi a favore dell'OdV

Valgono al riguardo i report di monitoraggio forniti dal gestore in outosourcing del sistema informativo, nonché i report originati dall'ufficio controlli interni alla banca, compreso il rendiconto sulle attività dell'amministratore di sistema.

I flussi al riguardo devono avere periodicità annuale, fatte salve specifiche circostanze.

Articolo 25-decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

La Legge n. 116 del 3 agosto 2009 di *"Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale"*, con l'art. 4 ha introdotto nel Decreto l'articolo 25 decies[50], con riferimento al reato di cui all'art. 377 bis del codice penale "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*".

Si valuta possibile il rischio che, nel corso di un procedimento innanzi all'Autorità Giudiziaria, qualcuno della Banca potrebbe indurre un soggetto chiamato a testimoniare a non rilasciare dichiarazioni o a rilasciare dichiarazioni non corrispondenti al vero.

Vale tuttavia a presidio di tale rischio l'affidamento a professionisti esterni degli incarichi di natura legale, i quali sono le uniche figure titolate a gestire i procedimenti penali e civili. All'interno dell'organizzazione della Banca opera un ufficio legale che svolge esclusivamente attività ed adempimenti di carattere amministrativo e gestionale.

Il sistema delle deleghe prevede la possibilità di scelta del professionista e conseguente conferimento dell'incarico al Presidente del Cda che vi provvede per incarico del Consiglio, mentre il rapporto con i legali in costanza di procedimento viene mantenuto anche dal Direttore Generale per i profili gestionali.

[50] In vigore dal 15 agosto 2009. Titolo così modificato dall'articolo 2 del D.Lgs. n. 121 del 7 luglio 2011, in vigore dal 16/8/2011, che ha modificato l'articolo 4 della legge 3 agosto 2009, n. 116.

Articolo 25-undecies Reati ambientali

L'art. 2, comma 2, del decreto legislativo 7 luglio 2011, n. 121 "Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni", ha introdotto l'art. 25 undecies[51] per i reati ambientali elencati nella parte generale del presente documento.

Tenuto conto della specifica attività svolta dalla Banca, si valuta che trattasi di reati di difficile realizzazione. Non appare, infatti, ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti della Banca possano porre in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio della Banca, fatti o azioni in violazione delle norme ambientali indicate nel Decreto.

Sono stati, altresì, valutati i casi relativi allo smaltimento di rifiuti, nonché la gestione di ristrutturazioni di immobili di proprietà o relativi a leasing immobiliare (sempre in caso di smaltimento di rifiuti pericolosi) ed infine lo smaltimento di apparecchiature elettroniche/ informatiche (monitor, pc, cellulari), toner/ contenitori inchiostri di stampanti e fotocopiatrici.

A fattor comune si riporta che la Banca affida le suindicate attività a società esterne, preventivamente valutate ai fini dei requisiti richieste dalle normative di settore. I toner sono smaltiti tramite l'affidamento a società esterna competente che ad ogni ritiro dei toner da smaltire consegna alla banca un documento in cui dichiara quanto è stato ritirato e le modalità/luogo di smaltimento. Le apparecchiature dismesse (rifiuti pericolosi quali computer), invece, fintanto che rimangono nella disponibilità della Banca, vengono conservate in apposito deposito interno alla Sede o alla singola Filiale.

[51] In vigore dal 16 agosto 2011.

Articolo 25-duodecies - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

La norma mira a punire il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri irregolari, commettendo il reato nella forma aggravata, ossia nei casi di più di tre lavoratori, oppure minori di età, oppure in condizione di sfruttamento.

Anche in questo, tenuto conto della specifica attività svolta dalla Banca, si valuta che trattasi di reati di difficile realizzazione. Non appare, infatti, ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti della Banca possano porre in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio della Banca, fatti o azioni in violazione delle norme della specie.

Si valuta, per altro verso, possibile il rischio che la banca possa finanziare (anche inconsapevolmente) clientela dedita alla commissione di tali reati. A tal fine valgono i presidi previsti nel regolamento a presidio del rischio di riciclaggio.

Si richiamano in questa sede, in quanto compatibili, i presidi ed i protocolli declinati nell'ambito della sicurezza nei luoghi di lavoro.

Articolo 25-terdecies Razzismo e xenofobia

Tenuto conto della specifica attività svolta dalla Banca, si valuta che trattasi di reati di difficile realizzazione. Non appare, infatti, ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti della Banca possano porre in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio della Banca, fatti o azioni in violazione delle norme della specie.

Art. 25- quinquesdecies – Reati tributari

Tra le importanti novità previste dalla Legge n. 157 del 19 dicembre 2019 (entrata in vigore il 25 dicembre 2019), che ha convertito il D.L. n. 124/2019 (c.d. "Decreto Fiscale"), vi è l'inclusione di taluni reati tributari previsti dal D. Lgs. n. 74/2000 tra quelli presupposto della responsabilità amministrativa degli enti.

L'art. 25-quinquiesdecies, co. 1, del D. Lgs. n. 231/2001 estende il perimetro dei reati presupposto per la responsabilità amministrativa degli enti, includendovi le seguenti fattispecie:

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art.2 D.Lgs. 10 marzo 2000, n.74) (ultime modificazioni con Dl. 26 ottobre 2019, n. 124)

2. Il fatto si considera commesso avvalendosi di fatture o 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.

2-bis. 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. 10 marzo 2000, n.74) (ultime modificazioni con Dl. 26 ottobre 2019, n. 124)

1. Fuori dei 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, sulla base di una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi fraudolenti idonei ad ostacolarne l'accertamento, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi, quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a lire centocinquanta milioni; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a lire tre miliardi.

Emissione di fatture o altri documenti per operazioni inesistenti (Art.8 D.Lgs. 10 marzo 2000, n.74) (ultime modificazioni con Dl. 26 ottobre 2019, n. 124)

1. 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.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Occultamento o distruzione di documenti contabili (Art.10 D.Lgs. 10 marzo 2000, n.74) (ultime modificazioni con Dl. 26 ottobre 2019, n. 124)

1. 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 di imposte (Art.11 D.Lgs. 10 marzo 2000, n.74).

1. 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.

Le attività individuate come potenzialmente sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati tributari

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'art. 25-quinquiesdecies del d.lgs. 231/2001 (Reati Tributari).

Rilevano in via generale gli adempimenti connessi con le seguenti attività:

- Definizione di nuovi prodotti;
- Acquisto del credito di imposte;
- La compensazione della tassazione della Banca;
- La dichiarazione fraudolenta con artifizi e raggiri;
- Il credito fiscale acquistato a valore inferiore ed il suo successivo trasferimento alla capogruppo.

Di seguito sono elencate le cosiddette attività sensibili o a rischio identificate – ad oggi - con riferimento ai reati tributari:

1) Gestione della contabilità ordinaria e del servizio amministrativo

2) Gestione della fatturazione attiva
3) Gestione oneri deducibili
4) Gestione IVA
5) Gestione degli adempimenti dichiarativi periodici e calcolo imposte - IRES
6) Gestione degli adempimenti fiscali, tributari e di sostituto d'imposta
7) Gestione degli adempimenti fiscali, tributari e di sostituto d'imposta in service per servizi resi a società controllate
8) Comunicazione informative ad Agenzia delle Entrate

In via residuale, l'ambito di impatto potrebbe anche riguardare il processo di anticipazione su documenti e/o fatture a favore della clientela e il più generale processo del credito con riferimento alle valutazioni del merito creditizio.

Principali presidi organizzativi e gestionali

Le procedure aziendali costituiscono parte essenziale ed integrante del presente Modello.

Si ritiene, sul punto, che il complessivo sistema dei controlli interni sia assolutamente compatibile e sufficiente con i presidi richiesti nel caso di reati della specie in trattazione. Il sistema è in grado di garantire alla Banca un presidio costante sui processi aziendali e sui conseguenti rischi fiscali, consentendole di adempiere al meglio ai doveri di trasparenza e collaborazione previsti dal regime di cooperative compliance. Inoltre, il sistema garantisce la promozione della cultura aziendale improntata a principi di onestà, correttezza e rispetto della normativa tributaria, assicurandone la completezza e l'affidabilità, nonché la conoscibilità a tutti i livelli aziendali.

Parimenti, nella regolamentazione interna sono previsti flussi informativi accurati, completi, tempestivi e facilmente accessibili, garantendo la circolazione delle informazioni a tutti i livelli aziendali.

Va soggiunto che il RAF contiene anche una chiara e documentata strategia fiscale nella quale vengono evidenziati gli obiettivi dei vertici aziendali. La strategia riflette la propensione al rischio, il grado di coinvolgimento dei vertici aziendali nelle decisioni di pianificazione fiscale e gli obiettivi che la banca si pone in relazione ai processi di gestione del rischio fiscale.

I temi toccati dal RAF riguardano, ad esempio:

- il c.d. risk appetite del vertice aziendale, che va nel senso di ridurre al minimo il rischio, trattandosi comunque di violazioni di legge;
- il livello di coinvolgimento del consiglio di amministrazione nelle decisioni che coinvolgono gli adempimenti di natura fiscale;
- l'approccio riguardante la prevenzione del contenzioso tributario;

- la trasparenza voluta nei riguardi del pubblico, al di là di quanto obbligatorio, per quanto attiene alla sfera fiscale.

E ancora. Il sistema assicura una chiara attribuzione di ruoli a persone con adeguate competenze ed esperienze, secondo criteri di separazione dei compiti, esplicitando le responsabilità connesse ai ruoli in relazione ai processi di rilevazione, misurazione, gestione e controllo del rischio fiscale, garantendone, altresì, il rispetto delle procedure a tutti i livelli aziendali. Il sistema prevede efficaci procedure di monitoraggio che, attraverso un ciclo di autoapprendimento, consentono l'individuazione di eventuali carenze o errori nel funzionamento dello stesso e la conseguente attivazione delle necessarie azioni correttive.

Dunque, per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati tributari:

a) Predisposizione di adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio, nonché di ogni altra comunicazione di carattere finanziario, nel rispetto dei principi civilistici e fiscali vigenti:
   - Identificazione dei dati e delle notizie che ciascuna funzione od unità organizzativa deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro trasmissione alla funzione responsabile;
   - Previsione di istruzioni rivolte alle unità organizzative che indichino dati e notizie che è necessario fornire alla funzione preposta alla redazione del bilancio per le chiusure periodiche;
   - Mappatura a sistema dei conti ed i relativi saldi del bilancio di verifica per la corretta riconduzione dei saldi ai conti del bilancio di esercizio;
   - Registrazioni contabili riferite ad un esercizio siano effettuabili solo nei periodi di contabilizzazione aperti;
   - Sistema che non consente la duplicazione dei numeri delle registrazioni contabili.

b) Mantenimento di una condotta improntata ai principi di correttezza, trasparenza e collaborazione nello svolgimento delle procedure volte alla formazione del bilancio, delle situazioni contabili periodiche e delle comunicazioni sociali in generale.

c) Controlli trimestrali da parte della Società di Revisione incaricata del controllo contabile.

d) Previsione della rilevazione, trasmissione e aggregazione delle informazioni contabili finalizzate alla predisposizione di comunicazioni sociali tramite sistema informatico, in modo che sia sempre garantita la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti che inseriscono i dati a sistema.

e) Sistema di monitoraggio e controllo del rischio fiscale afferente ai processi aziendali e di business e dei contenziosi fiscali.

f) Fornitura di informazioni veritiere ed appropriate sulla situazione economica, patrimoniale e finanziaria della banca.

Flussi informativi a favore dell'OdV

I flussi al riguardo devono avere periodicità annuale, fatte salve specifiche circostanze, quali ad esempio l'adattamento ai principali cambiamenti che riguardano l'organizzazione del comparto, ivi comprese le modifiche della legislazione fiscale.

Il responsabile dell'Ufficio contabilità provvederà a redigere apposita relazione con cadenza annuale, nella quale dovranno rilevarsi gli esiti dell'esame periodico e delle verifiche effettuate sugli adempimenti tributari, le attività pianificate, i risultati connessi e le misure messe in atto per rimediare alle eventuali carenze emerse a seguito di monitoraggio.

Le funzioni aziendali di controllo concorrono alla reportistica di competenza con la medesima cadenza.

Art. 25- sexiesdecies - Contrabbando

Come anticipato nella parte generale del presente modello, l'inserimento dei reati di contrabbando nell'elenco dei "reati presupposto" 231 incide sugli eventuali rapporti intrattenuti da banca - in via diretta o indiretta - con i paesi extra UE.

Al riguardo si precisa che ciò implica un'attenta analisi mirata ai rapporti intrattenuti dai clienti della Banca, specialmente nell'ambito delle operazioni di anticipazioni e/o di credito documentario, posto che la Banca per le sue caratteristiche non opera con fornitori di Paesi extra UE. Pertanto, verranno prese in considerazione e valutate le eventuali ipotesi da monitorare, non tanto con riferimento alle attività della banca, quanto alle operazioni realizzate dalla clientela con riferimento, ad esempio, all'importazione di merci da paesi extracomunitari, al ciclo passivo riguardo alla merce importata senza i dovuti controlli, ossia senza attinenza con quanto inserito nella bolletta doganale. A ciò rileva anche l'ipotesi di riciclaggio con il commercio internazionale da parte della clientela. Particolare attenzione verrà riposta nei confronti dei processi di individuazione degli spedizionieri, in quello di approvvigionamento delle materie prime e soprattutto alla possibilità di poter disporre del tracciamento della merce.

Il delitto di contrabbando potrebbe realizzarsi attraverso un uso fraudolento dell'istituto del c.d. "deposito IVA" (art. 50-bis del DL 331/1993) e, dunque, illecitamente profittando del meccanismo di autofatturazione: l'utilizzo illecito del meccanismo dell'importazione in libera pratica tramite "deposito IVA" viene, infatti, talvolta contestato quale modalità di realizzazione del contrabbando (Cass. pen. 26202/2015).

In estrema sintesi, la merce può essere fatta figurare come importata, salvo poi disporne l'estrazione immediata e il trasporto dalla dogana a magazzini nella disponibilità di altri soggetti. In tal modo, viene realizzata un'indebita messa in commercio del prodotto, sovente ceduto "in nero" a favore di aziende compiacenti, senza corrisponderne l'IVA dovuta.

Principali presidi organizzativi e gestionali

Valgono, per quanto rileva, i presidi organizzativi e gestionali riguardanti il processo del credito e, soprattutto, quelli relativi al rischio di riciclaggio, attraverso un attento processo di adeguata verifica rafforzata.

Ad ogni buon conto, la Banca:

- √ si impegna a rispettare le normative doganali, nonché i controlli sulle esportazioni ed importazioni

√ si assicura sempre di non intrattenere relazioni commerciali con persone o aziende che sono state inserite dalla Pubblica Amministrazione negli elenchi dei soggetti sottoposti a embargo o restrizioni e/o di dubbia affidabilità.

√ nell'ambito del processo di adeguata verifica della clientela e comunque in tutti i casi in cui si dovessero verificare per qualunque ragione un'operatività con Stati esteri, verifica compatibilmente con le proprie capacità organizzative:

- che tutti i documenti a supporto delle registrazioni, degli adempimenti e delle comunicazioni con le Autorità Doganali siano veritieri, autorizzati e conservati, per i periodi stabiliti dalla legislazione vigente, in modo ordinato e tale da poter effettuare verifiche in qualsiasi momento;
- il possesso dello status di Operatore Economico Autorizzato (AEO) da parte dei soggetti terzi incaricati di espletare le formalità doganali;
- la coincidenza dei documenti a corredo delle spedizioni (es. fatture) con le informazioni attestanti il valore, la quantità, l'origine e la classificazione delle merci riportati nella packing list.

Per quanto attiene alla gestione degli acquisti e tenuta della contabilità, i responsabili delle competenti U.O. provvederanno a:

- garantire l'ottenimento di tutti i permessi e/o autorizzazioni e/o sussistenza di tutti i requisiti di Legge per l'ingresso del bene nel Territorio Comunitario;
- verificare la corretta classificazione delle merci a cui corrisponde l'applicazione della franchigia e/ o regime di riduzione del dazio;
- verificare la corretta fruizione del beneficio in funzione della fattispecie agevolativa di riferimento (es. Ammissione temporanea, Carnet ATA, perfezionamento passivo);
- assicurare la sussistenza di controlli riguardanti i seguenti aspetti:
  - la provenienza dei beni e se i documenti di trasporto riflettano il paese di origine e il flusso di movimentazione;
  - la ragionevolezza nonché la congruità dell'operazione/acquisto rispetto al valore di mercato comunemente applicato sul mercato ed, eventualmente, la sussistenza di valide ragione che giustifichino l'eventuale acquisto di merce «sottocosto»;
  - il corretto calcolo del valore doganale delle merci importate e il pagamento dei diritti doganali;

- la corretta compilazione della dichiarazione doganale;
- assicurare la corretta classificazione doganale delle merci/prodotti e il relativo mantenimento dell'anagrafica degli stessi con indicazione del corretto codice doganale.

Flussi informativi a favore dell'OdV

I flussi informativi vengono assorbiti nell'ambito dei flussi relativi al processo del credito e del riciclaggio.

PARTE III

IL PROCESSO DI AUTOVALUTAZIONE (SELF ASSESSMENT)

Con l'approvazione del presente documento, viene deliberata anche la scelta da parte della Banca di provvedere – in coerenza con le best practice - al periodico processo di autovalutazione a prescinde dall'effettivo coinvolgimento della banca in un procedimento penale.

Trattasi di esame in ottica costruttiva, ossia l'opportunità di miglioramento non imposta proprio perché la banca non deve valutare l'idoneità e l'attuazione del Modello in relazione ad uno specifico rischio di reato già verificatosi, quanto, piuttosto, in relazione all'insieme dei rischi (ipotetici) ritenuti rilevanti nell'ambito del Modello organizzativo.

In particolare, si fa riferimento ad una periodicità:

- annuale, per quanto riguarda l'autovalutazione generale di idoneità e attuazione;
- triennale, per una autovalutazione specialistica e di dettaglio, che può essere opportunamente svolta anche in occasioni particolari, quali, ad esempio, eventuali vicende modificative della struttura aziendale o richieste di due diligence.

Per quanto ovvio, protagonista principale dell'autovalutazione annuale sarà l'OdV, con la collaborazione di tutte le Funzioni aziendali: Legale e Compliance in primis. Ma possono, evidentemente, essere coinvolti tutti i soggetti-chiave della governance aziendale e del sistema di controllo interno. Per la valutazione triennale specialistica potrebbe essere opportuno che la banca si avvalga di consulenti esperti della materia che gestiranno l'esame documentale e le interviste necessarie.

In entrambe le ipotesi, occorre provvedere alla redazione di apposito report al Consiglio di amministrazione sull'idoneità e l'attuazione del Modello organizzativo.

Per quanto rileva, si richiama integralmente – quale linea guida - il noto "Decalogo 231" del Tribunale di Milano, riassumibile come segue:

1) Il Modello deve essere adottato partendo da una mappatura dei rischi di reato specifica ed esaustiva e non meramente descrittiva o ripetitiva del dettato normativo.
2) Il Modello deve prevedere che i componenti dell'organo di vigilanza posseggano capacità specifiche in tema di attività ispettiva e consulenziale.
3) Il Modello deve prevedere quale causa di ineleggibilità a componente dell'OdV la sentenza di condanna (o di patteggiamento) non irrevocabile.

4) Il Modello deve differenziare tra formazione rivolta ai dipendenti nella loro generalità, ai dipendenti che operino in specifiche aree di rischio, all'organo di vigilanza ed ai preposti al controllo interno.
5) Il Modello deve prevedere il contenuto dei corsi di formazione, la loro frequenza, l'obbligatorietà della partecipazione ai corsi, controlli di frequenza e di qualità sul contenuto dei programmi.
6) Il Modello deve prevedere espressamente la comminazione di sanzione disciplinare nei confronti degli amministratori, direttori generali e compliance officers che per negligenza ovvero imperizia non abbiano saputo individuare, e conseguentemente eliminare, violazioni del modello e, nei casi più gravi, perpetrazione di reati.
7) Il Modello deve prevedere sistematiche procedure di ricerca ed identificazione dei rischi quando sussistano circostanze particolari (es. emersione di precedenti violazioni, elevato turnover del personale).
8) Il Modello deve prevedere controlli di routine e controlli a sorpresa – comunque periodici nei confronti delle attività aziendali sensibili.
9) Il Modello deve prevedere e disciplinare un obbligo per i dipendenti, i direttori, gli amministratori della società di riferire all'organismo di vigilanza notizie rilevanti e relative alla vita dell'ente, a violazioni del modello o alla consumazione di reati. In particolare, deve fornire concrete indicazioni sulle modalità attraverso le quali coloro che vengano a conoscenza di comportamenti illeciti possano riferire all'organo di vigilanza.
10) Il Modello deve contenere protocolli e procedure specifici e concreti.

Va, infine, tenuto in debita considerazione il contenuto della circolare n. 83607/2012 del Comando Generale della Guardia di Finanza, nella quale viene spiegato che l'attività investigativa dovrà essere indirizzata sul Modello, sul suo contenuto dichiarativo e descrittivo e, in secondo luogo, sull'efficacia del Modello, comportando la valutazione di circostanze fattuali concrete e l'acquisizione di ulteriori dati ed elementi di natura obiettiva. L'esclusione di responsabilità passa attraverso un giudizio sul c.d. sistema preventivo attuato dalla società, che l'organo giudicante penale, in occasione del procedimento a carico dell'autore dell'illecito, dovrà formulare, valutandone sia l'idoneità a svolgere la funzione di prevenzione che la legge gli attribuisce, sia le effettive, concrete e dinamiche modalità con cui lo stesso è reso operante all'interno dell'ente. Tuttavia, sul piano oggettivo, il Modello è sufficientemente identificabile in funzione degli obiettivi cui esso è destinato, e può descriversi come un sistema strutturato ed organico di procedure nonché di attività di controllo, da svolgersi anche in via preventiva (controllo ex ante), strumentale alla prevenzione dei reati responsabilizzanti ai sensi del D.Lgs. n. 231/2001. Deve,

comunque, essere considerata costantemente l'esistenza di un "sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro.